Learning from "Shadow Security": Understanding Non-Compliant Behaviours to Improve Information Security Management

Iacovos Kirlappos

A thesis submitted for the degree of

Doctor of Philosophy

at

University College London

Department of Computer Science

University College London

March 2016

I, Iacovos Kirlappos, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

This thesis examines employee interaction with information security in large organisations. It starts by revisiting past research in user-centred security and security management, identifying three research questions that examine (1) employee understanding of the need for security, (2) the challenges security introduces to their work, together with their responses to those challenges, and (3) how to use the emerging knowledge to improve existing organisational security implementations. Preliminary examination of an available interview data set, led to the emergence of three additional research questions, aiming to identify (4) employee actions after bypassing organisational security policy, (5) their response to perceived lack of security support from the organisation, and (6) the impact of trust relationships in the organisation on their security behaviours.

The research questions were investigated in two case studies inside two large organisations. Different data collection (200 interviews and 2129 surveys) and analysis techniques (thematic analysis and grounded theory) were combined to improve outcome validity and allow for generalisability of the findings.

The primary contribution of this thesis is the identification of a new paradigm for understanding employee responses to high-friction security, the *shadow security*: employees adapt existing mechanisms or processes, or deploy other self-devised solutions, when they consider the productivity impact of centrally-procured security as unacceptable. An additional contribution is the identification of two trust relationships in organisational environments that influence employee security behaviours: *organisation-employee trust* (willingness of the organisation to remain exposed to the actions of its employees, expecting them to behave securely), and *inter-employee trust* (willingness of employees to act in a way that renders themselves or the organisation vulnerable to the actions of another member of the organisation).

The above contributions led to the creation of a structured process to better align security with organisational productive activity, together with a set of relevant metrics to assess the effectiveness of attempted improvements. The thesis concludes by presenting a case study attempting to apply the above process in an organisation, also presenting the emerging lessons for both academia and industry.

Acknowledgements

None of the work presented in this thesis would have been possible without the continuous and invaluable support of my supervisor M. Angela Sasse and the other members of the Information Security Research Group at UCL. A special mention for Dr Simon Parkin, for his help in data analysis, paper writing and feedback throughout this PhD project. I would also like to thank all the people in partner organisations that helped me collect and analyse the data presented in this thesis.

I am grateful to be supported by an amazing family, Andreas, Varvara and Christodoulos, who, despite being thousands of miles away, never left me feeling alone throughout this work. I am also deeply grateful to all my friends, both in Cyprus, the UK, and anywhere else in the world, for their continuous and unconditional support.

Contents

List of figures

List of tables

Glossary

Affordable security: security mechanisms that create minimal (or acceptable) overheads on employee primary tasks

Assurance mechanisms: technical controls/mechanisms required for detection of security policy violations and enforcement of formal rules

BYOD: Bring your own device – employees allowed to use personal equipment for corporate tasks

Cyberattack: attempt to inflict damage on an organisations systems or access sensitive information

DLP: Data loss prevention; software that aids system administrators in monitoring and controlling what data users can transfer through data transfer channels

Externalities: term from economics referring to costs or benefits affecting parties who did not choose or act to incur those. Can be positive (benefits) and negative (costs)

Insecure behaviours: employee behaviours that increase organisational exposure to security risks - includes both actions prohibited by security policy or other organisational documents and others not officially prohibited.

Mental models: mental models are descriptions of a user's understanding of a problem and perception of how things work

Non-compliance: employees acting in ways explicitly prohibited by an organisation's security policy/mechanisms

Primary task: the actions humans perform when interacting with technology in order to achieve the goal of the interaction

Productive activities: set of different primary tasks leading to delivering desired organisational targets

Security-productivity friction: conditions where elements of a security implementation create problems or overheads in user attempts to complete primary task related activities

> *Friction-inducing*: elements of the security implementation that create friction

Security culture: set of collective norms and values, developed based on the employees' interaction with information security elements or the behaviour of their colleagues

> *Team security culture*: security culture developed within organisational sub-divisions

Security hygiene: property of security mechanisms or processes indicating that they have been designed around employee tasks and priorities

Security implementation: mechanisms, rules, policies, training and communication aiming to reduce organisational security risk exposure

Shadow security: employees deploying own solutions when security is perceived as not serving their primary task focus

Trust: the willingness to be vulnerable based on positive expectation about the behaviour of others

> *Inter-employee*: the willingness of employees to act in a way that renders themselves or the organisation vulnerable to the actions of another member of the organisation.
>
> *Organisation-employee*: the willingness of the organisation to remain exposed to the actions of its employees, expecting them to behave securely
>
> *Trustworthy behaviour*: employees behaving as the organisation expects

Chapter 1: **Introduction**

Information security is becoming increasingly relevant to modern organisations. Throughout the past four decades, technology has transformed organisational production processes, which led to the success, but also survival, of many organisations depending on their ability to protect their technology systems and the information stored on those. Uninterrupted system operation and continuous information availability are key enablers for organisational operations and ability to provide services to customers. In addition, sensitive customer information, financial results, upcoming product releases, R&D outcomes and any other information not available in the public domain, requires some level of protection to maintain competitive advantage, but also avoid potential legal consequences and reputation damages from sensitive information leakages. This led to information security emerging outside its original role in the military and secret service domain, and becoming a central part of modern organisational management (von Solms, 2006). Today, information security requires well-designed risk assessment and management, implementation of processes and technical mechanisms for information and system protection, but also policy formulation, communication and enforcement; all the above aim to deliver the best possible risk mitigation, using the available resources. The importance of information-related risks made information security[1] a significant priority not just for information security management, but also for corporate governance (Gabel et al., 2015).

Despite the increased attention and investment information security receives, industry reports on information security breaches (IBM, 2014, Table 1), suggest that current approaches are failing to provide effective protection. Organisations are still significantly exposed to information security risks and potential consequences.

Percentage of large businesses attacked by an unauthorised outsider in the last year	55%
Percentage of large organisations that suffered from infection by viruses or malicious software in the past year	73%
Percentage of large organisations that were hit by denial of service attacks in the last year	38%
Percentage of large organisations that detected successful outside penetration of their network in the last year	24%
Percentage of large organisations knowing that outsiders have stolen their intellectual property or confidential data in the last year	16%

Table 1: Latest security breach statistics (IBM, 2014)

According to IBM's Computer Security Incident Response team, a significant percentage of the above compromises (95%) relates to human error (IBM, 2014). Exploiting the human element to bypass technical protection has been a fruitful approach for attackers throughout the years. Kevin Mitnick for example testified to the US Senate committee how 9 out of 10 passwords he managed to compromise in a

[1] Lately increasingly referred to as *cyber security* but, as protection of information is not restricted to the cyber space, this thesis will stick to the traditional (and more common in academia) term, *information security*.

series of attacks were obtained by tricking target organisations' employees to share sensitive information with him, rather than breaking through their technical defences (Mitnick and Simon, 2002). Additional examples of how employee behavioural traits and willingness to be helpful can be exploited to damage organisational security protection have been described, amongst many others, by Winkler, (1997) and Hadnagy (2010). The vulnerabilities human behaviour can introduce in current security implementations led to Schneier (2000) stating that "*... security is only as good as its weakest link, and people are the weakest link in the chain*".

The success of attacks against employees, suggests that more research is required, in order to improve employee participation in organisational security implementations. In an attempt to improve existing understanding of employee security behaviour, and also improve security researchers' and practitioners' ability to better accommodate for employee behaviours in security management, this thesis presents an in-depth investigation and characterisation of employee interaction with organisational security implementations. Recognising the drawbacks and failures of past organisational security research and practice approaches, the research used a case study approach, engaging directly with employees, exploring their interaction with various elements of security implementations, the emerging problems in their productivity-related activities and their subsequent responses. This aimed to generate knowledge that can be used to design security mechanisms and processes better suited to employee productivity tasks, also allowing security managers to make more effective resource allocation decisions and deliver the best possible security protection.

1.1 Background

Effective information security cannot be delivered by perfecting the effectiveness of technical controls; it is also crucial for the systems and processes in place to be well-suited to the tasks, priorities and understanding of their users. This need to fit secure systems to their users was first discussed by Kerckhoffs (1883) in his military cipher design principles: "*Given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules*". Many years later, Saltzer and Schroeder (1975) first included usability in the requirements for modern security systems. The growing realisation that systems are as strong as the people who use them, led to the emergence of user-centred security as an academic discipline in the mid-to-late 90s. Researchers like Zurko and Simon (1996), Adams and Sasse (1999) and Whitten and Tygar (1999) presented research results demonstrating that security systems not designed around human behavioural principles lead to insecure behaviours. A significant amount of research on user-centred security has been published since then, aiming to provide knowledge and generate methodologies for behaviour-driven systems design to improve employee interaction with security. This research identified a number of drawbacks in current attempts to manage employee security behaviours in organisations:

1. Currently security is designed and deployed without considering employee productivity priorities, leading to ineffective policies (Saunders, 2012), inflexible control-based security management (Vroom and von Solms, 2004) and ineffective security communication (Stewart and Lacey, 2013).
2. Employees have to invest significant resources (time and effort) interacting with security processes, mechanisms and policies that were not designed around their productivity needs.

When security demands more resources than what they consider acceptable (their *Compliance Budget* – Beautement et al., 2008), insecure behaviours become the only way to limit their exposure to such resource-demanding security implementation elements (Herley, 2009; Inglesant and Sasse, 2010)

3. Current security management approaches to reduce insecure behaviours are primarily focused on increasing control to ensure employees behave as required (through increased formulation of security policies and mechanisms). But attempts to enforce increased control also increase security deployment costs (Pallas, 2009) and lead to alienation between security management and employees (Gurbaxani, 2010; Mintzberg, 1985). In addition, when control elements further increase the security-related overhead on employee tasks, employees have even stronger incentives to bypass security (Bartsch and Sasse, 2012; Beautement et al. 2008; Bulgurcu et al., 2010; Inglesant and Sasse, 2010); the emerging high non-compliance rates eventually make enforcement expensive and ineffective (Adams and Sasse, 1999; Hine, 2014; Tuyls et al., 2007).
4. Security education and training are also deployed by security managers to provide motivation for secure employee behaviours (Thomson and Solms, 1997). Current attempts fail to provide effective motivation though, due to information overload (Stewart and Lacey, 2013) and failure to adapt the communicated principles to role-specific risks employees face. The content communicated is generic (Morgan, 2002), often focusing on extreme cases rather than everyday employee challenges (Herley, 2014).

Given the above inability of security managers to implement security designed around employee productivity priorities, industry reports that insecure behaviours are rife in organisations (e.g. IBM, 2014) come as no surprise. Non-compliance with security mechanisms and processes may be increasing organisational exposure to security risks, but it is the only option for employees seeking to preserve their productive capabilities (Beautement et al., 2008; Blythe et al., 2014; Herath and Rao, 2009). As a result, attempts to eliminate it through technical solutions and user training are inevitably failing. When security managers possess little understanding of the behavioural principles that dictate employee security behaviours and their focus on productivity, the emerging security implementations will often lead to non-compliant behaviours, increasing organisational security risk exposure.

A number of researchers examined user security behaviours in the past few years. The main paradigm that emerged is the characterisation of employee security decision making as an economic problem (e.g. Beautement et al., 2008; Bulgurcu et al., 2010; Herley, 2009): security is a secondary task (Pfleeger and Sasse, 2015), but it often gets in the way of primary task completion, consuming significant user time and effort, with users gaining no additional perceived benefit from following it. As a result they eventually ignore it (Herley, 2009), also getting habituated to such behaviours over time (Schechter et al., 2007).

Despite improving understanding of security decision making, close examination of past security behaviour research identified a number of drawbacks:

1. Attempts for in-depth examination of security behaviour depth focused on individual home users (Dourish et al., 2004; Herley, 2009; Wash, 2010), without, to the author's best knowledge, any

attempts to holistically investigate employee interaction with organisational security implementations and identify their responses to those.

2. Attempts to characterise non-compliant employee behaviours and identify the factors that lead to those by directly interacting with them, were limited to password behaviours (Adams and Sasse, 1999; Inglesant and Sasse, 2010; Sasse et al., 2001; Weirich, 2005) and access control mechanisms (Bartsch and Sasse, 2013).
3. Employee behaviour is mostly approached as a binary decision, with their actions being characterised as either secure or insecure, with no attempt to identify the effect of security overheads on the attitude and actions of risk-aware employees who understand the need for it.
4. Attempts to deliver user-centred security by improving security design processes and requirements gathering focused primarily on providing guidance to design new systems (Faily and Fléchais, 2010; Fléchais et al., 2007). Despite their usefulness, these approaches are of limited use to organisations that need to improve their existing security implementations and incentivise secure employee behaviour within their current security implementations (Ashenden and Sasse, 2013).
5. The use of metrics in security behaviour is limited. Metrics are now a key part of modern information security management (e.g. Brotby et al., 2013; Payne, 2009; ISO27004), but no effective metrics for employee security behaviour have emerged to date. This prevents organisations from identifying potential areas to focus security improvement attempts to better accommodate for employee priorities.

The identified drawbacks of past research, suggest the need for further research in organisational security in order to: (1) improve current understanding of the drivers behind employee insecure behaviours, (2) understand and characterise employee experience when interacting with organisational security implementations, and (3) identify potential sources of information that can be used to devise metrics that can aid more effective information security behaviour management in organisations.

1.2 Research questions

Aiming to improve existing knowledge of employee security behaviour and provide guidance for effective security management, this thesis attempts to answer the following research questions (devised based on close examination of past research, but also emerging from the early stages of the iterative analysis approach used in this research – for more information on research question formulation please refer to sections 3.3.1 and 4.7.2):

1. *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?*
2. *What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?*
3. *When organisational security provisions appear to provide inadequate risk mitigation, what do employees do?*
4. *How do employees respond to perceived lack of organisational security support? What are the risks from their behaviours and what can organisations learn from those?*

5. *How can the improved understanding from the previous questions be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?*
6. *What trust relationships develop in an organisation and how do they influence security behaviours?*

Examination of the above research questions led to the emergence of three security behaviour paradigms: (1) categorisation of employee insecure behaviours based on the conditions that lead to their development (chapter 4), (2) identification of the existence of *shadow security* in the organisation, with employees deploying their own solutions when security was perceived as not serving their primary task focus (chapter 5), and (3) the existence of two security-related trust relationships that influence employee security decision making (*organisation-employee trust* and *inter-employee trust* - chapter 6). In-depth examination of the development of the above phenomena also allowed identifying a number of sources of measurable security behaviour-related information. This was then used to devise a process to identify shadow security in an organisation and then leverage it to deliver more effective information security management (chapter 7).

1.3 Research approach

In order to answer the research questions discussed in the previous section, the research presented in this thesis used two case studies conducted in two large commercial organisations (which will be referred to as *Company A* and *Company B* from here onwards). Case studies were chosen due to their compatibility with the exploratory nature of the research questions: they can reveal insights difficult to capture through statistical testing of predefined hypotheses (Eisenhardt, 1989). As a result, they were used to provide in-depth understanding of the drivers behind both secure and insecure behaviours in organisations. The researcher used existing and newly collected data, both collected through direct engagement with employees. The data collection process did not focus on studying security mechanisms in isolation, like the majority of past research has done. Instead, it attempted to holistically capture employee experience with, and attitudes towards security, together with their corresponding behaviours.

The exploratory nature of the research questions also required a data analysis approach that would allow for theories answering the research questions to emerge directly from the data. As a result, *grounded theory* (Strauss and Corbin, 1998) was chosen as the primary data analysis method. 200 semi-structured interviews from both organisations were analysed, with two large-scale surveys also used to confirm the prevalence of the identified behavioural patterns across the two organisations. Data analysis was done as an iterative process, with grounded theory categories and relationships between them continuously revisited and updated as new knowledge emerged, aiming to more accurately capture employee attitudes, beliefs, knowledge, priorities and better characterise any emerging behavioural phenomena. Before commencing the grounded theory analysis, a thematic analysis (Braun and Clarke, 2006) on a subset of the available data was also conducted, aiming to provide some preliminary understanding of employee behaviours represented in the data and drive the subsequent grounded theory analysis.

1.4 Research scope

The paradigms emerging from this research (employee behaviour categorisation, shadow security development and security-related trust relationships) improved existing understanding of employee interaction with organisational security implementations and their responses to the problems those cause. They also provided valuable knowledge that modern security management can use to better manage employee security behaviours. Despite that, two potential research scope limitations were identified:

1. *Organisational nature*: The organisations examined share a number of properties: they are large, have more than 10000 employees each, located in various locations around the UK, also operating at in international level. They also operate in highly regulated areas, with a significant part of the regulation and standards they need to comply with containing clauses that affect their security strategy and implementations.
2. *Employee characteristics*: Employees mostly work on computer-related tasks, in office jobs, and the majority also came from similar environments in their past work history. As a result, they should be assumed to possess slightly higher computer expertise than employees in organisations where tasks are less computerised; on the other hand this also means they are probably more exposed to information security risks, thus widening the scope of the emerging knowledge. In addition, employee security expertise was not possible to investigate before the research commenced to achieve maximal representation of various levels of expertise, but care was taken to engage with employees from various divisions to alleviate the potential impact of this.

Despite the above scope limitations, between-organisation differences in both the technology and processes used, combined with the use of pattern matching to confirm the presence of behavioural patterns identified in Company A with those later identified in Company B, improved the external validity and generalisability of the research findings (discussed in detail in sections 3.4 and 5.4). In addition, the security behaviour management guidelines and processes presented in Chapter 7 can potentially be customised to fit different environments, acting as a useful learning source for those responsible to deliver effective security protection in organisations of various sizes and other operational domains.

1.5 Thesis contributions

The results presented in this thesis significantly improve the available knowledge on employee interaction with security processes and mechanisms that create productivity overheads. They also provide security managers and researchers with valuable insights on how to create better security behaviour management tools and processes in the future. In particular the results provided:

1. Identification of employee desire to help in security and invest some of their time and effort to protect the organisation they work for, unless security is creating significant productivity overheads or they lack sufficient awareness.
2. Categorisation of the conditions that lead to insecure employee behaviours: (1) lack of awareness, (2) compliance with security mechanisms and policies being expensive, or (3) compliance being impossible due to mechanism problems.

3. Identification and characterisation of *shadow security* behaviours. When security experts insist on "standard" or "best practice policies" that create problems in employee productive abilities, employees do not wilfully disregard security; instead they procure, deploy and refine their own solutions, outside the control of the organisation's designated security management division.
4. Identification of two trust relationships that influence security behaviours. *Organisation-employee trust*, suggesting the presence of some implicit trust from the organisation towards its employees to behave securely that is not formalised in the security strategy, but can be inferred from the flexibility employees are allowed in their security behaviours. *Inter-employee trust* on the other hand, is developed between employees and acts as a readily-available resource when security creates productivity overheads, encouraging employees to procure their own shadow security solutions.
5. Development of a user behaviour model, demonstrating how various elements of the organisational environment influence employee security decisions, culture and habit development.
6. Demonstration of the importance of *security hygiene*: security designed around employee tasks and priorities is a prerequisite to any attempts to implement effective organisational security.
7. Guidance on how organisations can use the above knowledge (1-6) to develop a metrics-driven organisational learning approach to aid future security decision making and better align it with organisational risk management strategy.
8. Demonstration of the usefulness of case studies as an effective information security research approach, in combination with grounded theory analysis to generate new knowledge on topics where current understanding is limited.
9. Presentation of a number of lessons learned while attempting to apply the findings of this thesis in an organisation. These lessons are used to provide advice for future collaborative work between academia and industry, but also to aid application of the research findings to deliver more effective and efficient information security management.

Essentially this thesis argues that in any security implementation, no one should have to choose between security and productivity. If the right learning and improvement processes are implemented, security management can deliver effective and efficient protection, while also continuously assessing its effectiveness and productivity impact to intervene when usability improvements are required.

1.6 Thesis structure

Chapter 2 (*Background*) reviews past literature on user-centred security and security in organisations. It discusses past and current attempts to manage the human element of information security and identifies a number of reasons for the failure of current approaches to deliver effective protection. It then explains how the research gaps identified led to the emergence of the research questions and drove the work presented in the remainder of this thesis.

Chapter 3 (*Methodology*) presents the research approaches, data collection and analysis processes used, discusses steps taken to improve outcome validity, also presenting a set of ethical research principles followed while conducting this research.

Chapter 4 (*Security behaviour drivers*) presents the process of the thematic analysis conducted, discusses emerging codes and themes and explains how their identification led to the characterisation and categorisation of non-compliant behaviour drivers, based on the conditions that led to their emergence. It also discusses the identification of a third category of security behaviours, in addition to the existing compliant or non-compliant categorisation: employees devising their own security solutions outside the control of security managers. Identification of this third category drove the subsequent grounded theory analysis presented in Chapter 5. The findings of this chapter also led to the creation of a preliminary model of employee security behaviour and identified the potential existence of security-related trust relationships that drove the analysis presented in Chapter 6.

Chapter 5 (*The shadow security*) presents a grounded theory analysis of the available interviews, investigating employee experience with the organisation's security implementation and emerging behaviours. This analysis led to identification and characterisation of a new security behaviour paradigm, the *shadow security*: employees deploying own solutions when security is perceived as not serving their primary task focus. The chapter also analyses the drivers of shadow security development, the emerging risks and consequences for organisational security management, and how security managers can use shadow security as a tool to reduce conflicts between security and productivity. It also presents the steps taken to improve the validity and understanding of the emerging behavioural phenomena.

Chapter 6 (*Trust and security behaviours*) presents a new grounded theory analysis examining the development and influence of trust on employee security behaviours. It identifies two different security-related trust relationships in the organisational environment (*organisation-employee trust* and *inter-employee trust*), explains how they come to conflict, and presents their impact on shadow security development.

Chapter 7 (*Using shadow security to improve security management*) uses the lessons learned from Chapters 4, 5 and 6 to provide guidelines for effective and productive management of shadow security by security managers, focusing on five areas: (1) the need to move away from current binary understanding of user behaviour, (2) understanding that "unusable" elements of security implementations need to be removed before attempting to influence employee behaviours, (3) leveraging shadow security as a learning tool to engage employees in security management, (4) leveraging the presence of trust as an additional defence layer, and (5) measuring readily available or easy to collect data to assess the effectiveness of existing approaches and identify areas where improvements are required.

Chapter 8 (*Case study in industry and lessons learned*) discusses how the improved understanding of employee security behaviours that emerged from the other chapters was used to drive security improvement attempts in Company B, focusing on the lessons learned from applying the findings of this thesis in a corporate environment.

Chapter 9 (*Conclusion and contributions*) uses the findings presented in this thesis to answer the research questions, discusses research contributions for industry and academia, presents a critical review of the thesis and outlines potential future research directions based on the emerging paradigms.

Chapter 2: **Background**

A growing number of information security researchers and practitioners are now focused on creating security mechanisms that accommodate for the needs and understanding of their target users: in the past 15 years, a significant amount of research has been published on user-centred security, covering a wide range of topics from improving interface design to better understanding security decision making. Modern organisational security management also considers user behaviour as a key element of effective security, but current approaches fail to leverage employees as an effective defence layer. This chapter presents an examination and discussion of past and current attempts to manage the human element of information security, by both researchers and practitioners. The chapter identifies a number of reasons for the failure of current approaches to deliver effective protection. It also explains how the identified research gaps inspired the work presented in the remainder of this thesis, in order to create an approach that improves employee participation in delivering effective information security.

2.1 Defining information security

Before discussing the current state of information security in organisations and its impact on employee behaviours, it is important to define information security as a term and its use in this thesis. The term has been defined in various ways, either as (1) a risk management discipline (e.g. Blakley, McDermott, and Geer, 2001), (2) a process that aims to protect intellectual property (Pipkin, 2000), or as (3) an action/state of protecting information and information systems (CNSS, 2010). Aiming to disambiguate and consolidate the various definitions, Cherdantseva and Hilton (2012) examined a number of those by various sources, from both industry and academia. Based on the above, they defined information security as *"a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats".* The above definition positions information security as a discipline that identifies the threats to information and information systems, and then implements appropriate controls to protect from those. This approach is in line with information security risk management practices, as defined by a number of widely-adopted international standards (NIST 800-39; ISO 27005; IRAM2):

1. *Identify threats*. A threat is "*anything that is capable, by its action or inaction, of causing harm to an information asset*" (IRAM2). Some common ones are: software attacks (e.g. Viruses, worms, phishing attacks, and Trojan horses), theft of intellectual property, identity theft (acting as someone else to obtain access to systems or vital information), theft of information-carrying equipment, sabotage (to cause operational disruption), and information extortion (e.g. theft and ransom demands to return information or ransomware). Threats are identified and categorised through risk analysis.
2. *Assess vulnerability and exposure*. Vulnerabilities are elements of the organisational environment (systems, assets, procedure) that can lead to the threats materialising as a security incident or breach (ISO27005). They can emerge from weaknesses in design, implementation,

operation or internal control (ISACA, 2009), and exposure to those is also assessed through risk analysis.

3. *Define security goals*. Based on the identified threats and exposure to those, a set of security goals is devised, aiming to protect the target environment or reduce exposure to identified threats to acceptable impact levels.
4. *Implement appropriate controls*. Controls are security mechanisms and processes, implemented to achieve the security goals.

The primary goals of an information security implementation are encapsulated in what is known as the *CIA Principle* (*Confidentiality, Integrity, Availability* - Whitman and Mattord, 2011):

- *Confidentiality*: Limit access and disclosure of information stored and communicated through a system to authorised entities (individuals or systems), also preventing access by or disclosure to unauthorised entities.
- *Integrity*: Ensure unauthorised creation, modification or deletion of information is either impossible, or detectable through implementation of appropriate mechanisms.
- *Availability*: Ensure uninterrupted access to information and services for those authorised to access those.

The desired elements of the CIA triplet, are delivered by the implementation of appropriate controls, depending on the environment to be protected and the identified risks. Successful control delivery above reduces organisational risk exposure to levels acceptable by an organisation's security management (Pelaez, 2010).

2.2 Information security goes mainstream

The need to protect information has evolved significantly since its early deployments by military generals in ancient times to protect their message exchanges (Graves, 2007; Kelly, 1998). From a primarily military and political concern, it has now become a major consideration for anyone who uses information handling systems: individuals, law enforcement, government and corporations, all require some level of protection for their information. This need for commercial information security significantly increased in the 1970's, when computers and data communication technologies started expanding outside the military and political domain and were widely adopted by the commercial world: organisations and businesses started integrating information and communication technologies in their day-to-day operations, which radically changed the way corporate information is stored and shared, consequently increasing the need for information protection mechanisms.

The evolution of the Personal Computer (PC) in the 1980's also created new security challenges. In its early stages, corporate technology adoption was mostly limited to centrally managed-servers in large organisations. The introduction of stand-alone devices (PCs), with independent processing, storage and communication capabilities, led to their wide deployment both at work and home environments for production, entertainment, education and communication. This led to large volumes of digital information being stored on different devices and transferred through a wide range of corporate, home and public networks, which complicates attempts to centrally manage that information. The emerging

challenges were further accentuated by the wide adoption of mobile technologies in the late 20th/early 21st century: modern portable devices store and exchange vast amounts of personal and corporate information through a variety of communication media, with latest ones also increasingly relying on cloud information storage facilities. Consequently, protection of information is now a serious concern for every technology user: from home gamers and online shoppers, to IT managers of multinational organisations and agents of government intelligence agencies, everyone requires effective personal or corporate information protection. This led to the emergence of information security as a professional discipline, combining the principles of the CIA triplet to create solutions that effectively prevent unauthorised access to or disclosure of information, but also guarantee the authenticity and availability of information stored or communicated through technology systems.

2.3 Cryptography and access control

The traditional approach to delivering the CIA triplet is the implementation of access control systems and cryptographic mechanisms[2]. The first aims to provide formal rules and processes to regulate and control access to information, only allowing authorised entities to access, modify, transmit or share it. It is usually implemented by asking access requesters to provide information on identification (*who they are*), authentication (*what they know* or *what they have*) and, using pre-defined *authorisation* rules, grant them access to information or use of a system (Garfinkel et al., 2003). Setup and maintenance of access control is done either by the information owner or, in large information systems, by centrally managed administration authorities. In both cases it involves setting permissions on who is to access specific information or systems and what they are allowed to do with those (e.g. read only, write, execute etc.), with decisions taken on a "need to know" basis (Anderson, 2008). The format of the emerging rules varies across implementations and depends on the access control system in place (e.g. access control lists or role-based access control).

Cryptography is often complementing access control in order to deliver security, changing the form of stored and transmitted information to one unrecognisable by unauthorised entities (Schneier, 1996). This can be done using either (1) *private key encryption*, where a pre-shared key is used to encrypt information at one end and then reused at the other end to reverse the process, revealing the original plaintext, or (2) *public key encryption*, where encryption and decryption are done using separate keys: a public one that can be openly shared with anyone that wants to communicate with its owner, and a private one, known only to the recipient. There are a number of differences between the two, but discussing their application

[2] Cryptography is defined as "*The art and science of keeping messages secure*" (Schneier, 1996): Turning meaningful information to non-sense, unless someone possesses a specific decryption key. Related fields are cryptanalysis ("*the art and science of breaking ciphertexts*") and cryptology ("*branch of Mathematics encompassing both cryptography and cryptanalysis*").

is beyond the scope of this thesis[3]. Correct implementations of cryptography and access control can deliver a significant part of the protection required to meet the CIA triplet:

1. *Confidentiality* is achieved using cryptographic keys to store and transmit information in a form unrecognisable by someone without access to the keys. Access control is also deployed to ensure users can only see and modify information they are authorised to.
2. *Integrity* is achieved through the use of digital signatures, ensuring that the document was created by a particular entity and was not modified during transit.
3. *Availability* is achieved by ensuring access to decryption keys is provided only for those authorised to access encrypted information, with correct access control ensuring no authorised individual is left without access to desired information.

In summary, a correct implementation of cryptographic and access control mechanisms should provide effective information protection (confidentiality and integrity), but also pose no problems to anyone that needs to access it for legitimate reasons (availability).

2.4 Humans and information security

Technical controls can significantly reduce exposure to information security risks, but they can become irrelevant if the users of a system are unable to act appropriately to keep it in a secure state. This section examines how user behaviour leads to security compromises, focusing on two main behavioural traits: (1) users considering security a secondary priority, thus acting in ways that expose the systems they use, and (2) how various elements of human behaviour create vulnerabilities that attackers can expose to compromise information holding systems.

2.4.1 Security is a secondary task

Before examining human behavioural principles that make computer users vulnerable to attackers, it is important to understand what the primary goal of human-technology interaction is. The use of technology usually aims to achieve a goal, for example shop online, with the need for security always being a secondary requirement. Pfleeger and Sasse (2015) formalise this by distinguishing user tasks between *primary* (steps required to achieve goal)[4] and *secondary* (steps required, but not directly perceived as serving goal achievement). For a computer user, security is usually a secondary task and often appears to get in the way of primary task completion (e.g. warnings about expired SSL certificates that are almost always false positives – Herley, 2009). As a result, given limited resources to complete their primary tasks (time or effort), users often ignore secondary tasks: when security becomes an obstacle to primary task completion, users choose to ignore it. This happens either consciously, to reduce impact of emerging externalities on their primary task completion ability (Herley, 2009), or due to

[3] For the remainder of this thesis, references to cryptographic mechanisms should be assumed to include any of the two methods of encryption

[4] In this thesis the *primary task* is defined as: the actions humans perform when interacting with technology in order to achieve the goal of the interaction.

habituation from long-term exposure to security warnings (Schechter et al., 2007). This exposes users and the systems they use to a number of possible attacks, discussed in the following section.

2.4.2 Exploiting human vulnerabilities – understanding scam victims

In an attempt to better understand what makes humans vulnerable to cyberattacks, (Stajano and Wilson, 2011) examined a number of real life scams, identifying seven human behaviour principles that attackers exploit to carry out successful attacks. They argue that "*systems can only be made secure if designers understand and acknowledge inherent vulnerabilities of the human factor*". The seven principles they revealed are discussed below, together with four additional ones that the Stajano and Wilson analysis failed to capture, but emerged from examining further information security research.

2.4.2.1 Distraction

People are always focused on their primary task, whether that is getting a job completed, access their online banking information or buy products online. When security mechanisms or processes are perceived as creating barriers to those activities, they may just ignore those. For example, problems in connecting remotely to a corporate network, caused by a recent change in a company system to improve security, may create tension between end-users and system administrators, with the latter ending up having to relax the rules to restore the access flexibility users were accustomed to. Another distraction example comes from phishing attacks: attackers send emails asking their targets to quickly change their online banking or online shopping password and redirect them to scam websites that steal their money, personal or financial information. The success of those attacks often relies on people paying limited attention to security indicators created to prevent those, or even entirely failing to notice the absence of those indicators from scam websites, due to either long-term habituation or being focused on getting their primary task completed as quickly as possible (Dhamija et al., 2006). A characteristic example comes from a study of phishing indicators by Schechter et al. (2007), where a significant number of computer users in an experiment still attempted to log-in on a website, even after their task was interrupted by a strong security warning. The above strongly suggest that when security appears to get in the way of primary task completion, users often choose to ignore it, making themselves and the systems they use vulnerable to attackers.

2.4.2.2 Social compliance

In many military and corporate environments people are often trained not to question authority, with the same applying to societal authorities (e.g. police). This increases potential susceptibility to *social engineering*: skilled individuals psychologically manipulating people into performing actions compromising security or divulging sensitive information (Anderson, 2008). In his book called "*The Art of Deception*", Kevin Mitnick, a well-known hacker, explains how he took advantage of human willingness to be helpful to successfully carry out a number of large-scale attacks (Mitnick and Simon, 2002). For example, he gained access to proprietary corporate information about a start-up company by waiting until the CEO went out of town, then showing up at the company headquarters pretending to be a close friend and business associate of the CEO. As Mitnick says, the more people are trained to follow superior's demands without questioning those, the more likely they are to fall victims to this type of attacks.

2.4.2.3 Herd principle

People let their guards down when others around them appear to take similar risks. Computer users rarely check the authenticity of reviews on websites for example, which makes them vulnerable to fake reviews by malicious agents using those to appear trustworthy (Mukherjee et al., 2012). Kirlappos et al. (2012) also identified similar behaviour in the use of online reputation seals, with users reporting their presence affected their trust placement decisions for websites, but never checked their authenticity. This leads to users often failing to notice attacks on online reputation and customer review systems, like the creation of fake review systems or the addition of fake reviews on a genuine one. Thinking they are dealing with a reputable retailer, they often fall victims to cyberattacks.

2.4.2.4 Dishonesty

Anything illegal an individual does can be used against them by law enforcement. This makes it harder for victims to report potential crimes against them, as they may have demonstrated intention to engage in illegal activities. Falling prey to Nigerian 419 scams for example (Smith, 2009), often involves agreeing with the other party (the attackers) to carry out money laundering-related activities. As Stajano and Wilson explain, once initiating such a transaction an individual may be reluctant to discuss their actions with the police, leaving them to absorb potential losses they suffer from an attack.

2.4.2.5 Deception

In a digital environment things are often not what they appear to be; many trustworthiness signals of the physical world break down once activities are transferred online (Riegelsberger et al., 2005). Attackers take advantage of this, creating online scam websites and faking elements of their visual appearance to make those appear legitimate: fake URLs and fake security symbols (e.g. browser padlocks and trust seals) are often added to scam websites to deceive their targets (Kirlappos and Sasse, 2012). Unsuspected users often assume they are dealing with a reputable retailer. This comes to no surprise, as security experts and public awareness campaigns often tell the public that the presence of those indicators signals trustworthiness (Sheng et al., 2007). As a result users often engage in transactions with those websites, suffering financial losses or identity theft.

2.4.2.6 Need and Greed

Greed makes people vulnerable and attackers take advantage of this. Websites advertising luxury products at significantly reduced prices lead to people letting their defences go and dismissing initial suspicions, in order to seize “unmissable” deals. Attackers then steal victims’ card details or money, often shipping nothing at all (Winch, 2014) or providing them with counterfeit goods (Melik, 2011).

2.4.2.7 Time

People’s decision strategies change significantly when they are (or believe they are) under time pressure. Reasoning about secondary issues like security becomes less important, as their focus is on completing the required task as quickly as possible. This leads to people often ignoring security advice, and behaving insecurely (Herley, 2014). Time constraints also play a crucial role in security behaviour in organisations, where employees may choose to ignore security policies, when tight timeframes force them to decide between completing their productivity-related tasks or adhering to security rules (further extensive discussion on organisational security behaviours follows later in this chapter).

2.4.2.8 Propensity to do good

The first behavioural vulnerability missed by Stajano and Wilson is human propensity to do good. People are by nature willing to help a fellow human who appears to be in trouble. This can also act as a driver for successful social engineering, in addition to unwillingness to question authority. Winkler (1997) for example, explains how he used public information obtained from the internet and the telephone register to impersonate company employees and obtain access to sensitive corporate information. Mitnick and Simon (2002) also provide examples of two similar attacks:

1. Attackers gained access to a company's internal computer system that had a password that changed every day. During a snowstorm they called the helpdesk, pretending to be an employee who was snowed-in and wanted to work from home. The operator was happy to share that day's password with them.
2. A person who got a speeding ticket conned the police to reveal a time when the officer who arrested them will be out of town. They then requested a court date coinciding with that time and avoided paying a fine.

What the practices of both Mitnick and Winkler demonstrate is that, instead of breaking into a well-secured system, it is often much easier for an attacker to con users willing to help a fellow human that appears to be in need; they then provide them with information that may have been otherwise potentially unobtainable or expensive to get access to.

2.4.2.9 Human error

In addition to the vulnerabilities defined above, computer users often make mistakes that increase their exposure (or of the systems they are using) to potential attacks. This often compromises the effectiveness of hard to break technical security mechanisms. A classic example of this comes from World War II, when a group of British codebreakers at Bletchley Park took advantage of an Italian operator's error (sending a test message full of the letter L) to decipher the German Enigma machine[5]; an encryption system that was considered unbreakable given the resources of the time (Smith, 2004; Churchhouse, 2002). Seven decades later the problem is still rife: more recently, the UK's serious fraud office accidentally circulated information on a serious closed investigation to unauthorised third parties (Evans, 2013). In both cases, the actions that led to the security failure were unintentional, highlighting the potentially catastrophic impact of human errors in security and the importance of understanding and allowing for potential erroneous behaviours when designing security systems.

[5] "The one snag with Enigma of course is the fact that if you press A, you can get every other letter but A. I picked up this message and — one was so used to looking at things and making instant decisions — I thought: 'Something's gone. What has this chap done. There is not a single L in this message.' My chap had been told to send out a dummy message and he had just had a fag [cigarette] and pressed the last key on the keyboard, the L. So that was the only letter that didn't come out. We had got the biggest crib we ever had, the encipherment was LLLL, right through the message and that gave us the new wiring for the wheel [rotor]. That's the sort of thing we were trained to do. Instinctively look for something that had gone wrong or someone who had done something silly and torn up the rule book." (Smith, 2004)

2.4.2.10 Lack of knowledge and skills

Humans often completely ignore how attackers operate and how they can be potentially targeted. Jannson and von Solms (2013) for example found that many users are unaware about a wide range of phishing attacks, while Stone-Gross et al. (2013) demonstrated how effective fake antivirus software is in extracting large amounts of personal information and large sums of money from unsuspected victims.

2.4.2.11 Reduced cognitive ability

Security that demands excessive cognitive resources from users can lead to them resorting to insecure practices. Adams and Sasse (1999) for example, explain how asking employees to remember an excessive number of different passwords led to writing those down. Böhme and Grossklags (2011) also discuss how over-consuming human attention by security applications reduces overall user ability to behave securely. In the long run, security mechanisms not designed around target user capabilities lead to users becoming habituated to taking meaningless and unnecessary decisions (e.g. dismissing false positive warnings - Dhamija et al., 2006) increasing the likelihood of becoming victims to various types of attacks (Krol et al., 2012).

2.4.2.12 Folk models

Users develop their own understanding of security mechanisms and threats. Wash (2010) examined home user understanding of security, identifying eight *security folk models*: user-devised perceptions and understanding of security (mental models[6]), representing home user understanding of viruses and hackers, together with how they may be targeted by attackers. He then explains how users use those models to justify decisions to ignore expert advice on security, leading to insecure behaviours that increase their risks of being victimised.

2.4.3 The emergence of user-centred security

To design effective security solutions, designers need to combine technical controls with good understanding of human behavioural principles that drive security behaviours. Any secure system is as strong as its weakest component, which is the point of maximal return for an attacker's invested effort (security is an economic problem of return on time and resources invested problem after all – Anderson and Moore, 2006). Whitten and Tygar (1999) have named this the "*weakest link property*"[7]. The human behavioural traits identified in the previous section that lead to successful attacks, leave users as the weakest link of security implementations (Schneier, 2012). When technical mechanisms are sufficient to make attacks expensive and uneconomic, it is more attractive for attackers to focus on the identified

[6] Mental models are descriptions of a user's understanding of a problem and perception of how things work (Johnson-Laird,1980)

[7] Kevin Mitnick also uses the "weakest link term" when referring to humans in an information security context: "The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and its money wasted, because none of these measures address the weakest link in the security chain" (Poulsen 2000)

human vulnerabilities, in order to achieve cost-effective returns for their invested time, effort and resources.

Improved understanding of the importance of well-designed security mechanisms, combined with the realisation that effective management of the human element is important to provide effective security, led to the emergence of user-centred security as an academic research discipline. Researchers started introducing principles from the fields of human-computer interaction, the social sciences and, a few years later, economics, in the design of security measures. This aimed to enable the implementation of systems designed around human cognitive capabilities and behavioural traits to reduce the potential for erroneous behaviours, but also design and implement appropriate safeguards to limit the impact when those happen (Sasse et al., 2001). Today user-centred security is a well-established research discipline, with a number of dedicated workshops, symposia and journals, and its findings are widely acknowledged by security practitioners (e.g. the growing understanding amongst practitioners about the need to replace passwords with less taxing authentication mechanisms – Muncaster, 2015).

2.4.3.1 Principles of user-centred security

Identification of the need for usable security systems predates modern computers, again finding its roots in the design of military encryption mechanisms. In 1883 Dutch linguist and cryptographer Auguste Kerckhoffs presented six principles for effective military cipher design (Kerckhoffs, 1883):

1. The system must be practically, if not mathematically, indecipherable
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will
4. It must be applicable to telegraph communications
5. It must be portable, and should not require several persons to handle or operate
6. Given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules

Principles 3, 5 and 6 suggest Kerckhoffs' understanding of the need for military ciphers to be designed around the needs of their users. In commercial information security, the need for easy to use interface design was first stated many years later by Saltzer and Schroeder (1975): "*It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized.*" Twenty years on, Zurko and Simon (1996) introduced the term user-centred security, referring to security models, mechanisms, systems, and software that have usability as primary motivation or goal[8]. Subsequent research improved understanding of user security behaviours, leading to the realisation that security design cannot afford to ignore human

[8] Usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." (ISO 9241).

behavioural principles. Adams and Sasse (1999) showed that making impossible demands in organisational security policies and implementations leads to users circumventing those e.g. writing down passwords when they had too many and could not recall those from memory. In the same year, Whitten and Tygar (1999) demonstrated that bad mechanism design makes secure behaviour impossible, by showing the impact of bad usability of PGP email encryption tools on the ability of users to successfully encrypt a message. All the above demonstrate the need for security design to better accommodate for capabilities and priorities of target users in order to deliver effective protection.

The first attempt to formalise a set of principles of user-centred security design is presented by Pfleeger and Sasse (2015), who explain that in the context of enabling confidentiality, integrity and availability, usable security should aim to:

1. Keep a user aware of the security status of data, machines and networks.
2. Make visible the security implications of a user's action or choices.
3. Enable the user to understand related risks and externalities.
4. Prevent the user from doing harm.
5. Prevent (as much as possible) security from interfering with a user's primary activities, as availability is a key requirement for any secure system.

Of course, none of the above principles should damage the security implementation's ability to deliver effective risk mitigation. User-centred security aims to work within human capabilities to design security systems that are fit for protecting sensitive information, also imposing minimal impact on users' primary tasks.

2.4.3.2 Problems with application of user-centred security

Two decades after identifying the need for user-centred security, progress in delivering effective security design principles is still limited. As Cranor and Garfinkel (2005) put it ten years ago: "*While there is much agreement among security practitioners that we need to find ways of designing secure systems that people can use, there is less agreement about how to reach this goal.*" Unfortunately, today we are still seeing minimal application of user-centred security principles in security design. A number of reasons for this have been identified, discussed below.

2.4.3.2.1 Lack of appreciation for usability by security designers

Sasse et al. (2014) explain how current security mechanisms are developed and implemented without usability principles being taken into account. Security experts generally fail to consider user effort (Herley, 2014), also failing to design around the principle that security is a supporting task (Sasse and Fléchais, 2005). Current authentication mechanisms for example, fail to accommodate for user primary task focus, thus end up imposing excessive workload on users. Security mechanisms then become an obstacle between the user and primary task completion, often demanding disproportionate time or effort. Brostoff and Sasse (2000) for example, found that users were not willing to spend one minute authenticating if they were planning to only spend a short time on a system.

2.4.3.2.2 Failure to consider context of interaction

Security designers also fail to consider that different primary tasks or physical and social contexts may require different security mechanisms (Pfleeger and Caputo, 2012). Today's password rules for example, often require complex passwords, with varying length and upper/lowercase requirements. Entering a long complex password on a mobile device with a touchscreen while on the move, possibly also having strangers around, requires more effort from the user and carries higher risks than working on a desktop computer at home or in a well-secured corporate environment (Schaub et al., 2012).

2.4.3.2.3 Attempt to fix the human instead of the systems

Herley (2014) explains that there is a reluctance amongst security designers to admit that some existing approaches are ineffective and require improvements. Instead, they insist on asking for more and more user time and effort, ignoring potential optimisations in existing mechanisms and processes that could either reduce user effort or improve security. Examining past research on user-centred security, a significant proportion of the work presented in academic literature has focused on encouraging secure behaviour by "fixing the human" – e.g. improve user ability to detect phishing sites (Kumaraguru et al. 2009; Sheng et al. 2007), improve security warnings to enable users taking more secure decisions (Egelman and Schechter, 2013; Schechter et al., 2007), or deploy public awareness campaigns giving users instructions on how to protect themselves and their machines (e.g. US-CERT, 2015). But, as Herley puts it, in many cases security designers and professionals insist on things they know users will not or cannot do. Security warnings for example have been proven to be ineffective, but they are still used extensively (Krol et al., 2012); essentially their only achievement is liability transfer for potential compromises to the user that has already been habituated to dismissing those. Passwords are also putting excessive cognitive load on users, but users are still told they need to be long, complex, unique and not written down (Adams and Sasse, 1999; Inglesant and Sasse, 2010). Again such advice only transfers responsibility for securing a system away from its designers and on the shoulders of its users, for whom security is a secondary consideration (Pfleeger and Sasse, 2015), and their understanding of it may be erroneous and inadequate (Wash, 2010). In the end, such attempts only aim to achieve security by increasing the workload it creates for the end user (Herley, 2009), ignoring the need to better accommodate for user priorities when designing security systems (e.g. Adams and Sasse, 1999). This attempt to intervene on the human rather than the systems in place increases the burden on the shoulders of end users, encouraging further dismissal of communicated security principles, thus failing to deliver effective security.

2.4.3.2.4 Usability is still treated as an expensive afterthought

Other parts of usable security research focused more on explaining the need for user behaviour principles to be included in the design of security systems (Camp, 2009; Faily and Fléchais, 2010; Kirlappos and Sasse, 2012) and the need to integrate usability and security in requirements design (Flechais et al., 2007). Despite this, security products often suffer from limited budgets and time pressure, pushing usability at the bottom of the priority list for security requirements design and implementation (Flechais et al., 2007). This leads to attempts to retro-fit usability in an almost final product, an approach which usually fails to create usable security solutions.

2.5 Organisations and the need for information security

Organisations worldwide have widely adopted technology in their production tasks. The use of technology in organisational processes provided, amongst others, improved efficiency in production lines, improved ability to manage large information databases, faster communication, easier and faster information exchange and dissemination, new marketing platforms, access to large international markets, and improved customer services (Palmer et al., 2001). In addition the worldwide spread of the Internet as a productivity and marketing medium led to the emergence of new technology-based business models, with corporate success often being interlinked with an organisation's online presence (Chen and Yen, 2004). The above advantages, combined with ever-decreasing technology costs (Moore, 1998), led to wide technology adoption by the majority of modern organisations aiming for success in today's highly competitive environment.

The benefits of technology for organisations do not come without problems though: the task of securing organisational information systems becomes increasingly complex and challenging as technology becomes an integral part of modern production lines, with information handling also getting more and more decentralised. The old *dumb terminals* and *time-sharing systems* of the 70s (Auerbach, 1974), where information was stored in centralised systems with only accessed by authorised users through networks, are now obsolete. Modern stand-alone PCs, usually come with vast amounts of local storage, giving an organisation's employees significantly more control and responsibility over the data they use. Employees can now keep local copies of documents, take those at home to work, share information amongst them electronically and use the information they have access to maliciously if they want to. The increasing adoption of modern mobile devices like smartphones, tablets and laptops in corporate environments complicates attempts to secure information even further: employees access corporate information while on the move, from devices also used for personal purposes, through third-party networks over which an organisation has no control. All these advancements make correct implementation of information security mechanisms complex, but significant for the vitality of every organisation that has introduced technology in its working processes (military, government and commercial). The remainder of this section discusses (1) major security-related threats modern organisations currently face, (2) how information security management evolved from a purely technical challenge in its early days to a corporate governance issue in modern organisations, and analyses (3) current challenges security managers face when attempting to deliver effective protection for an organisation.

2.5.1 Modern security landscape and threats

Increased dependency on technology means that security compromises can have potentially catastrophic consequences for an organisation, leading to a wide range of damages:

- *Operational ability damage*: Attacks like Denial of Service (DoS) can render organisational systems inoperable for significant time periods. This negatively impacts an organisation's ability to carry out its operations, produce and sell its products, communicate with customers or deliver services to them (McDowell, 2009). Customers are often left unable to access desired services, which then negatively affects an organisation's revenues, also damaging customer

satisfaction, as customers expect organisational systems to be both secure and continuously available (Johnson and Goetz, 2007).

- *Intellectual Property theft*: Intellectual property (e.g. research and development manuscripts and upcoming product designs) is one of the key targets of modern attacks (Winkler, 1997). Consequently, protection of corporate information is a major organisational concern in order to secure corporate secrets and product designs that may be of high value to competitors. Successful attacks by malicious insiders, corporate espionage and malicious software (designed to relay data from corporate machines to remote machines controlled by attackers) can result in information theft, reducing potential competitive advantages, and leading to significant financial losses for an organisation, from which many may struggle to recover (GRT, 2012).
- *Reputation:* Many organisations rely on their reputation as reliable service providers to get returning customers, with those customers also expecting the organisation to protect their personal information. Breaches of information that become publicly known can damage an organisation's reputation. As latest research suggests, people often abandon companies that suffer security breaches (Ponemon Institute, 2014).
- *Legal consequences*: Legislators require protection of sensitive information held by organisations (e.g. UK DPA, 1998), defining potential consequences for organisations that suffer data breaches.

Statistics released by the UK government highlight the seriousness of information security threats modern organisations face (UK Cabinet Office, 2014):

- 81% of large UK-based corporations and 60% of small businesses reported a cyber-breach in 2013.
- On average more than 33,000 malicious emails are blocked at the Gateway to the Government Secure Intranet (GSI) every month. These are likely to contain or link to sophisticated malware. A far greater number of malicious, but less sophisticated emails and spam are also blocked each month.
- The cost for the worst cyber-security breach estimated between £600,000 to £1.15 million for large businesses and £65,000 to £115,000 for smaller ones.

The seriousness and variety of the problems suggested by the above statistics, together with their potentially catastrophic consequences, demonstrate the importance of achieving the CIA security triplet for any modern organisation:

- *Confidentiality* is required to protect intellectual property, customer data and classified information that may damage the organisation's viability.
- *Integrity* to ensure employees work with accurate, unmodified data.
- *Availability* to provide uninterrupted and flawless access to systems and information both for employees required to carry out organisational processes and customers who want to use company services.

2.5.2 Evolution of security management

The role of information security management in an organisation is to deliver all the information security activities described in section 2.1 (*Identify threats*, *Assess vulnerability and exposure*, *Define security goals* and *Implement appropriate controls*). The ever-changing nature of organisational technology mechanisms, leads to changing threats, with information security management having to adapt accordingly. As a result, organisational information security practices have evolved significantly from the early days of mainframe-based computing. Back then, security was a concern limited to small teams of technically-minded employees, responsible to keep the organisation safe. This usually involved minimal management involvement and minimal visibility to end users. In contrast, nowadays information security is a significant concern for all employees in an organisation, has a substantial management aspect and is a key part of modern corporate governance. This evolution of security from a technical to a governance concern, is well captured by von Solms's (2006) taxonomy of the four different eras (waves) of information security management (Figure 1):

1. *Technical wave*: In the early years of mainframe-based computing, implementing strong technical solutions was assumed as adequate for effective protection. Security implementations included measures like access control lists, together with creation of different user IDs and passwords, while the importance of user awareness and security policies was still unknown. As a result, security was solely a concern for a small community of technical experts who designed, implemented and managed the deployed technical protection mechanisms.
2. *Management wave*: A few years later, technical experts and top organisational managers realised the need for security management processes, in order to coordinate protection efforts and resource allocation. Security managers were now appointed, provided with authorisation and resources to deliver the desired protection, and reported to organisational management on their deployment progress and effectiveness. This wave led to the creation and wide adoption of security policies, together with security communication and training in order to improve employee motivation and ability to act as required to keep the organisation secure.
3. *Institutionalisation wave*: The need for organisations to compare their protection against each other and share knowledge and experiences in order to improve their security approaches, led to increased standardisation and certification: international standards and best practice guidelines for security management were created, based on collective experience, together with metrics and benchmarking tools to allow for security implementation effectiveness assessments.
4. *Corporate governance and information security:* It is now widely accepted that security in organisations should be a top management concern due to its importance for the organisation's operational ability and viability. This made information security an integral part of corporate governance, with security risk management standards being created (e.g. ISO27005), while security procedures and existence of adequate security controls became part of compulsory requirements for public companies (e.g. the Sarbanes-Oxley Act, 2002) defining strict requirements on the need to protect information held by an organisation.

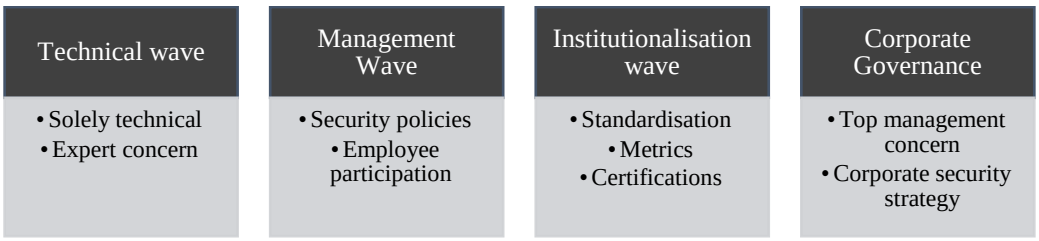

Figure 1: Von Solms waves of information security management

Modern attempts to deliver organisational information security, require the deployment of various meta-measures that combine elements of more than one of von Solms' waves. Examining the different types of controls deployed in organisations, together with corresponding economic costs of deployment and enforcement, Pallas (2009) created three controls (or *meta-measures*) categories, with different costs related to each one:

1. *Architectural means*: Physical and technical measures implemented to ensure employees are behaving in accordance with security rules. They are strict, governed by well-defined rules, and can only protect an organisation from already identified risks. They provide no ability to adapt to exceptional situations unforeseen during their setup, thus are mostly aiming to provide prevention rather than detection (e.g. blocking specific types of traffic from corporate firewalls) and often come with high fixed-costs to implement.
2. *Formal rules*: Security measures not focused on technology, but on accurately defining obligatory, allowed and forbidden activities (e.g. by defining those in a security policy). They are well-defined, thus inflexible in taking changing conditions into account (although not as rigid as architectural means). They follow an ex-post enforcement approach, as forbidden activities are not prevented, but punished after they have happened. As a result, they come with high marginal costs for monitoring and enforcement.
3. *Informal rules*. Norm-like factors influencing individual behaviours, with "good behaviour" principles being defined in a social rather than a formal organisational manner. They are less strict than formal rules, not defined in writing and often emerge in a bottom-up direction (but sometimes influenced in a top-down manner). This makes those difficult to influence, as change can only happen slowly and indirectly. As they do not define acceptable and non-acceptable behaviours, they make it easier to respond to unanticipated events. Enforcement is formalised through social control in an ex-post manner, thus it is more complex to control than architectural means or formal rules. In addition, enforcement lies significantly with the community members (e.g. an organisation's employees to whom the informal rule violation is visible), thus reducing enforcement costs for centralised security management.

Effective combination of the three different types of meta-measures is required to deliver effective protection. Unfortunately, as discussed later in this chapter (see section 2.6), current security approaches fail to achieve a working balance between the three.

2.5.3 Combining the four waves

All four of von Solms waves play a significant part in modern information security management. None of the four can deliver effective security in isolation, with clear distinction between those in modern security approaches being almost impossible. Each organisation identifies their own risks through appropriate risk analysis techniques and mitigates those depending on its risk appetite, combining all four waves to deliver the desired risk mitigation (Anderson and Choobineh, 2008; Stoneburner et al., 2002). The emerging security solutions are usually based on five different security management elements, each of which requires a combination of von Solms's four waves (Table 2): (1) technical defences, (2) adoption of information security standards, (3) information security policies, (4) policy communication and employee education, and (5) assurance mechanisms to ensure policy compliance.

Elements of security management	**Purpose**	**Von Solms' waves used**
Technical defences	Protect organisational systems from outside attacks, enable accountability	Technical, Management
Information security standards	Aid knowledge exchange, best practice adoption, better policy/mechanisms deployment	Management, Institutionalisation, Corporate governance
Information security policies	Define desired employee behaviours	Policies, Institutionalisation and Corporate governance
Policy communication and employee education	Provide employees with skills required to enact principles presented in policy	Policies, Corporate governance
Assurance mechanisms to ensure policy compliance	Detect potential misuse of systems and policy violation (either accidental or wilful)	Technical, Policies, Institutionalisation, Corporate governance

Table 2: Elements of modern organisational information security implementations

2.5.3.1 Technical defences

Technical protection is the first level of organisational security defence, but also requires effective management to deliver the desired protection. Firewalls and intrusion prevention systems are used to filter unauthorised traffic, encryption is deployed to protect hard drives and communication channels, access control aims to limit access to information on a "need-to-know basis", and different types of information logging systems are used to allow for accountability of user actions. In large organisations though, often spanning various geographical locations, the complexity that comes with the implementation of technical mechanisms needs to be well managed in order to provide functional security: different mechanisms are often managed by different teams, with different areas of expertise, also positioned in various locations around the world. Additional challenges also arise from the need to deliver the strongest protection possible, constrained by budget allocations. This makes effective security management an essential part of the design and deployment of technical security mechanisms, to deliver the best possible risk mitigation.

2.5.3.2 Information security standardisation

Information security standards are today highly adopted by organisations in order to improve their security deployment and management approaches. They are frameworks aiming to provide management direction and support for information security decisions and deployment, in agreement with business requirements and relevant laws and regulations. They are usually based on industry-wide accepted rules and principles, (e.g. COBIT - ISACA, 2014; ISO 27000 series and ITIL) or, in other cases, they are required by government or other entities for an organisation to be granted a license to operate in specific

domains (e.g. PCI-DSS for card payments or PSN for public service networks in the UK). The use of standards allows organisations to develop and manage their security implementations based on common industry knowledge and experience, which is often much broader than the knowledge obtained by operating within their own organisational boundaries (BSI Group, 2014). Today the use of standards is at the forefront of any security implementation, with dedicated bodies overseeing and auditing their application and management in organisations.

2.5.3.3 Information security policies

An information security policy is a set of principles an organisation's security management considers critical for its employees to adhere to. Their formulation is based on past organisational security experience, identified security risks, industry-wide good practice guidelines, international standards and potential regulatory requirements. Policies are the foundation of any security regime, thus their existence is crucial for organisations: without those, security practices are developed without clear understanding of objectives and responsibilities (Fulford and Doherty, 2003; Hagen et al., 2013; Higgins, 1999), which can undermine the effectiveness of technical security solution deployment. They usually materialise as documents or webpages on corporate intranets and define the security objectives of the organisation, the responsibilities of employees and desired employee behaviours to reduce organisational security risk exposure.

2.5.3.4 Security communication and education

Communication of desired employee behaviours defined in security policies is done through security awareness, education and training (SAET). This consists of information periodically sent out to employees defining their responsibilities and desired security behaviours, and security modules in internal e-learning modules (also widely referred to as CBTs – computer-based training). Through SAET organisations aim to increase employee awareness of information security risks, expecting this to motivate them to comply with security processes (Thomson and von Solms, 1997). The significant risks that can emerge from erroneous employee behaviours (section 2.1.2) make effective SAET essential for the success of any organisational information security implementation (Höne and Eloff, 2002).

2.5.3.5 Assurance mechanisms to ensure policy compliance

Security policies and technical defences are often complemented by additional assurance mechanisms. Those aim to reduce organisational exposure to security risks by limiting and monitoring employee behaviour, prohibiting malicious or careless actions, or attempting to minimise their impact after they happen. They are usually complemented by additional mechanisms to detect non-compliance with security policies, with potential sanctions defined for identified offenders. Data loss prevention (DLP) software for example, is used to monitor data storage and sharing to prevent potential security incidents (Symantec, 2014), encrypted USBs aim to prevent data leakages, while firewalls and port-blocking software aim to prevent malicious software from infecting corporate machines or unauthorised access to information or systems. Assurance mechanisms are today deployed in the majority of modern organisations and many security companies offer those as part of information security management solutions.

2.5.4 The need for productive balance

The complexity of managing security stems from the need to effectively and efficiently combine all five elements of security management presented in the previous section into a security implementation that delivers sufficient protection for the organisation, while minimally impacting organisational productivity. Effective security management needs to fortify the organisation's technical systems (both hardware and software) against potential attacks, but should also aim to reflect the priorities and social constraints of the corporate environment in which security processes and mechanisms are used (Karyda et al., 2005; Sasse et al., 2001). Security may have risen to the corporate governance level, but if the technical implementation is ineffective or inefficient, then no protection can be delivered, or even if it does, the resulting overheads will prevent the organisation proceeding with its day-to-day operations.

2.6 Insecure behaviour drivers

In order to deliver effective security that is also aligned with employee priorities, security management needs to understand the drivers of insecure employee behaviours in modern organisations. With technical protection constantly improving, attackers increasingly target vulnerabilities created by the human element in an organisational security implementation: examining a number of attacks, IBM's Computer Security Incident Response team identified human error as a contributing factor to the occurrence of over 95% of identified security incidents (IBM, 2014). This highlights the inability of current information security approaches to correctly manage the human element of security implementations, also suggesting the need to radically rethink current information security management practices to better reflect challenges employees face in their work environment.

Despite wide industry adoption of the security measures outlined in the section 2.5.3, research suggests that employee behaviours that significantly deviate from organisational security policies are still widely prevalent within modern organisations (Beautement et al., 2008; Blythe et al., 2014; Herath and Rao, 2009a; Pahnila et al., 2007). User-centred security research identified the root of that problem to be the failure of security managers to accommodate for employee priorities (primary task focus) and understanding (security risk perceptions) in the design and deployment of security implementations. This leads to badly-implemented security mechanisms that negatively affect employee ability to focus on their primary tasks, creating friction[9] between security and employee productive activities. As a result, in order to maintain productivity, employees' inevitably choose not to follow the policy. The remainder of this chapter discusses past research on information security compliance, explaining why current security approaches fail. It then identifies a number of problems in past research attempts to create effective user-centred information security, and presents the justification for further research in order to devise new approaches to manage employee information security behaviours.

[9] Friction refers to conditions where the presence of security creates problems for completion or primary task-related activities

2.6.1 Failure to capture employee priorities

A major factor that creates security-productivity friction in current security management approaches is the failure to accommodate for employee priorities when designing or attempting to improve organisational security systems. This leads to highly inconsistent security behaviours across different organisational divisions, better understood by categorising employees in three different groups based on their role in the organisation (adapted from Gurbaxani, 2010):

- *Top Management*: The part of the organisation setting business goals and deciding on the strategies required to meet those. For them information security is something they often authorise funding for, expecting it to keep the organisation risk free, thus able to flawlessly continue with its day to day productivity operations. They may asked to be briefed on the current security achievements or challenges by security management, but do not participate in security deployments.
- *Business operations/functional areas*: This group includes the majority of employees in the organisation who work towards achieving organisational goals. Employees in this category act both for the organisational interest, but also their own: completion of the desired tasks within specific timeframes benefits both the organisation and themselves, as this is what their performance assessment is based on. Information security is something they often know they should participate in, but they do not always understand related risks or what the correct actions they need to take are.
- *Information Security Management*: Their goal is to implement the controls required to reduce security risks, allowing operations to proceed smoothly towards primary task completion. Their day-to-day tasks involve implementation and correct operation of all company information security-related activities presented in section 2.5.3.

The varying priorities of different organisational functions lead to the development of value differences between them. The tensions emerging from those value differences are captured by the economic paradigm of the "*Principal-Agent problem*". This occurs when a principal hires an agent to pursue their interests, but the agent aims to maximise their own benefit, which results in conflicting targets between them (Gurbaxani and Kemerer, 1999; Holmstrom, 1989). In an information security implementation, the higher the goal asymmetry between different organisational parts, the more severe the Principal-Agent division is: organisational management may care about both productivity and security, but employee performance is judged based solely on productivity targets met. Mintzberg (1985) captures the emerging *value conflicts* by describing an organisation as a political arena where different conflict situations exist: everyone pursues their own interests, based on their own understanding and priorities. This leads to the development of three distinct "conflict zones" when attempting to implement solutions to mitigate information security risks (Figure 2):

- *Top Management – Information Security Management*: Management wants to keep the organisation risk-free but does not want this to severely impact the organisation's ability to complete its production-related tasks. As a result, restrictions in information or system access implemented by information security managers, may be blocked by top management if their

impact on organisational productivity is considered prohibitive. In addition, requests for budgets to implement new security mechanisms or improve existing ones may be rejected by top management, who may prefer to invest in other organisational divisions outside security. This ends up leaving information security managers feeling unable to implement all the measures they believe are required to deliver effective security.

- *Information Security Management – Functional Areas*: Information Security Management wants employees to comply with controls implemented to reduce the organisation's exposure to information security risks. But when those controls create significant security workload for employees they negatively affect their ability to proceed with primary task completion. User refusal to comply with security then leads to security managers considering them a vulnerability point (Kraemer et al., 2009). This leads to further restrictions, deepening the gap and creating further tensions between these two sides (Inglesant and Sasse, 2011).
- *Top Management – Functional Areas*: Employees in functional areas are under pressure by the organisation to produce required productivity deliverables on time. As a result, anything that hinders their primary task activities (in this case security measures that slow them down), may be ignored to stay on track with their productivity and keep the top management satisfied.

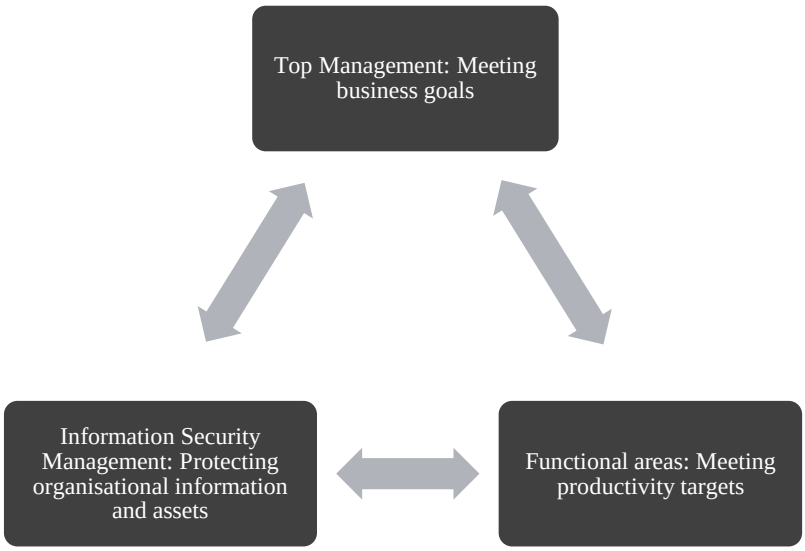

Figure 2: The Principal-Agent conflicts in organisations

The identified value conflicts increase the costs of implementing effective security (Pallas, 2009): both the cost of architectural means to deliver effective security and the motivation costs required to effectively influence employee behaviour increase with high value misalignment. In addition, varying priorities lead to employees exhibiting very different behaviours, even under the same conditions and having received the same level of knowledge or training (Hedström et al., 2011). Any subsequent attempts to change security behaviour through increasing controls increase the identified tensions, creating a number of practical problems in security implementations: (1) policy formulation becomes difficult, (2) assurance becomes ineffective and (3) effectiveness of risk communication is reduced.

2.6.1.1 Policy formulation problems

Currently security policies often fail to allow for employee productivity focus, which often leads to failure to reduce information security risks (Saunders, 2012; Wood, 2000). Wood attributes a large part of this failure to the fact that current security policy formulation is still based on a militaristic approach: policies define the rules to which security management *believes* employees should abide to, usually adding elements required to comply with legislation and security standards the organisation needs to comply with. This results in a *command-and-control* based security implementation that fails to capture the dynamics of modern organisational environments: modern workers are independent and quite capable of making local decisions (Wood, 2000), a trait encouraged by organisations, as it improves productivity and adaptability to new primary task-related challenges. Blind obedience to information security policies contradicts this behaviour: expecting employees to follow a set of rules they do not understand and do not perceive as beneficial is unrealistic. This lack of alignment of security policies with employee primary tasks, is accentuated by the fact that security rules and policies only rarely get evaluated for fitness for purpose (Björck, 2001) and no input from employees is incorporated in their creation process (Bartsch and Sasse, 2012).

The second problem with current policy formulation approaches is their over-reliance on information security standards (Pallas, 2009). Despite allowing easy and quicker policy creation, research has shown that information security standards are currently ineffective (Baskerville and Siponen, 2013; Siponen and Willison, 2009; Siponen, 2006). They are developed based on generic and universal principles, without paying adequate attention to organisational differences and how other factors (like environment-specific contextual elements) affect the practical deployment of information security in an organisational environment (Lacey, 2011). In addition, the ever-increasing number of regulatory frameworks that organisations need to comply with, leads to vast amounts of resources being consumed to achieve compliance. This leaves little time for fine-tuning security policy design and formulation to address organisation-specific security risks (Anderson and Choobineh, 2008). As a result, the emerging security implementation often misses organisation-specific threats, and the lack of additional resources negatively impacts the potential to deploy novel, more context-appropriate security for an organisation.

Another problem with current policy formulation approaches is that they are mostly reactive, driven by past failures and lessons learned from those, either internal to the organisation or based on breaches other organisations suffer. Emerging security mechanisms primarily focus on protecting an organisation from threats closely resembling current or past ones, essentially leaving the organisation unable to adapt to new, changing threats that are very common in the fast-changing modern information security landscape (Dourish and Redmiles, 2002).

2.6.1.2 Problems with excessive assurance

Unable to recognise the failure of current policy formulation approaches, information security management attributes non-compliance to user ignorance and wilful disobedience. As a response to this "user laziness" (Adams and Sasse, 1999), various architectural assurance mechanisms are put in place, to limit employee behaviour within desired domains (e.g. access control restrictions, anti-virus software, data loss prevention systems). When control is impossible (e.g. employees handling confidential documents as part of their tasks), monitoring and sanctions are introduced to deter misbehaviour (Fléchais

et al., 2005); employees violating policies are threatened with potential reprimands that can be as serious as losing their job and legal action taken against them.

In theory, implementing extensive security controls and sanctions should prevent both intentional insider breaches and reduce the impact of erroneous behaviours that increase organisational security exposure. In practice, and despite their wide popularity amongst information security professionals, assurance mechanisms have been shown to suffer from a number of drawbacks, negatively affecting security effectiveness:

1. *High cost*: Strict assurance controls that aim to exhaustively eliminate all information security risks come at prohibitive costs (Handy, 1999) and can drain organisational resources, including employee time and effort required to comply with those (Beautement, Sasse, and Wonham 2008; Herley, 2009). In addition, human-related security risks cannot always be defined well and are constantly changing, depending on factors both internal and external to the organisation. Any attempt to exhaustively eliminate those risks, requires implementation of a wide range of architectural means to identify and eliminate all potential vulnerabilities. For any budget-sensitive organisation this is prohibitively expensive and can lead to security implementers having to compromise with suboptimal solutions (Björck, 2001; Pallas, 2009).
2. *Flexibility reduction*: Strict controls take away employee flexibility to respond to changing environments, reducing their ability to respond to non-predictable situations (Vroom and von Solms, 2004). When employees engage with tasks where flexibility is required (e.g. remote or home working), control becomes time-wasting, inefficient or even impossible to implement. As a result, in order to maintain this flexibility, organisations end up relaxing security policies, weakening their security implementation (Flechais et al., 2005). In addition, excessive controls reduce the capability of employees to take any initiative to aid the organisation in managing its security challenges.
3. *Ignore the role of trust in achieving security*: Strict assurance mechanisms tend to underplay the importance of trust in employees as part of effectively and efficiently managing information security (Williams, 2008). Attempts to eliminate the need for trusting any employee also contribute to the creation of a negative attitude towards security ("*resistance to information security policy implementation*" – Lapke and Dhillon, 2008), which also hinders the creation of a collaborative security culture within the organisation (Inglesant and Sasse, 2011): employees feel less trusted, their motivation to behave securely decreases, and are less willing to report any problems regarding information security issues.
4. *Dissatisfied employees*: Excessive assurance and sanctions can also lead to employee dissatisfaction, deepening the value gap between security enforcers and other employees (Albrechtsen and Hovden, 2009). This hinders the development of social capital and shared values, leading to minimal incentives for secure behaviour, and increased probability of insider attacks (see section 2.6.2, Moore et al., 2011). It also negatively affects an organisation's ability to retain its valuable employees, as dissatisfaction can lead to them eventually leaving the organisation (Ken Blanchard, 2010).
5. *Security perceived as hindrance*: Excessive monitoring and sanctions accentuate employee perception that security is a hindrance for organisational productivity (Vroom and von Solms,

2004). Despite a small improvement in compliance when probability of detection is high (Herath and Rao, 2009a), assurance costs a lot (Pallas, 2009), provides no guarantees for long-term compliance and does not contribute to the creation of a compliant security culture amongst employees.

In general, excessive assurance negatively affects employee behaviour: it creates conditions where employees are less willing to follow information security policies and has no long-term effect on security compliance for risk-aware employees.

2.6.1.3 Risk communication and education problems

Security risk communication (or user education) is also used to encourage employee compliance with security policies. Current approaches though, fail to effectively influence employee behaviours, for a number of reasons:

- Problems with employee behaviour are attributed to a lack of facts available to them, ignoring potential problems in the usability of security mechanisms in place (*stupid, lazy, ignorant users* – Adams and Sasse, 1999). Security experts seem to overlook primary task focus as the key driver of employee decision making, thus creating SAET programs that fail to accommodate for it: they just tell people what they *think* they *ought* to know (Stewart and Lacey, 2013). This technocratic view of risk communication has been strongly criticised by experts in the field of safety risk communication as ineffective and inefficient: it completely overlooks employees' own understanding of the systems in place and role-specific risks arising as part of their primary-task related activities (Morgan, 2002).
- Sometimes information security communication presents demands that security management knows are impossible to adhere to; they either ask for too much (e.g. no password writing down) or they mostly focus on worst-case scenarios instead of risks employees have to deal with in their daily activities (Herley, 2014). When end-users realise the lack of connection between communicated principles and employee day-to-day tasks, the credibility of that advice is damaged, further accentuating user alienation from security.

The above problems result in SAET approaches that simply flood employees with generic information, of which only a small percentage is related to information security risks they encounter while working towards their primary task completion. As a result much of that information goes unnoticed and the limited employee resources available for security are quickly exhausted on attempts to understand communicated information unrelated to their role (Beautement et al., 2008).

2.6.2 Non-compliance as an economic decision – focusing on the primary task

In their normal day-to-day operations, organisations and their personnel are primarily concerned with producing required productivity deliverables – the primary task. Employees have limited available resources and they can either spend those complying with security or proceeding with their primary tasks (Ashenden 2008; Sasse et al., 2001). As a result when security poses unrealistic time and effort demands, they may choose to ignore it. An example comes from Adams and Sasse (1999), who identified that having a large number of systems to which the users are required to authenticate to, also requiring long

passwords and frequent password changes, results in overloading employees with unmanageable password management responsibilities: it becomes impossible to recall their passwords from memory, and changing those frequently also imposes high effort overheads to them. As Beautement et al. (2008) explain, the available resources for compliance are both *cumulative* and *limited* – what they call the "*Compliance Budget*": employees need to invest time and effort to comply with security and are only willing to bare a limited cost for compliance. This cost may be further reduced when they are under pressure to deliver within tight timeframes (e.g. circumventing a corporate website filtering system using a personal machine, when they need urgent access to information). Weirich (2005) classifies the security compliance costs employees have to endure in four different categories:

1. *Primary:* the impact of compliance on their primary task (e.g. slowdown)
2. *Secondary*: potential loss of access to a source or service, blocked for security reasons (e.g. ability to work from home)
3. *Social*: Loss of trust amongst colleagues when refusing non-compliance that can benefit each other (e.g. password sharing)
4. *Image*: Appearing as a paranoid or not a team player when non-compliance can benefit a colleague (e.g. when they request for information they do not have official access to).

When organisations ignore the presence of these costs, the emerging security mechanisms and processes increase the friction between security and the organisation's primary tasks. This quickly exhausts employees' compliance budget, making non-compliance inevitable: it comes as an employee economically rational decision, as a response to friction-inducing security. When security controls become barriers to primary task completion, a conflict between primary task completion and information security compliance emerges (Albrechtsen, 2007), and the perceived (or even actual) risk mitigation benefit employees receive by complying does not appear to be worth the time and effort investment (Karyda et al., 2005, Herley, 2009, Bulgurcu et al., 2010). When security asks for too much, non-compliance is the only mechanism employees possess to satisfy primary task demands.

Employees respond to friction-inducing security by developing coping strategies to overcome its high overhead, re-organising their primary tasks to avoid or minimise their exposure to security mechanisms that are too onerous (Inglesant and Sasse, 2010). Inflexible access control systems for example, which restrict access to information for those who genuinely need it, lead to informal sharing of sensitive information through channels outside official systems (Bartsch and Sasse, 2013). As those channels were not designed for this purpose, and the organisation possesses no control over their security, the exposure of the organisation to potential breaches is now dependent on the level of security provided by the external channels employees resort to. In general, any security implementation that fails to capture and manage the effect of deployed security mechanisms or processes on employee primary tasks, leads to employees ignoring or bypassing those, in order to minimise security-related overheads on their productive abilities.

2.6.3 Discipline is currently impossible and ineffective

Organisational security policies usually warn employees that breaches will be followed up by warnings and sanctions. But given widespread non-compliance due to friction-inducing security, an unmanageably

large number of employees would have to be disciplined under such an approach. In addition, the high volume of false positive alerts from monitoring systems creates noise in attempts to detect non-compliance, making effective monitoring and enforcement impossible (Tuyls, Skoric, and Kevenaar 2007). Subsequent attempts to discipline employees hinder collaboration between different organisational parts and increase tension between security enforcers and the rest of the organisation (Adams and Sasse, 1999). When non-compliance eventually becomes widespread and unsanctioned, sanctions cease to act as an effective deterrent.

Excessive enforcement also runs the risk of compliant behaviours not stemming from correct employee risk understanding, but from increased pressure by the organisation and the fear of potential consequences. This can be ineffective in a discipline like information security, where changes in the threat landscape occur very rapidly; it is impossible to devise and communicate effective desired behaviours whenever a new threat emerges, as this can be expensive for security managers and annoying for users. It is also hard to accurately define rules around desired behaviours or implement mechanisms to detect non-compliance if threats constantly change, as they would require frequent revisions to ensure all potential misbehaviours are effectively captured. In general, wherever flexibility is required (e.g. organisations that need to provide provisions for home and remote working), enforcement of strict security becomes complex and impossible to deliver (Hine 2014): it is inefficient and ineffective for any modern organisation and can even negatively affect an organisation's ability to protect itself.

2.6.4 Risks and vulnerabilities of ineffective behaviour management

Information security attacks targeting the human element can be distinguished between (1) outsiders taking advantage of human behaviours that increase organisational security risk exposure and (2) malicious insiders who abuse their access to cause intentional damage to the organisation or steal information for their personal benefit.

2.6.4.1 Outsiders exploiting employee behaviours

This type of attacks includes situations where attackers take advantage of vulnerabilities created by user behaviours to compromise an organisation. Many of the human behavioural principles exploited by attackers targeting organisations are similar to those presented in section 2.4.2, but their impact on employee behaviours in an organisational environment creates different types of vulnerabilities (Table 3). Exploitation of these vulnerabilities provides attackers with significant opportunities for successful attacks. Laszka et al. (2014) for example, explain how attackers can obtain sensitive information, without even targeting the obvious "highly-knowledgeable" individuals that may be more security-sensitised: they often collect pieces of information perceived as less sensitive from various individuals in various roles in an organisation and then piecing those together to create an accurate representation of the desired content. To reduce related risks, it is crucial for organisations to have access to security design principles that allow designing organisational systems around employee behaviours and priorities, thus minimising potential risks.

Behavioural property	Impact on organisational environment	Vulnerabilities created
Distraction	Employees focused on getting their job done, security creates barriers Tension between security and productivity divisions – rules may need to be relaxed	Relaxing rules without mitigating risks otherwise exposes organisation Disregard for security leads to further insecure behaviours
Social compliance	Employees unwilling to challenge requests from people higher up in the organisational hierarchy	Increases success likelihood of social engineering attacks
Propensity to do good	Employees willing to help colleagues in need May resort to insecure actions in order to do so	
Herd principle	Widespread non-compliance amongst employees reduces propensity to follow policy	Allows attackers to identify loopholes created and take advantage
Dishonesty	Employees unlikely to report potential breach if prior actions that led to it were against policy	Breaches remain unreported and difficult to detect
Deception	Phishing emails manage to pass through organisational firewall (with relaxed rules to reduce distraction)	Loss of organisational credentials Lack of reporting can create long term risks
Need and greed, Time	Time pressure for employees to meet productivity targets Employees rewarded for productivity not security Increased non-compliance when under time pressure	High non-compliance increases potential for attackers to identify it and take advantage
Human error	Employees forgetting to log out or leaving sensitive documents exposed Employees losing devices holding sensitive information	Sensitive organisational information leaked to the public Attackers can get hold of sensitive information through targeted attacks
Lack of knowledge and skills	Ineffective communication leads to reduced risk understanding and mitigating actions	Employees cannot detect, report or act in security-critical conditions
Reduced cognitive ability	Excessive number of security mechanisms and policy clauses creating overload for employees Impossible to comply with all (e.g. do not write down passwords for 20 different systems with password re-use not allowed)	Insecure behaviours widely prevalent Increased potential for successful attacks Disregard for security
Folk models	Employees using own understanding and perceptions to tackle organisational security challenges Widely varying information security behaviours Organisational protection depends on what employees perceive as required security at individual level	Inaccurate employee perceptions and understanding lead to insecure behaviours that expose the organisation

Table 3: Organisational behaviour-driven security vulnerabilities

2.6.4.2 Insider attacks

The second human-related security challenge organisations face is intentional attacks by insiders aiming for personal benefit, often referred to as insider attacks[10]: "*current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data to steal confidential or proprietary information from the organization*" (Moore et al., 2011). As Moore et al. explain, employees may have many reasons to turn against an organisation: IT sabotage, fraud, theft of intellectual property (IP), and national security espionage provide significant monetary or personal incentives for attacks (e.g. hacktivism). With a large amount of the value of modern corporations stemming from intangibles such as trade secrets, the presence of such insider threats poses a serious risk to modern organisations' viability. Recent industry reports on insider attacks indicate they are still a major threat: despite their potentially catastrophic consequences, current organisational security management approaches still do not manage to effectively detect and reduce risks emerging from those (PwC, 2015).

2.6.5 Need to rethink assurance and control

As discussed at the beginning of this chapter, information security aims to protect an organisation from both malicious outsiders and insiders. But treating employees as malicious or unknowledgeable all the time, damages the collaborative nature of an organisation and makes its defences weaker. Non-compliance stems from the fact that almost no modern organisation evaluates whether deployed information security policies and mechanisms are fit-for-purpose for the real working environment in which they are deployed (Adams and Sasse, 1999). The resulting friction between security mechanisms and productivity slows down the organisation's day-to-day productive operations, leading to the creation of a negative attitude towards security. This reduces overall compliance rates, risking rendering any implemented security mechanism as completely ineffective (Lapke and Dhillon, 2008). In order to eliminate the drawbacks of current security design outlined in this section, organisations need to carefully reconsider their information security goals before attempting to design risk mitigation approaches. They need to decide on: (1) what are they trying to protect, (2) how much are they willing to sacrifice to receive that protection, and (3) whose values is information security trying to address? (i.e. is the focus on productivity or being secure for the sake of security).

To reduce the excessive friction created by attempts to enforce badly-designed security in an organisation, it is important to revisit Pallas' (2009) classification of information security meta-measures (section 2.5.2). Currently all architectural means and formal rules implemented are based on scenarios aiming to meet information security managers' priorities, with potential benefits of informal rules being ignored. As a result emerging policies, mechanisms deployed, and policy-driven SAET campaigns have always been based on what managers think their target group (employees) should do and know. There is

[10] The terms insider threats and insider attacks tend to be used interchangeably, often including to vulnerabilities emerging from human actions presented in section 2.6.4.1. For the remainder of this thesis, reference to insider attacks refers to the definition by Moore et al. presented in section 2.6.4.2.

minimal consideration for employee priorities, the impact of deployed measures on those, and no attempts to understand their risk perceptions and their perceived need for security. In addition no consideration appears to exist on the variation of security requirements for employees in various organisational divisions with varying responsibilities that may even require different security implementation and training for different roles (Beautement et al., 2009). There is also limited consideration of the fact that employees may possess internal values that can drive their secure behaviour, like personal connection to the organisation they work for[11] (Bussing, 2002). This leads to limited use of Pallas' informal rules in delivering security and attempts to enforce inflexible "one size fits all" security implementations, heavily reliant on policies and architectural means. The resulting employee alienation and negative perception of security, fails to engage employees in organisational security strategies, thus failing to address the risks emerging from employee behavioural vulnerabilities.

Security approaches need to be redesigned to accommodate for the productivity focus of both the employees and the organisation. Employees should be treated as an asset, not as a liability that could break the system (Kraemer et al., 2009). Security design should acknowledge this and develop an approach for a "middle ground" solution that balances user perceptions and priorities with security experts' priorities (Dourish et al., 2004; Kirlappos and Sasse, 2012; Thomson and von Solms, 2005). In addition, the distributed and decentralised nature of modern IT systems makes the hierarchically-driven information security management approaches described earlier in this chapter inefficient. As Pallas (2009) argues, managing information security in increasingly decentralised organisational environments should be seen as a problem of coordination and motivation.

- *Coordination*: Security management needs to identify optimal state of employee behaviour that represents highest overall value for organisation (e.g. who should be granted access to a service with an organisationally acceptable increase in the emerging risks)
- *Motivation*: Motivation mechanisms need to exist to enforce coordination outcome. Individual members often have various incentives for opportunistic behaviour, so they have to be motivated to behave in the collective interest of the organisation instead. Motivation mechanisms aim to influence employee decisions, encouraging secure behaviours (e.g. through improved visibility of contribution) or discouraging insecure ones (e.g. by ensuring detection and appropriate sanctions)

As Pallas argues, security management can only be effective if it is addressed as a cooperation problem. It should attempt to address the priorities of everyone in an organisation, delivering productivity-focused security controls. This should be done through implementations that effectively balance expensive architectural means, cheaper formal rules and more flexible informal rules to mitigate security risks without creating productivity barriers.

[11] Employee emotional connection to organisations is well documented in organisational research (e.g. Bussing, 2002), but its impact on security has not been examined. This is examined later in this thesis (Chapters 6 and 7)

2.7 Improving compliance though behavioural change: changing the cost-benefit balance

As discussed in section 2.6.2, to achieve an effective balance between security controls and employee productivity, security design needs to understand employee priorities and the economic nature of employee information security decisions. Employees are focused on their primary task: what the organisation has hired them to do and what their performance assessment is based on. As a result, they allocate their available resources to achieve maximal return on their effort and time input. If the costs of security compliance are higher than the perceived benefit, any economically rational actor would choose not to comply, even if that increases organisational risk exposure; security is always a secondary requirement. In addition, as described in section 2.6.1.3, when security advice fails to communicate secure behaviour benefits, compliance incentives are minimal. This section presents past research on how to positively influence employee security decision making and incentivise compliance, focusing on three key areas: (1) understanding the impact of organisational security culture on security compliance and improving it, (2) improving security design elements to make compliance easier, and (3) improving employee motivation to behave securely.

2.7.1 Influencing compliance decisions

Beautement et al. (2008) presented a number of different factors that influence employee security compliance decisions (Figure 3):

1. *Design*: Friction-inducing systems that require significant effort investment from employees, negatively impact their cost-benefit decisions, leading to reduced compliance. On the other hand, a well-designed system that accommodates for employee productivity needs, reduces compliance costs, making compliance an economically attractive option.
2. *Security culture of the organisation*: In organisations where employees value security, perceiving it as an enabler to the organisation's productive operations, the benefit of compliance is higher and the cost-benefit balance is more likely to favour compliance.
3. *Awareness*: Accurate understanding of the information security challenges an organisation faces and employees' individual (or collective) contribution in risk mitigation, improves the perceived benefit of secure behaviour.
4. *Monitoring*: The probability of non-compliance detection can also affect compliance decisions: the more likely employees are to be caught misbehaving the more likely they are to comply (Herath and Rao, 2009b).
5. *Sanctions*: If non-compliance sanctions are seen to be enforced, their avoidance is a perceived benefit for employees that can incentivise compliance.

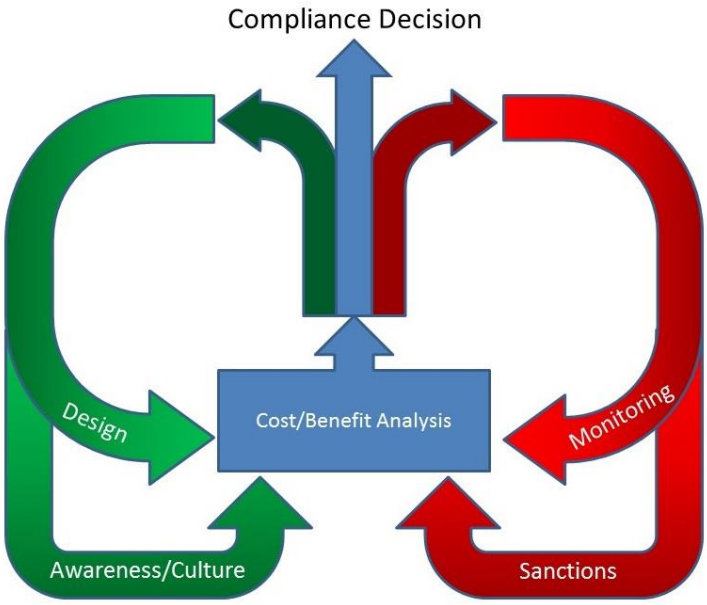

Figure 3: Security Compliance Decision (adapted from Beautement et al., 2008)

As discussed in section 2.6.3, current information security approaches focus more on assurance-based security (monitoring and sanctions), rather than improving the positive elements that could encourage employee compliance. But if employees do not understand why they need to comply (awareness), they are individually and collectively habituated to not doing so (culture), and also the systems in place do not support compliance (bad design: unusable or friction-inducing security mechanisms), then there is minimal benefit for compliance and high benefit from non-compliance (time and effort saved). As a result, attempts to improve security behaviours need to focus on improving the compliance cost/benefit balance.

2.7.2 Improving security implementation design

The problems leading to insecure behaviours presented in section 2.7, and the need to improve security compliance in organisations led to security design rightfully receiving a lot of attention from user-centred security researchers. Well-designed security can reduce security-productivity friction, reduce compliance costs and aid in the development of a positive organisational information security culture. Past research on improving security design focused on two main areas: (1) improving the process of security policy creation and (2) improving the process of security mechanism and process design.

2.7.2.1 Improving information security policy formulation

Current policy formulation needs to be widened to include the priorities of all stakeholder groups presented in section 2.6.1 - *functional areas*, *management* and *information security management* (Checkland and Poulter, 2006; Dhillon and Backhouse, 2001). By doing so the emerging solutions can better accommodate for the needs of primary task-focused employees and improve the alignment of different party incentives in the principal-agent problem discussed in 2.6.1. Drawing parallels from King's definition of *Information Systems Alignment* as "*The degree to which the information systems plan reflects the business plan*" (King, 1978), alignment should also be a key goal for information security implementers: the more a security policy and its implementation accommodate employee priorities and

values, the more it improves incentive alignment in the enforcer-employee principal-agent relationship (Herath and Rao, 2009). This can lead to security strategies and deployments that better reflect productivity priorities, reducing employee resistance to comply with organisational security policies and mechanisms, thus improving security compliance across the organisation (Lapke and Dhillon, 2008; Trompeter and Eloff, 2001; Höne and Eloff, 2002; Fulford and Doherty, 2003).

2.7.2.2 Creation of usable security mechanisms and processes

Security researchers have long argued that complex systems that do not support user activities incentivise insecure behaviours and that secure behaviours can only be achieved by less taxing security solutions. Adams and Sasse (1999) for example, identified that users forced to comply with password mechanisms incompatible with their work practices, responded with coping mechanisms that often included policy violations (e.g. writing passwords down). Such friction-inducing elements of organisational security need to be removed, to avoid exhausting employees' compliance budget (Beautement et al., 2008), also making compliance an economically attractive option. Florêncio and Herley (2010) present a good example of how design plays an important role in security effectiveness and acceptance from users: companies like Amazon and some online banking services demand considerably simpler passwords from their customers compared to government websites, as an easy-to-use customer login process is important for their business models. To prevent security breaches, customers are only asked for additional security information (e.g. use a second form of authentication) when they transfer money to third party accounts or ship orders to new addresses. This creates low security overheads for frequent actions (e.g. buying and shipping to the same address), only burdening users with high-overheads when they carry out infrequent ones (shipping to a new address). Designing organisational security systems around similar principles is important to create security controls and policies that fit the organisation's business processes, imposing low overheads on low-risk employee tasks.

2.7.3 Improving motivation

Research on improving employee motivation to comply with security focused on two key areas: (1) improving user education, and (2) encouraging company leadership to lead by example. Before attempting to do any of the above though, it is important for security management to deliver the improvements outlined in section 2.7.2 to improve security implementation design; removing friction-inducing security mechanisms, should be a prerequisite to attempts to deliver behavioural change (Figure 4, Furnell et al., 2006).

Behavioural change attempts should aim to elevate the value of security for employees by emphasising its importance and its contribution towards the achievement of organisational objectives (James, 1996). As Pawson and Tilley (1997) explain, the effectiveness of any active intervention program that requires target group engagement to succeed, depends on incentivising cooperation from corresponding target groups. After removing (or improving) security mechanisms to reduce security-productivity friction, the organisation should (1) communicate the importance of security through effective security awareness, education and training, and (2) ensure organisational management participates in security protection to "lead by example" and incentivise secure behaviours.

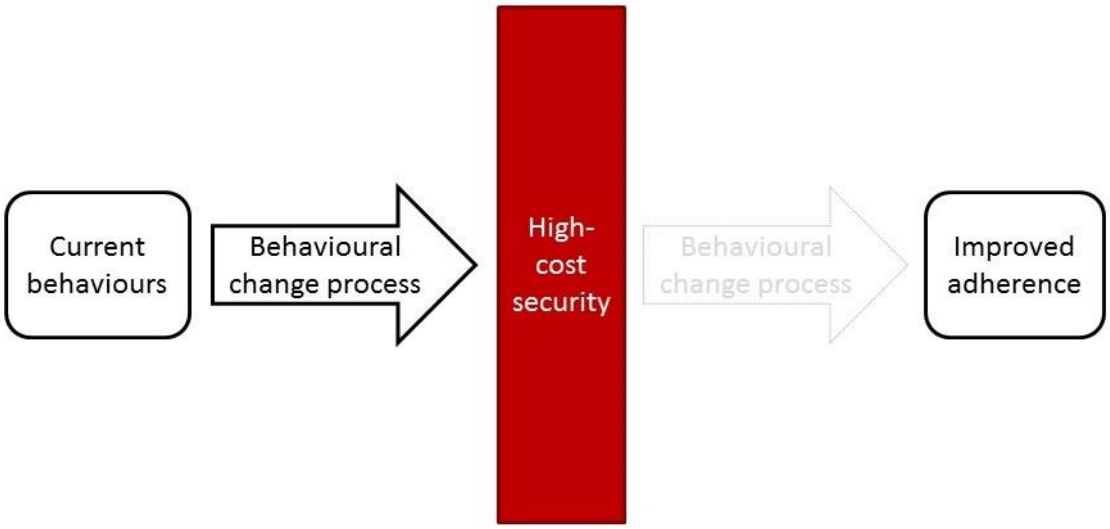

Figure 4: High-cost security as a barrier to behavioural change attempts

2.7.3.1 Security awareness, education and training

To effectively elevate the value of security for employees and management, re-thinking of current security awareness, education and training (SAET) approaches is required. As discussed in section 2.7.1, accurate understanding of organisational information security risks, together with corresponding mitigating actions can motivate employees to behave securely (Hagen, Albrechtsen, and Hovden, 2013; Adams, 1995; Martins and Eloff, 2002). On the other hand, inaccurate understanding of threats and low motivation make compliance a less attractive option, as the perceived benefit (risk avoidance) is much lower than the associated costs of compliance (Adams and Sasse, 1999; Albrechtsen, 2007; Lapke and Dhillon, 2008). The importance of SAET campaigns in changing this is already well understood by organisations but, as discussed in section 2.6.1.3, past approaches failed to deliver effective behavioural change.

As a first step towards effectively redesigning SAET approaches, it is important to understand how secure and insecure behaviours emerge, driven by employee understanding of security risks and awareness of appropriate mitigating actions. Alfawaz et al. (2010) present four different employee knowledge-action states regarding security behaviours:

1. *Not knowing – not doing*: An employee is unaware of the information security rules concerning their role and consequently does not comply with any of those.
2. *Not knowing – doing*: Again an employee is unaware of information security rules but is behaving in a secure way; usually due to organisational norms that influence their behaviour (e.g. culture, mimicking security habits of colleagues). This, once again, underlines the importance of a security-conscious culture and collaboration in delivering effective security. It is not the most desired state though, as employees cannot make secure decisions when faced with rare problems and new challenges that are not part of their (or their colleagues) day-to-day routine.
3. *Knowing – not doing*: Employees know the rules defined in security policy but are not following those, either unconsciously or consciously to reduce the impact of security on their primary task completion abilities.

4. *Knowing – doing*: Employees know the rules defined in the security policy and are following those. This is the desired state that a comprehensive organisational SAET program should aim to achieve.

Unfortunately, existing organisational risk communication campaigns fail to deliver the desired behavioural transition. Sasse et al. (2007) explain that a major driver behind this failure is the inability to distinguish between the different states of behavioural change: *security awareness*, *security education* and *security training*. As they explain, the above terms are often mistakenly used interchangeably. Instead, they should be addressed as 3 distinct steps of a behavioural change process.

1. *Awareness*: Its aim should be to get employees interested in security, attract their attention and help them understand its importance for the organisation and themselves. Once aware they are more likely to respond to security education.
2. *Education*: It should provide information about security threats and vulnerabilities, also presenting employee actions required to protect themselves and the organisation. It should also provide adequate depth of understanding for employees to be able to deal with uncertainty and complexity in security decision-making.
3. *Training*: Awareness and education only prepare the ground for security behavioural change; changing people's behaviour though, requires training. In training, desired behaviours presented in the education stage are thoroughly tested and corrected. Effective training needs to be closely related to clear and well-understood examples from the organisational context, clearly explaining employee security roles within their specific organisational tasks and responsibilities.

Sasse et al. also state that, once the 3 SAET steps have been applied, regular reminders of the key messages are also required. This can reinforce awareness and keep the employees informed on new risks (Weirich, 2005). In addition training material should always be available for employees that need to refer back to it. The information included in SAET material should aim to communicate:

- *The importance of security for everyone*. Security controls play a vital role in mitigating the risks the organisation faces. Re-framing security as a productivity tool can attract the additional attention required by all other parts of the organisation. Employees need to realise that by following recommended security practices they are also contributing to the uninterrupted and efficient operation of business processes; if security collapses, productivity will suffer as well. Employee perception of security needs to be changed from "something that gets in the way of achieving organisational goals" to "something that is important to the organisation achieving its goals". Von Solms and von Solms (2005) suggest that, in an organisational context, information security should be called *business security*, as it secures the prolonged existence of the company.
- *Employee role in protecting the organisation.* Employees should understand that everyone is part of security. Most employees in an organisation have access to some confidential information; thus they all bear some responsibility to keep the organisation safe. Even a single employee's misbehaviour can have catastrophic consequences (e.g. unauthorised disclosure of organisational secrets or dangerous malware entering the organisational network). As a result,

they all need to know what precautions they should be taking to reduce the organisation's exposure to security risks.

2.7.3.2 Active management participation

Security behavioural change cannot be delivered without active management engagement: managers need to participate in security deployments, as security is also a corporate governance issue (von Solms, 2006, section 2.5.3). Organisational managers need to lead security implementation by example: adoption of security by all levels of management leads to increased visibility to everyone in the organisation, positively affecting the organisation's information security culture and encouraging employee compliance with the implemented policies (Da Veiga and Eloff, 2010; Höne and Eloff, 2002; Kritzinger and von Solms, 2005; Van Niekerk, 2007). Unwillingness of organisational management to participate in security can lead to failures of security behavioural change campaigns (Karyda et al., 2005).

Management participation may demand allocation of significant management resources in early stages of behavioural change (mostly in terms of time and effort), but the long term benefits of improved compliance can balance out the initial investment. Management involvement in security can also bridge the value gaps between organisational divisions identified in section 2.6.1: increased adoption by organisational management can lead to information security managers feeling they have management support in performing what is required to protect the organisation, while productivity-focused divisions are more likely to follow their superiors' example and participate in protecting the organisation. The importance of middle management in the adoption of security should also not be overlooked. Managers of smaller teams interact much more frequently with employees in the functional areas; by raising the level of security awareness amongst them and changing their behaviour, it is more likely that employees will follow their managers' behaviour (Johnson and Goetz, 2007). As a result any attempts for security behaviour changes should ensure adequate engagement from all levels of the organisation.

2.7.4 Information security culture and its effect on compliance

As discussed in section 2.7.1, organisational information security culture plays a major role in employee compliance decisions. Information security culture is defined as a set of collective norms and values, developed through employee interaction with information security elements (Da Veiga and Eloff, 2010; Schlienger and Teufel, 2003) or by adjusting their behaviour to match that of their colleagues (Thomson et al., 2006). It is developed at individual, group and higher organisational management level, and is not formalised, but can severely affect employee behaviour and intention to comply with security policies. As a result, many researchers argue that it is equally important to organisational security as technical implementations (Fléchais et al., 2005; Johnson and Goetz, 2007; Karyda et al., 2005; Knapp et al., 2009; Pahnila et al., 2007; Williams, 2008). Faily and Fléchais (2010) explain that the formation of organisational security culture is based on a combination of *tangible factors* (technical and procedural controls) and *intangible factors* (assumptions, norms, and values of employees) within the information security implementation. Any attempts to influence employee culture and incentivise secure behaviour, need to target both tangible and intangible factors: friction-inducing technical and procedural controls need to be eliminated, and employee assumptions, norms and values that lead to insecure behaviours need to be understood and addressed to deliver effective security.

2.7.5 Enforcing monitoring and sanctions

Organisational attempts to increase the cost of non-compliant behaviours through monitoring and sanctions should also be implemented and enforced. But, as discussed in section 2.6.3, identifying potential disciplinary offences by employees is currently unmanageable, inefficient and in many cases impossible when rule-breaking is part of an organisation's security culture. To make detection of non-compliance possible (1) security implementation design should provide the potential for low-cost secure behaviours, (2) employees should be aware of information security risks and required actions to participate in risk mitigation, and (3) an organisational security culture that values and favours compliance should be nurtured. Only then it becomes possible for an organisation to create mechanisms that can effectively detect non-compliant behaviours and, potentially, impose sanctions on employees who practice those. The consequences for such violations should be clearly stated both in policies and in SAET content.

2.8 Problems with past organisational security research

The past information security research presented in the previous section provides valuable insights for attempts to re-design security and align it with employee primary tasks. Despite that, as section 2.6 identified, past research failed to provide organisations with solid guidelines, tools and methodologies that can drive the implementation of an end-to-end approach to manage the human element of information security. This can be attributed to a number of reasons:

1. In-depth security behaviour research focused on individual home users, while organisational research focused mostly on higher-level security risk management and policy formulation.
2. There were limited attempts to engage with organisational security users, to better understand and characterise non-compliant behaviours and their drivers.
3. Security behaviour is usually approached as a binary decision, either secure or insecure, failing to identify potential responses to high-friction security by risk-aware employees.
4. The majority of research attempting to create user-centred security design processes focused on designing new systems, with limited attention given to creating methodologies that can improve existing organisational implementations and corresponding security behaviours.
5. Limited attempts were made to define measurements for employee behaviour, and no tools exist that allow for long-term and continuous assessment of employee behaviour and organisational security culture. This prevents organisations from implementing ongoing measurement and learning approaches to constantly monitor and improve the compatibility of their security implementations with their productivity-related activities.

This section provides an in-depth analysis of the above research drawbacks and explains how new research needs to improve on those, in order to provide knowledge that can enable better management of security in modern organisations.

2.8.1 Focus on high-level aspects of organisational security

The vast majority of past organisational security research did not focus on employee decision making, but on high-level aspects of security, like improving information security management (e.g. von Solms,

2006), risk assessment integration in security (e.g. Anderson and Choobineh, 2008; Stoneburner et al., 2002) and writing better policies (e.g. Björck, 2001). On the other hand, attempts to improve security design by better understanding user decision making at the micro level, mostly focused on home security users (Wash 2010; Dourish et al. 2004; Herley 2009), providing no insights on the effects of an organisational environment on employee compliance decisions.

Past organisational security research also failed to deploy research methods that accurately capture the complexity of employee security behaviours: the majority of the work discussed in this chapter was done through surveys and questionnaires (e.g. Da Veiga and Eloff, 2010; Fulford and Doherty, 2003). The use of such data collection methods limits the scope of the investigation to predefined topics decided by researchers (and corresponding organisations) *before* commencing the research, limiting the potential to explore and identify currently unknown behavioural patterns and their causes. The only exception to this is Albrechtsen and Hovden's (2009) open-ended interviews that identified the existence of a value gap between information security managers and end users. This constituted a significant breakthrough in understanding the dynamics that drive security behaviours in modern organisations. The reasons behind the identified lack of direct research engagement with organisations can be attributed to three categories:

1. Lack of perceived direct benefits reduces willingness of organisations to engage with academia. Academic research often needs to verify its findings through further studies, especially when exploring areas where existing knowledge is currently limited. For an organisation that seeks readily available solutions to manage its security challenges, resources invested in working with researchers may often be perceived as better spent elsewhere.
2. Fear of disclosure of sensitive information on security compromises through academic research also acts as a deterrent. Potential legal and reputational consequences make it hard for organisations to allow academic researchers to access such information, and later potentially publish it in the public domain.
3. Reluctance of information security managers to use "untested" innovative approaches proposed by academics to replace their existing ones, although this is a bit of an oxymoron given the current craft nature of information security management, using principles learned "through experience", with minimal scientific knowledge used.

The above problems suggest that, unless the benefits of engaging with academia are made obvious to an organisation (i.e. the possibility to apply scientifically-validated novel ideas to solve a widely prevalent problem), academic access to organisations and industry data will remain hard. This negatively impacts both researcher's ability to produce knowledge that can improve security implementations in organisations, but also security management's ability to deliver more science-driven security implementations.

2.8.2 Limited attempts to engage with users

User-involvement in security design can play a key role in the effectiveness of emerging security implementations (Camp, 2011). Unfortunately, past research that engaged with organisational users, is minimal and, to the author's best knowledge, limited to the following:

1. Adams and Sasse (1999), Sasse et al. (2001), Weirich (2005) and Inglesant and Sasse (2010) used user interviews to investigate user's understanding of security and its effect on their password behaviours.
2. Bartsch and Sasse (2013) found that employees circumvent access control mechanisms when policy change requests appear to ask for too much effort.
3. Beautement et al.'s (2008) *compliance budget* showed that employees are only willing to tolerate a fixed amount of effort for security. Once the organisation demands more than that, they will just stop complying.

The findings of the above research provided valuable insights on how to improve the usability of passwords and access control, but research focus needs to be widened to other aspects of organisational information security. Information handling for example (i.e. how information is stored and shared in organisational or other systems), is a key issue for many organisations. It is currently heavily monitored, with expensive DLP technologies that can block employees from sharing valuable information for work purposes that the DLP admin-defined rules may identify as sensitive. The frustration created by such restrictions can lead to user alienation and create a negative attitude towards security, which can then impact their willingness to comply even with other well-designed security mechanisms. As a result, security research should look further than examining mechanisms in isolation, and aim to identify the complete impact of organisational security implementations on employee workflow, together with emerging employee responses.

The need to further include users in security research also calls for a paradigm shift in how such research is defined. Security aiming to understand and improve user security behaviour is often called *usable security*, but such a definition points to creating easy to use mechanisms. Research on improving user behaviours should always be referred to as *user-centred.* This better reflects its attempt to capture and design for elements of human behaviour that have little to do with ability to interact with a system like employee risk perceptions, their cost-benefit driven security decisions, management pressure to focus on other organisational priorities, and the effectiveness of organisational risk communication.

2.8.3 Focused on security compliance as a binary decision

All the past research presented in this chapter considered users engaging with organisational computer systems as being either in a secure or an insecure state. Undesirable behaviours were those where employees deviated from the security policy content or what the researchers considered to be a "correct" or secure behaviour. This may be partly accurate but it is important to examine for the existence of a middle ground employee behavioural state: how do employees follow up non-compliance? Do they discard security in its entirety or do they resort to other actions outside the security policy? If yes, can the organisation (and other organisations) learn something from the emerging employee behaviours? To answer these questions, security research needs to better understand employee security decisions when they recognise the presence of security-related risks in their work environment, but feel that the mechanisms and processes in place are incompatible with their primary task activities. This can lead to better understanding of current security behaviours in organisations, and development of research and organisational ability to tailor proposed security solutions that better reflect employee priorities and risk perceptions. Emerging new (or improved) security solutions driven by employee understanding and

behaviours are less likely to be resisted, thus improving their real world effectiveness compared to existing ones.

User understanding, perceptions and corresponding behaviours for home computer users have been studied by a number of researchers in the past: Dourish et al., (2004) presented home user perception and understanding of security systems, Wash (2010) revealed home users perceptions of threats and attackers, while Kirlappos and Sasse (2012) and Kirlappos et al. (2012) discussed how users make trust decisions online, using their own understanding instead of provided security indicators, suggesting that such user perceptions and rationalisations should be taken into account when designing security systems. Unfortunately, to the researcher's knowledge, no research similar to the above has been conducted in a corporate environment to date.

2.8.4 Focused on designing new systems, ignored existing ones

Past research on user-centred security focused primarily on devising principles to gather requirements in order to design new, bespoke software or systems to fit the requirements of specific work environments (e.g. Fléchais et al., 2010, Faily and Fléchais, 2010). This provides limited usefulness for organisations seeking to improve their existing security systems and processes; as Ashenden and Sasse (2013) identified: "*a key responsibility for CISOs is to remove blockages that prevent information security from becoming 'business as usual'*". In many modern organisations complete replacement and redesign of a system is not an option, due to corresponding time and cost overheads. For information security research to add value to organisations, it should aim to provide tangible suggestions on how existing organisational security processes and mechanisms can be improved to bring security and productivity closer. Blythe et al. (2014) suggest that this can be achieved in policy rethinking and redesign by identifying existing user behaviour and workarounds: "*Workarounds that don't endanger security and that allow more efficient workflow processes should be incorporated into the organisation's policies, essentially moving the policy "deviations" to actual policy*". This is a promising suggestion, but putting it into practice requires much better understanding of organisational security behaviours than what existed before the work presented in this thesis commenced. In addition, the need to rethink policy design is just one of the three elements of current security implementations that need to be improved to deliver effective protection, as presented in section 2.7 of this chapter. Secure behaviour also requires security mechanisms designed around employee primary tasks, to reduce security-productivity friction, and improved communication, to effectively communicate organisational risks and better understand employee priorities. Information security research should always aim to help organisations in deploying effective protection without the need for expensive and time-consuming adaptations of organisational security (or even complete redesign) that may be uneconomic and difficult to justify.

2.8.5 Lack of measurement and learning-driven security management

Learning needs to become an integral part of modern organisational security management. Schein (2010) explains that in fast changing environments, like modern organisations, it is not appropriate to base decisions in the past or in the present. It is necessary to think *"in terms of the near future to assess whether or not our solutions are working"*. Organisations should aim to develop an ability to learn, which is important for adapting to changing organisational environments, where the business and

technologies constantly evolve and become more complex. In this context of change, security cultures can benefit from becoming more *learning-oriented*. By observing and learning from employee behaviours, organisations can implement continuous improvement programs, in an approach similar to the Plan-Do-Check-Act cycle of ISO27001. This can also allow accurate post-deployment assessment of the impact that security measures have on employee activities, prioritisation of intervention programs and implementation of targeted interventions to address specific security shortcomings.

An effective way to drive organisational learning on information security is the deployment of information security metrics. Current use of metrics in information security management is mostly focused on technical aspects of security (Brotby et al., 2013; Payne, 2009), with some limited attempts to measure employee behaviour being basic and providing outcomes of limited usefulness. Current information security metrics provide information on issues like application vulnerabilities, firewall configuration effectiveness and incident response statistics (Wong, 2011). Relevant standardisation also exists, with the ISO27004 standard on information security metrics defining a number of measurement areas for assessing the effectiveness of Information Security Management Systems (ISMS). Despite that, existing metrics to measure security behaviour in the latest edition of ISO27004, are not suitable to capture the complexity of employee security behaviours in an organisation (e.g. *Count of logs/registries with annual information security awareness training field/row filler as "Received"* or *ask each user about number of passwords which satisfy organisation's password policy*).

Organisational security research needs to generate knowledge that leads to more effective and representative behavioural metrics, and then use those to leverage measurement-based learning and decision-making; this should allow for increased consideration of employee behaviours in the management of organisational security. Looking deeper into organisations to devise metrics that can be used to better understand employee behaviours may sound as difficult at first, but information exists in abundance in modern organisational IT systems. As Hubbard (2010, p48) puts it, "*anything detectable at different amounts is measurable*". In addition, combining various sources of measurable information can provide organisation-wide snapshots of employee behaviours on various information security areas at any given point in time. It also enables user involvement without the need for continuous, and potentially disruptive, direct engagement. This allows security managers working within organisations to be aware of what happens within the wider organisation and can lead to more productivity-focused information security management, prioritising risks closer to the concerns of the business, while also minimising the impact of security on the organisation's productive capabilities.

2.9 Purpose of research

The identified gaps and drawbacks of past user-centred security research demonstrated the need for further research to examine and understand employee security decisions in organisational environments. Hands-on, "on the ground" organisational security research is required to obtain better understanding of existing information security approaches, their influence on employee behaviour, together with corresponding employee responses to those. The identified research gaps led to the emergence of three themes of required research:

1. Need to improve current understanding of insecure behaviours in organisational environments by better capturing and understanding the challenges security introduces in employee workflow. This needs to be done by examining:
    i. employee understanding of organisational information sensitivity and security risks, together with actions required to mitigate those (understanding of what organisationally prescribed secure actions are and how to comply)
    ii. employee experience with organisational security provisions to mitigate aforementioned risks and protect the organisation
    iii. corresponding employee behaviours (how and why security mechanisms and processes are followed or bypassed) and responses to high-friction security, also examining employee understanding of the risks related to their actions
    iv. the difference between insecure behaviour driven by lack of awareness and insecure behaviour driven by high-friction security, together with lessons organisations can draw from those
2. Widen the scope of user-centred security research to capture a more holistic view of the organisational security implementation, including as many mechanisms and policies employees have to deal with as possible. Past research approaches demonstrated the difficulty of attempting to understand user compliance by only studying specific parts of it. Attempts to remove security-productivity friction require reducing the overall impact of security mechanisms and processes on organisational productivity, so studying those in isolation can only partly address the problem. As a result, in order to deliver approaches that lead to more effective protection, the goodness-of-fit of the overall security implementation with employee primary tasks needs to be evaluated.
3. There is also a clear need to identify elements of organisational security implementations that can be used to devise metrics for employee security behaviours. These can then be used to assess organisational security effectiveness, create learning and communication channels for information security management, drive future improvements, and assess the effect of those on employee behaviour and the overall organisational security environment.

Research aiming to address the above topics requires active engagement with organisations in a way that can provide rich information on employee interaction with security systems, rules and processes. In the remainder of this thesis, I discuss how I proceeded to conduct two case studies with two large organisations to (1) overcome identified problems in security research by engaging directly with organisations, (2) produce knowledge that significantly addresses the identified gaps in the approaches and findings of past research, (3) improve understanding of the impact of security on employee productive activities, (4) better characterise employee response to that impact and their emerging behaviours, and (5) use the emerging knowledge to provide organisations with an approach to drive more effective and user-centred information security management.

Chapter 3: **Methodology**

The identified gaps in past organisational security research, discussed at the end of the literature review, suggested the need to improve existing understanding of employee security behaviours, as a prerequisite to any attempts to improve existing organisational security implementations. In order to deliver such understanding, further research examining security behaviours in organisational environments was required. When this research commenced, the author was presented with a unique opportunity to conduct such hands-on research: an EPSRC-funded project ("*Productive security*"[12]) that started at the same time as the author's PhD degree (led by the UCL Information Security Research Group - ISRG), provided access to organisations and data that would not be possible otherwise. The two organisations involved in the project (*Company A* and *Company B*) were large multinational companies with strong UK presence. In both organisations, security management had recognised the need to improve understanding of employee security behaviours in relation to their current security implementations. As part of their attempts to improve, they approached ISRG asking for knowledge and guidance that could drive future security planning and implementation. As part of this, they agreed to provide access to their employees, together with additional data required for this research, in order to identify and characterise employee behaviours, identify potential areas for improvement, and provide knowledge and guidance to drive those improvements.

The two organisations agreed for the author to conduct two case studies, which involved both using existing data and collecting new one. The data collection and analysis process aimed to capture employee interaction with existing security mechanisms and processes, but also their attitude towards security. The research work presented in the remainder of this thesis was conducted in six phases:

Phase 1 *Company A thematic analysis.* The research commenced with a preliminary thematic analysis of 30 interviews from Company A. Previous work of the ISRG with Company A during a past project ("*Trust Economics*"[13]) led to a large interview set (118 interviews) and a survey (1488) on employee security behaviour being readily available. This dataset was previously used for other publications relating to access control (Bartsch and Sasse, 2012, 2013), but no analysis attempted to holistically examine employee interaction with security, investigate friction-inducing security and identify employee responses to it. The preliminary analysis of phase 1 allowed categorising identified insecure employee behaviours, based on factors driving their development. It also allowed identification of cause and effect relationships between existing security mechanisms or processes and corresponding employee behaviours, also identifying areas where further research was required. The thematic analysis process followed is outlined

[12] Productive Security is an EPSRC funded project at UCL Research Institute for the Science of Cyber Security. It aims to scientifically assist decision makers in the field of information security to make more optimal choices with respect to both their organisation's security and productivity.

[13] http://sec.cs.ucl.ac.uk/projects/trust_economics/

later in this chapter (section 3.5.1), while its application and findings are presented in chapter 4.

Phase 2 *Company A grounded theory analysis.* Based on the improved understanding that emerged from the Phase 1 analysis, a second analysis was done of the full set of Company A interviews. This analysis improved and enriched the early analysis findings on employee insecure behaviours. The prevalence of insecure behaviours across the organisation was confirmed by analysing the available survey results. This led to the emergence of the main contribution of this thesis – the identification of *Shadow Security*, its impact on employee security behaviours and its relevance to organisational security management (chapter 5).

Phase 3 *Company B data collection*. Based on the improved knowledge from Phases 1 and 2, 82 interviews were conducted in company B. Those were used to confirm and strengthen the validity of the paradigms that emerged from Phases 1 and 2. In order to capture the prevalence of the identified security behaviours across the organisation, a survey of 641 employees was conducted, based on a preliminary analysis of the 82 interviews (chapter 5).

Phase 4 *Company B grounded theory analysis.* This stage allowed confirmation and better characterisation of shadow security, confirmation of its existence in a different organisational setting than the one in which it was originally identified, better characterisation of its occurrence and impact in a security implementation, and potential approaches to better manage its development in organisations (chapter 5).

Phase 5 *Trust-focused grounded theory analysis.* The analyses from Phases 1, 2 and 4 suggested the need to examine the development of security-related trust relationships in the two organisations and its influence on employee security behaviours. In order to do so, a secondary grounded analysis of both interview datasets was conducted, focusing on instances where the presence of trust influenced employee behaviours (chapter 6). The findings from Phases 4 and 5 were used to devise a set of principles, guidelines and metrics that allow organisations to better incorporate shadow security and trust in their security management approaches (chapter 7).

Phase 6 *Case study.* On-site work with Company B for 6 months, allowed examining the application of the emerging principles, guidelines and metrics in an organisational environment. This led to identification of the challenges of doing research in the field, but also potential challenges for researchers attempting to deploy research findings in organisations, together with ways to address those (chapter 8).

The remainder of this chapter presents and justifies the choice of research methods used in the above research phases, also describing the data collection and analysis processes. It also discusses the steps taken to improve outcome validity, presents an ethical analysis of the research in question and discusses the required ethical research principles followed while conducting this research.

3.1 Case Study

The exploratory nature of the research problem made standard statistical methods an unsuitable research approach. It required an exploratory approach that would allow improving the current understanding of both practitioners and researchers on how security behaviours in organisations are affected by various elements of an existing security implementation. As a result, a case study appeared to be the most

suitable method to use. Thomas (2011) defines a case study as "*…analyses of persons, events, decisions, periods, projects, policies, institutions, or other systems that are studied holistically by one or more method*". It is focused on understanding the dynamics presented within single settings, investigating a phenomenon within its real-life context, revealing "*Not only what, but also why and how*" (Yin, 2009). A case study is a form of interpretive research (Lapke 2008, p68): it does not predefine independent and dependent variables, focusing on the complexity of human sense as the situation in question emerges, attempting to understand phenomena based on the meanings people assign to them. It can be both descriptive and explanatory (Eisenhardt, 1989), and is good for subjects where existing knowledge is fundamentally flawed or non-existent: case study outcomes can enrich the available understanding of the research issues of interest (Gerring, 2004). The case that is the subject of the inquiry is an instance of a class of phenomena, providing an analytical frame, an object, within which the study is conducted and which the case illuminates and explicates. A case study also has "*…an aim to generalise across a larger set of units*" (Gerring, 2004). Essentially a case study's purpose is "*not hoping to prove anything but learn something*", on a problem where lack of existing understanding prevents the use of other research methods (Eysenck, 2013).

3.1.1 Merits of case study

The use of case studies in research provides a number of advantages compared to statistical approaches (Table 4):

1. *Identification of difficult to capture insights*: Case studies offer insights, observations and examples not easily revealed using other research approaches. The depth of investigation allows for improved understanding of situations of interest where pre-existing knowledge is limited (Eisenhardt, 1989).
2. *Providing causal explanation of phenomena*. In-depth description of phenomena during a case study allows identification of causal explanations for phenomena of interest (Yin, 2009).
3. *Biased towards falsifying theories*. Case study research is not more biased towards verification than statistical methods. Instead there is greater bias towards falsification, as single case studies can disprove a theory by showing that a current situation is problematic; in such cases one proof of evidence is adequate for falsification of a theory (Flyvbjerg, 2006).
4. *Avoids removing extreme cases*. Case studies also avoid the problem of having rare, but potentially critical, situations being treated as outliers by other statistical methods. They also prevent the potential for the effect of such rare events on the phenomenon of interest being lost in normalisation (Yin, 2009).
5. *Useful for theory generation*. The improved situational understanding of the phenomena of interest, emerging from case studies, can be used to provide justification for generation of both theories and testable hypotheses that can drive further research (Gersick, 1988).

	Case studies	Statistical methods
Strengths	Depth High conceptual validity Process and context understanding Understanding causes and outcomes of phenomena Fostering new hypotheses and research questions	Breadth Understanding prevalence of phenomena across population Measuring correlation for case population Establishment of probabilistic levels of confidence
Weaknesses	Selection bias may overstate or understate relationships Weak understanding of occurrence in population Statistical significance often unknown or unclear	Conceptual stretching to get larger samples Weak understanding of context, process and causal mechanisms Correlation does not imply causation Weak mechanisms for fostering new hypotheses

Table 4: Case study vs Statistical methods (adapted from Yin, 2009 - p8)

3.1.2 Criticism and defence of case study as a research tool

The main criticism against the use of case studies in research is that they lack generalisability. This argument is based on the lack of statistical testing or statistical proof of causal relationships in phenomena that occur in the context examined, which often leads to researchers immediately dismissing case study findings as situation specific (Lee and Baskerville, 2003). But the truth is that case study research has no need or desire to be statistically generalisable (Lapke and Dhillon, 2008). Instead of looking for numbers to perform statistical analyses on, a case study aims to interpret a situation of interest as much as possible to: (1) provide *holistic* and *meaningful* understanding and description of real events within a problematic situation (Yin, 2009), then using that understanding to (2) generate knowledge that can be useful in tackling similar problems in the future. Consequently, generalisability of case study findings is not achieved through statistics, but by applying the acquired knowledge to similar contexts when studying new cases. In addition, emerging knowledge can be usefully applied without having to keep all other parameters constant, as traditional statistical methods strongly require (Guba et al., 1994). As a result, despite the lack of *statistical* generalisability, findings and knowledge generated from case studies are much easier to transfer across different complex environments than those generated by statistical methods. The case study definition of generalisability ties well with its dictionary definition: "*forming general notions by abstraction from particular instances*" (*Oxford Dictionary of English*, 2010). As Walsham (1993) puts it: there are no correct or incorrect theories, just interesting and less interesting ways to view the world and case studies can provide rich representation of such worldviews.

3.1.3 Why it was chosen

The exploratory nature of the research topic and the complexity of the research problem (insufficient existing understanding of employee security behaviours) required a research method that would focus on improving existing knowledge, instead of testing specific theories. This made a case study the most suitable approach. Case studies currently amount for a large proportion of published books and articles in

psychology, anthropology, sociology, history, political science, economics and medicine (Flyvbjerg 2011) due to their exploratory and learning-oriented nature. They have already been reported as a good research method to use in software engineering and information systems, when the boundaries between phenomena and their context is unclear, offering insights impossible otherwise; examples can be found in Runeson and Höst (2008) and Walsham (1993). Despite that, there are few reports of case studies being used in studying the application of information security in organisational environments. A notable exception is Lapke (2008), who used case studies to demonstrate that organisational power relationships significantly influence the formulation and implementation of information security policies, and Moore et al. (2011), who used those to characterise the drivers and nature of insider attacks in US-based organisations. This section outlines the reasons for which case study was chosen as a suitable methodology for the research presented in the remainder of this thesis.

3.1.3.1 Proving the existence of a problematic situation

The case studies conducted aimed to demonstrate the ineffectiveness of current information security approaches, by providing organisations with tangible examples of failures of their existing processes and mechanisms to tackle current security challenges. This proved to be a useful tool for the author (and other ISRG researchers) in attempts to provide relevant and practical suggestions for improvements to partner organisations.

3.1.3.2 Deep understanding of a problem where knowledge is limited

As previously explained, the aim of this research was to better understand and characterise how existing security controls fail to deliver compliance and how employees respond to those. A case study makes this possible by identifying causal explanations for non-compliance by revealing missing or incorrect elements of the security implementation that negatively influence employee behaviour. In addition, to the best of the researcher's knowledge, no research has been published to date on employee security behaviours that had access to such a large dataset from more than one organisation. When access to such a dataset was secured, a case study approach would provide insights previously inaccessible and unattainable.

Directly interacting with employees during the interview phase allowed for better understanding of employee priorities and the effect of current security implementations on the organisations' primary task-focused functions. This allowed identifying causal links between friction-inducing security and corresponding employee behaviours. The emerging knowledge proved to be useful when engaging with corporate partners: it attracted attention from industry by providing tangible evidence that current security approaches are ineffective and require improvements. In addition, the combination of two studies from different organisations allowed for widening the scope of the emerging paradigms on information security compliance, also improving the validity of the outcomes and transferability of those to solve security behaviour challenges in other organisational settings (Yin, 2009; Flyvbjerg, 2011).

3.1.3.3 Looking for rare events

Unless a security implementation suffers from severe drawbacks, information security behaviours in many organisations may appear "good enough" on a macro scale, when average-case behaviours are examined. This means that statistical testing can potentially miss infrequent events, by dismissing those

as outliers or losing those in normalisation. The rarity and "extreme case" nature of many high-risk behaviours (security breaches are often rare events, with non-compliance affected by many different contextual and individual factors), made statistical testing unsuitable for this research and case studies a more suitable method to use.

3.1.3.4 Hypothesis testing unsuitable to use

Hypothesis testing calls for a controlled environment where control of other influences to the phenomena examined exists. In addition it requires possession of sufficient knowledge on that phenomena for statistical hypotheses to be devised before the research commences. This made hypothesis testing unsuitable for this research for three reasons:

1. As mentioned in section 3.1.3.2, existing knowledge on employee behaviour by security researchers, designers or decision makers is not specific enough to devise hypotheses that accurately capture the nature of insecure behaviours and their causes.
2. Attempting to only verify a set of statistically testable hypotheses ends up focusing only on specific, predefined factors that a researcher assumes to influence security behaviours. This carries the risk of missing the bigger picture, failing to identify previously unknown drivers behind employee behaviours (Flyvbjerg, 2011; Yin, 2009).
3. It is impossible to control elements of organisational environments to avoid damaging the validity of hypothesis testing research. In organisations changes in the environment happen very quickly and are often unpredictable (this became even more obvious when research commenced and during the subsequent fieldwork): organisations have projects, audit deliverables, annual targets, changes in their target markets they may need to adapt to, even mergers, acquisitions and outsourcing of key divisions happening constantly, often at very short notice. Any attempt to engage with them to improve their security should pose a minimal impact on their production related tasks, but also be adaptable to the pace with which the above changes happen in the corporate world. This makes controlling organisational elements for statistical testing impossible, as all the above changes would invalidate the results.

3.1.3.5 Creates potential for future research

The improved knowledge on employee security behaviours that can emerge from case studies provides significant ground for future research. It allows the formulation of future testable hypotheses, grounded on real-world problems identified during the case study (and clearly outlined in case study reporting), leading to wider applicability of the findings. This proved to substantially address the "narrow focus" problem of past information security research discussed in section 2.8 of the literature review.

3.2 Data collection

3.2.1 Interviews

The interviews conducted covered various aspects of information security in the organisations examined and the experience of employees with it, aiming to identify friction points between security and business processes that lead to insecure employee behaviours. Interview questions were semi structured: combining features of structured interviews (closed, questionnaire-like questions) and unstructured (open questions). The choice of a semi-structured approach was driven by the need to cover interaction with

various mechanisms and areas of interest to the organisation, but also provide adequate flexibility for employees to share their behaviours and beliefs on the interview topics, aiming to improve understanding of security behaviours in the organisational setting (Rogers et al., 2011). The interviews were conducted one-to-one by a team of three researchers in Company A and four researchers (including the author) in Company B, lasting approximately 50 minutes each, allowing for elicitation of a suitably rich representation of the employee experience of security. All interviewers received interview training together by the ISRG group leader and the study protocol was pre-shared, discussed extensively and was well understood by the interviewers before the interview process commenced. During the interview process, interviewers were instructed to follow up employee responses: when interviewees reported problems with a security mechanism, they were asked additional questions, to further explain the implications of those problems on their primary tasks and the actions they take to alleviate those. At no point were participants encouraged to admit to security infractions though. They were simply asked about their awareness of, and experience with, a set of corporate security policies and mechanisms. Researchers probed interviewees to discuss insecure behaviours only when they reported those first. Out of the 82 interviews conducted in Company B, the researcher directly conducted 20.

To ensure interviews were adequately context-specific for each organisation, question formulation was done in collaboration with the organisations' security managers. This led to interview questions that accommodated for the organisation's security policy, security mechanisms, the nature of organisational primary tasks, the organisation's goals and security objectives, and concerns of the organisation's management on employee behaviours that could potentially lead to security compromises. Interview sets were also structured to reflect other organisational characteristics (e.g. localised differences between office locations). Piloting of the interview sets was also done with employees from both companies, ensuring that the formulated question set accurately reflected the organisational environment in question. The structure of interviews touched upon aspects of security awareness and compliance, including:

1. Employee perception of potential sensitivity of the information they handle and how security affects their role.
2. Employee understanding of organisational support for security. This included awareness of the existence of security policies and corresponding security mechanisms that they should or could use to protect information and reduce security risks.
3. Where employees exercised non-compliance as a response to shortcomings or friction in the organisational security experience, identification of the conditions that led to those behaviours being divergent from organisation policy. In those cases, the interviews also assessed their understanding about the need for security, despite non-compliance, and potential actions that emerged from it.

The general topics included in all interviews were (detailed topics and extended questions for one of the two sets of interviews can be found in Appendix B: Sample interview questions):

1. Information Security policy awareness
2. Employee awareness of the sensitivity of information they handle
3. Management involvement in security compliance

4. Information Security Culture
5. Password use and handling
6. Information handling and sharing
7. Document sharing
8. Laptop and removable media usage

Sampling (selection of interview participants) did not aim for randomness but for broad organisational coverage, aiming to extend the context of emerging theories as much as possible (Eisenhardt, 1989). Participants held various lower and lower-to-middle management positions within a number of organisational divisions, including maintenance, customer service, marketing, administration, finance, procurement and IT, and were based in various US or UK locations. They were recruited via the company email newsletter, sent to a random sample of employees from each department. Participation was also encouraged by the organisations' Chief Information Security Officers, who also assured that participants would not be identified or followed up when insecure behaviours were identified.

In company A the first 118 responders were scheduled for interview in person or by phone. Participants were given a consent form that described how transcripts would be anonymised and only aggregated results reported to the organisation, also explaining that they could ask the interviewer further questions about the process and terminate the interview at any point. After the interview, participants were paid the equivalent of £25. The same applied to Company B although, being a slightly smaller organisation, the number of employees interviewed was 82. The interviews were recorded in duplicate recorders and copied on encrypted external drives when travelling between interview locations and the university. Due to the high volume of interview data in audio format, transcription to text was done by an external company. It was done on an accurate word-to-word basis to ensure all employee responses were captured accurately in text format.

3.2.2 Using available data in new research

As mentioned earlier in this section, interview and survey data from Company A was already available before commencing this research, so a secondary analysis was conducted on those. The main advantage of secondary analyses is that they save a significant amount of time compared to the collection of bespoke data (Bryman, 2012). This was crucial for successfully carrying out the work presented in this thesis, as collecting two large data sets was beyond possibility for a PhD project, both in terms of cost and time required for the desired data collection and analysis in two large organisations. Availability of one large interview set and collection of a second one, led to high-quality data being used, which allowed for better exploration of the research problem in question and creation of an end-to-end story that can be used to drive future improvements of organisational security management.

3.3 Case study: How it was done

3.3.1 Case study process

The case study process followed in the research presented in this thesis was based on Yin's (2009) six steps for a successful case study (Figure 5): (1) Identification of questions, (2) Identification of unit of

inquiry, (3) Definition of study propositions, (4) Collection and analysis of data, (5) Logical linking of data to propositions, and (6) Interpretation of findings.

Figure 5: Yin's case study process

3.3.1.1 Identification of study questions:

As previously discussed, this research aimed to improve on the existing understanding of security behaviours in organisations, based on the identified failures of organisational security management and past security research to effectively include employee primary-task priorities to the design of security solutions. To achieve this, the two case studies presented in this thesis aimed to better understand and answer the following research questions[14]:

1. *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?*
2. *What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?*
3. *How can the improved understanding from the previous question be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?*

3.3.1.2 Identification of unit of inquiry

The focus of this case study was both the users of organisational security (and their security behaviours) and the security mechanisms and processes they interact with (in order to provide insights to organisations on how existing security mechanisms and processes can be modified to better accommodate for employee focus on the primary task).

3.3.1.3 Definition of study propositions

Based on the identified research gaps of section 2.8, the questions that needed to be examined and the identified units of inquiry, five study propositions were defined:

P1. "Directly discussing problems of security implementations and compliance with employees can lead to improved understanding of the reasons driving employee insecure behaviours"

P2. "*Engagement with employees can allow falsifying current beliefs that employees can be forced to comply with security*"

P3. "Engagement with employees can allow identification of employee responses to friction-inducing security"

[14] After completion of Phase 1 (Thematic analysis of 30 Company A interviews presented in Chapter 4), the question set was updated with three more questions – see section 4.7.3.

P4. "*Engagement with employees can allow the identification of problems in security implementations (both policies and mechanisms) that organisations have not currently identified through other means*"

P5. "*Engagement with employees can improve existing organisational ability to manage current information security challenges*"

3.3.1.4 Logical linking of data to propositions

A number of different techniques were used to generate the theories presented in the remaining chapters of this thesis: pattern matching (Trochim, 1985) was used to test emerging theories against user behaviours across both organisations, explanation building (Amaratunga et al., 2002) was used to identify causal links between conditions in the organisational environment and emerging security behaviours, and cross case synthesis was used (Yin, 2009) to verify the existence of the observed phenomena across organisational divisions in both organisations examined. As previously discussed, the emerging theories were the results of an iterative process: many rounds of data collection and analysis were used to arrive at the findings and theories presented in the remainder of this thesis.

3.4 Improving outcome validity

In order to provide guidelines to assess the validity of case study findings, Yin (2009) defines four axes on which the quality of any empirical social research is judged:

1. *Construct Validity*: Identifying correct operational measures for concepts studied
2. *Internal Validity*: Establishing causal relationships between conditions
3. *External Validity*: Ability to analytically generalise the findings within a larger domain of interest
4. *Reliability*: Demonstrating repeatability of the findings

This section discusses the steps taken during the analysis process, in order to meet all four of Yin's research quality requirements.

3.4.1 Investigator triangulation – Improving Internal validity

As discussed in section 3.2.1, many researchers took part in data collection and all received training from the ISRG group leader, who has significant experience in conducting research in similar settings. Researchers also spent a lot of time discussing each other's interpretation of the data, in order to ensure no unjustified conclusions emerged from the work presented in this thesis, or any of the other research publications related to this work.

3.4.2 Methodological triangulation – Improving Internal validity

Another way to improve the validity of case study results is to combine more than one sources of evidence (Bryman, 2003; Klein and Myers, 1999). For Company A, this was done using an already available set of survey data. The surveys were conducted based on a preliminary analysis of the interview data by Dr Adam Beautement. They presented participants with examples of scenarios where security and productivity came to conflict, drawn from the interview results, and asked them to respond to those.

To capture both employee behaviour and attitude towards friction-inducing security, two different interview scenario types were used:

- *Behaviour scenarios*: Survey participants were presented with a scenario where a conflict between security and their primary occurs and were offered four non-compliant courses of action that would allow them to resolve the conflict. They were then asked to rank the options in order of how likely they would be to follow them and also to rate how severe is the breach of policy the chosen course of action presents. The presented courses of action are based on Schwarz and Thompson's risk models (Schwarz and Thompson, 1990) and each one corresponds to a different risk response behaviour (individualists, egalitarians, hierarchists, fatalists – short description for each in Appendix C).
- *Attitude scenarios*: Attitude scenarios reflected different levels of maturity on the Security Behaviour Maturity Model (SBMM – an adapted version of the Carnegie Mellon Capability Maturity Model – Appendix D, Paulk et al., 1993). A security violation or non-compliant action was presented to employees, who were then given four potential actions representing attitudes towards that action, each one referring to a different level in SBMM. Again participants were required to rank the available options in terms of how likely they were to follow each of the described courses of action.

A similar survey was conducted inside Company B, with the researcher taking part in formulating the scenarios and the corresponding responses, in collaboration with a team of 3 other researchers. As discussed at the beginning of this chapter, in total 1488 employees from Company A and 641 from Company B took part in the survey. Example scenarios for both attitudes and behaviours and the available actions can be found in Appendix E. For the purpose of this research the survey data from both organisations were used to (1) strengthen interview findings by demonstrating the prevalence of identified insecure employee behaviours in both organisations on a much larger scale than the 200 interviews. The quantitative nature of survey results also (2) allowed the two organisations to prioritise solution deployment to address the more serious of the identified issues first.

3.4.3 Pattern matching – Internal validity

Matching and comparing emerging patterns is another way to improve internal validity of case study findings. Behavioural patterns identified in early interview analyses were matched to behaviours observed in subsequent interview analyses across both organisations. This led to improved validity of the findings, together with improved applicability and generalisability to a wider domain (Yin, 2009; Flyvbjerg, 2011).

Pattern matching example

Paradigms emerging from early analysis: When security policy or mechanisms impose significant overheads on employee primary tasks, employees restructure those tasks or find alternatives that they perceive as preserving security, but are less taxing on their productivity.

Patterns identified in follow-up analyses:

1. Company A: Company provided encrypted USB drives were described as "slow and problematic" for file transfers within the office. Employees used their own unencrypted ones and then deleted the data, assuming their actions preserve security.
2. Company B: Internal file sharing mechanisms were slow to setup and fine-graining access control was slow and hard to get right. Employees then used third-party file sharing facilities, ensuring only those who needed access to that information could see it.

3.4.4 Data Triangulation – Improving construct validity

As discussed at the beginning of this chapter, the primary data collection method used to devise the paradigms presented in this thesis is interviews. Investigating potential validity compromises, two factors were identified in the use of interviews as a research tool that could negatively affect the validity of the outcomes:

1. *Non face-to-face interviews:* Despite the majority of interviews being conducted face to face, some employees were located at remote locations or working from home. In order to include them in the sampling and improve the representativeness of the research sample, they had to be interviewed over the phone (this was a challenge present in both companies, but more prevalent in Company B). This initially seemed as a limitation, but over time it became obvious that, in both the organisations studied, employees spend a significant part of their time working remotely, and are accustomed to discussing business issues over the phone. Ignoring this element of the organisational setting by removing them from the sample would narrow the focus of the study to the few office locations where physical access was possible. This would exclude employees in smaller offices around the country or working from home, missing a large part of the organisational structure. Combining face to face and phone interviews allowed for improved data collection and better company representation.
2. *Selection bias:* Interviews can also result in overstating or understating the importance of identified problems due to selection bias. In addition they may provide weak insights on the seriousness of phenomena of interest (Flyvbjerg, 2011). Despite this, as previously reported, statistical generalisability was not a goal for this research; the focus was on improving current understanding of employee responses to friction-inducing security mechanisms.

Despite not aiming for statistical generalisability, a number of steps were taken to improve the validity of the emerging case study constructs:

1. Employees across different divisions were interviewed, which ensured the emerging constructs were valid across various organisational divisions. In addition the number of interviews was

high compared to past case studies, which also improves the validity of the constructs and demonstrates their prevalence in the examined settings (Yin, 2009).

2. The use of pattern matching to confirm findings in more than one organisations and improve internal validity also improves construct validity (Trochim, 2006).
3. Inferences were never made unless cause and effect could be identified in employee interviews. The chain of evidence that led to the knowledge emerging from this work was purely based on what employees reported as their response to non-compliance (no pre-conceived notions existed, no hypotheses to be tested), which was then confirmed by the surveys (Yin, 2009).
4. The findings of the case studies were reviewed by the organisations involved to ensure reported outcomes were consistent and valid within the environment in which they were observed, which again improves construct validity (Yin, 2009).

3.4.5 External validity

Improving the external validity of the findings was also important, as research lacking external validity cannot be applied to settings differing from the one in which the theories were developed. This significantly narrows the scope and applicability of emerging knowledge, also reducing their usefulness to other researchers or practitioners operating in different contexts. The combination of method and investigator triangulation, pattern matching and data triangulation from different case studies aimed to provide external validity for the findings (Flyvbjerg, 2011; Gerring, 2004), which improves their generalisability (Eisenhardt, 1989).

3.4.6 Reliability

Attempts to improve the reliability of the analysis process focused on two areas:

1. The coding process and the findings were reviewed by and compared amongst the four researchers that analysed the interview data, to ensure emerging themes were consistent with the behaviours represented in those.
2. The iterative approach of the analysis (revisiting interview sets after early identification of the concepts reported in this thesis), ensured the process managed to capture a rich understanding of the examined environment and corresponding behaviours (Figure 6).

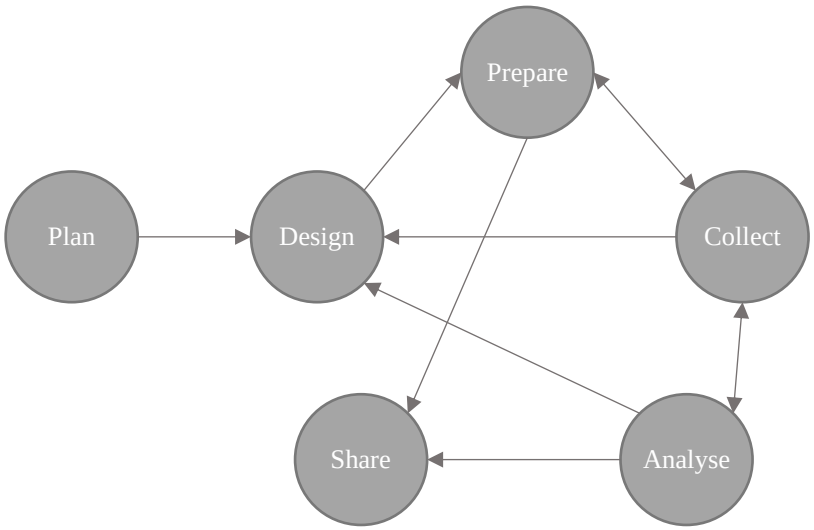

Figure 6: Iterative case study approach (Yin, 2009, p1)

3.5 Analysis

As discussed in section 3.1.3, the exploratory nature of the research problem required the use of a research approach that would iteratively revisit the available data sets, continuously aiming to enrich and strengthen the emerging theories. To achieve this, the analysis of the interview sets was done in many stages, using two different approaches:

1. *Thematic analysis*: During the first phase of this work (*Phase* 1) an exploratory investigation was required to examine employee interaction with Company A's security implementation and their corresponding behaviours. As a result, a thematic analysis was conducted on a subset of the Company A interviews, aiming to gain some initial understanding of the research questions and allow focusing of further research and analyses.
2. *Grounded theory*: *Phases* 2, 4 and 5 required an analysis approach that would build on the knowledge that emerged from Phase 1. Using a grounded theory approach, allowed enriching understanding of the concepts identified by the thematic analysis, but also led to the emergence of new concepts that better characterised employee behaviours (*shadow security, security-related organisational trust relationships* discussed in chapters 5 and 6).

3.5.1 Thematic analysis

Braun and Clarke (2006) define thematic analysis as: "A method for identifying, analysing and reporting patterns within data." A thematic analysis is a data driven analysis that offers an accessible and theoretically-flexible approach to qualitative data analysis. It is an inductive process, with data coded *without* trying to fit it into a pre-existing coding frame, or the researcher's analytic preconceptions. *Codes* are assigned to pieces of text, identifying a feature of the data (semantic content or latent) that appears interesting to the analyst, referring to "the most basic segment, or element, of the raw data or information that can be assessed in a meaningful way regarding the phenomenon of interest". Codes then develop to *themes*, which are broader concepts, aiming to capture important properties of the data in relation to the research questions asked. Emerging themes represent patterned responses or meanings within the data set, providing an interpretative analysis of the data in relation to the phenomenon being examined (Boyatzis, 1998).

The process followed for the thematic analysis presented in chapter 4 was based on Braun and Clarke's (2006) set of 6 steps for an effective thematic analysis (Figure 7)

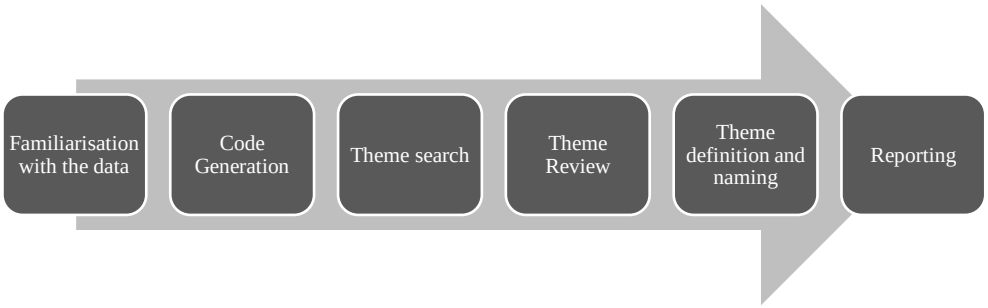

Figure 7: Thematic analysis steps (Braun and Clarke, 2006)

3.5.1.1 Phase 1: Familiarising with the data

Read and re-read data in order to become familiar with what it entails, paying specific attention to any patterns that occur. Present preliminary "start" codes and detailed notes, along with a description of what each code means and the source of the code.

3.5.1.2 Phase 2: Initial code generation

Generate the initial codes by documenting where and how patterns occur. This happens through data reduction where the researcher collapses data into labels in order to create categories for more efficient analysis. Data complication is also completed here. This involves the researcher making inferences about what the codes mean. The researcher also needs to provide detailed information as to how and why codes were combined, what questions are asked of the data, and how codes can improve the researcher's ability to answer those questions.

3.5.1.3 Phase 3: Searching for themes

Combine codes into overarching themes that accurately depict the data. It is important in developing themes that the researcher describes exactly how the codes were interpreted and combined to form themes, clearly define themes and their assigned meaning, even if some theme does not seem to "fit" the initial analysis purpose, or if they contradict each other. The researcher should also describe what is missing from the analysis and present a list of candidate themes for further analysis.

3.5.1.4 Phase 4: Theme review

In this stage, the researcher looks at how the devised themes support the data and the overarching theoretical perspective. If the analysis seems incomplete, the researcher needs to go back and investigate available data to close any identified knowledge gaps. This stage should present a coherent recognition of how themes are patterned to tell an accurate story about the data, including the process of understanding themes and how they fit together with the given codes. Any answers to the research questions and emerging data-driven questions need to be abundantly complex and well-supported by the data.

3.5.1.5 Phase 5: Theme definition and naming

The researcher needs to define what each theme is, which aspects of data are being captured, and what is interesting about the themes, in relation to the research questions. They also need to provide a comprehensive analysis of the themes' contribution to the emerging understanding of the data.

3.5.1.6 Phase 6: Reporting

When the researchers write the report documenting thematic analysis findings, they must decide which themes make meaningful contributions to understanding what is going on within the data. Researchers should also conduct "member checking" for themes by going back to the data at hand to see if their description of phenomena is an accurate representation of what is depicted in the data. In this stage researchers provide a thick description of the results, noting why particular themes are more useful at making contributions and understanding what is going on within the data set.

As discussed earlier in this chapter, thematic analysis was chosen as the data analysis approach for the first stage of this work, to identify phenomena in the organisational environment related to the research questions asked. The findings from applying the thematic analysis process on 30 of the Company A

interviews provided useful insights and improved understanding of employee security behaviours. They identified cause and effect relationships between security mechanisms and insecure behaviours, and allowed categorising insecure behaviour occurrences to three major categories: (1) expensive compliance, (2) lack of underlying conditions required for compliance, and (3) employees lacking compliance motivation (for more on this categorisation and thematic analysis findings, please refer to chapter 4). Despite the usefulness of the knowledge emerging from the findings, better understanding was required on some emerging phenomena (e.g. employee responses to perceived lack of organisational support for security, or the influence of trust relationships in the organisational environment on employee security behaviours). This led to research question refining and, using the preliminary understanding that emerged, in depth investigation of security behaviours using a grounded theory analysis on the full available interview data set from both companies.

3.5.2 Grounded Theory analysis

Grounded theory consists of the process of taking data, breaking it down, conceptualising it and putting it back together in new ways. It is an established social science methodology that provides a focussed and structured approach for the collection and analysis of data, with the aim of creating empirically-based theories. It is suited to the systematic creation of a theory of complex high-level phenomena about which little knowledge is available. It was originally conceived by (Glaser et al., 1968) as the product of the close inspection and analysis of qualitative data, but was later developed further by Strauss and Corbin (1998), who defined it as "*…theory that was derived from data, systematically gathered and analysed through the research process. In this method, data collection, analysis and eventual theory stand in close relationship to one another. A researcher does not begin a project with a preconceived theory in mind (…). Rather, the researcher begins with an area of study and allows the theory to emerge from the data*." This makes it particularly suitable for investigation of complex subjects or phenomena on which knowledge is limited before commencing the analysis (Strauss and Corbin, 1998).

3.5.2.1 Why grounded theory

Grounded theory was used in the work documented in this thesis, as it is considered ideal for investigating phenomena about which little knowledge exists, or available knowledge is fundamentally problematic (see identified research gaps in section 2.8). In addition, reporting of emerging theories is usually in the form of story-lines, which made it easier to generate prescriptive knowledge to practitioners and security decision makers in the form of context-specific scenarios that reflected conditions they may encounter in their own organisational setting.

3.5.2.2 Process

In order to ensure the grounded theory analysis process takes place in a structured manner, Strauss and Corbin (1998) identify 3 major coding stages (*open*, *axial* and *selective* – Figure 8).

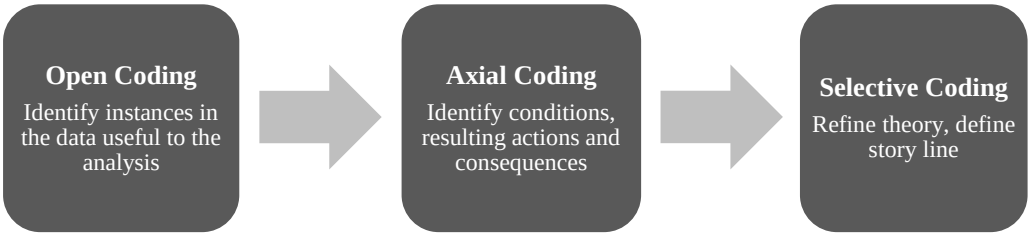

Figure 8: The Grounded Theory process (Strauss and Corbin, 1998)

3.5.2.2.1 Open coding

Notable reported facts or behaviours about the issues of interest to the analysis are identified as *concepts* and similar concepts are grouped together under *categories.*

1. *Concepts*: Labelled phenomena of interest, representing abstract representations of an event, object or action/interaction that the researcher identifies as being significant in the data.
2. *Categories:* Groups of concepts grouped together under a more abstract higher-order concept.

During the process some categories can be turned to sub-categories and vice versa. This is all part of an iterative approach, aiming to ensure the emerging theories accurately represent the facts reported in the data.

3.5.2.2.2 Axial coding

This stage reassembles data that were fractured during open coding. At first, *properties* of a category (characteristics or attributes) and *dimensions* (possible values of a property along a continuum) are determined. The emerging categories are then broken down to *subcategories* based on those properties and dimensions: these specify a category further by denoting information such as when, where, why and how an identified phenomenon is likely to occur. Subcategories can take the form of *conditions*, *actions/interactions* and *consequences*. Categories are then related to their subcategories along the lines of their properties and dimensions, in order to form more precise and complete explanations about phenomena, integrating process with structure.

1. In this analysis, *conditions* describe the elements of the security implementation, employee knowledge and beliefs that drive security behaviours.
    a) *Causal conditions*: represent sets of events that led to the occurrence or development of a phenomenon.
    b) *Intervening conditions*: mitigate or otherwise alter the effect of causal conditions on phenomena.
    c) *Contextual conditions:* are the specific sets of both causal and intervening conditions that intersect dimensionally at a specific place and time to create the set of circumstances to which employees responded through actions/interactions.
2. *Actions/Interactions* are specific behaviours of employees that resulted from the identified conditions.
    a) *Strategic actions/interactions* are purposeful or deliberate acts that are taken by people in response to issues, problems, happenings or events that arise under the contextual conditions.
    b) *Routine actions/interactions* are more habituated ways of responding to occurrences in everyday life.
3. *Consequences* are the conditions resulting from identified actions/interactions (employee behaviours) that increase security risks for the organisation (for a full list of these please see the axial coding results in Appendix G). It is important to note here that, in this research, lack of action by employee (i.e. choosing to do nothing) is also considered an action by itself.

Axial coding example: Security slowing down production tasks

Conditions: Problems in organisational security mechanisms (slow VPN, slow encrypted USB drives and slow SharePoint access setup), combined with problems in security processes (slow access control setup, IT support and password resets) and employees caring more about productivity than security.

Actions/Interactions: Use of unencrypted USB drives, Copying data locally on laptops, USB and email-based file sharing, Password sharing, Frustration with security

Consequences: Increases employee perceived need to come up with ad-hoc solutions that minimise the impact of high-cost security, Increases data leakage risks, Reduces perceived security usefulness

3.5.2.2.3 Selective coding

This stage integrates and refines the theory. It is an iterative process and is validated by continual comparison of coding results with the raw data to confirm or refute the conclusions that are being made. A specific narrative is created based on the identified consequences from axial coding and a *core category* is chosen: the central phenomenon around which all related categories are integrated. A *story line* is then created: a descriptive narrative about the central phenomenon of the study, created around a core category by means of its properties.

Once the selective coding stage is finished, it is possible to take the analysis one step further by integrating *process effects*. These describe the sequences of actions/interactions which can be traced back to changes in structural conditions and which might themselves change these structural conditions, possibly resulting in further actions/interactions. This stage can also identify gaps that need to be filled by further research.

3.5.2.3 Applying the grounded theory process

For the work presented in this thesis a combination of open, axial and selective coding was used. The preliminary thematic analysis of Phase 1, in combination with the literature review findings, provided some specific starting points for the subsequent research. These were used as starting themes to drive the analysis, but an open coding process was also conducted, aiming to identify potential employee behaviour paradigms missed by the analysis in Phase 1, better understand relationships amongst emerging categories and generate sub-categories. All the coding was done using the software tool atlas.ti, which was also used for code comparison, code re-use across interview sets, also allowing for the creation of a code repository that was later used by other researchers for further analysis.

3.6 Research ethics

The nature of data collected for the research presented in this thesis (access to organisational confidential information, potential risk for individual employees reporting insecure behaviours if they can be later identified by the organisations, and potential unwillingness of employees to report those behaviours), created a number of ethical considerations that had to be considered to prevent potentially severe consequences for research participants, the researcher, the Information Security Research Group and the

university. This section explains how the ethical principles by professional bodies from both the scientific disciplines related to this work (information security and psychology), the ethical guidelines of the UCL Ethics Committee, and a set of personal ethical principles were used to reduce the impact of potential ethical implications.

3.6.1 Code of ethics

3.6.1.1 Professional codes of ethics

University College London's ethical guidelines suggest that researchers should follow recognised codes of conduct suitable for their research specialism ("UCL Research Ethics Committee"):

- The British Computer Society ("BCS Code of Conduct", BCS, 2011) and the Institute of Information Security Professionals ("The IISP Code of Ethics", IISP, 2007) codes of conduct ask their members to respect the privacy of others, accurately reporting research findings and upholding the reputation of the profession.
- The British Psychological Society's ethical code ("BPS Code of Ethics and Conduct", BPS, 2009), is mostly concerned with respecting the confidentiality/anonymity of research participants, eliminating potential unwanted consequences from their participation and acknowledging others for their contributions to any literature/findings reported.

3.6.1.2 Personal ethical principles

In addition to the university and professional ethical principles, the researcher has also recognised the need for a set personal ethical principles that drove collaboration with other researchers and the organisations. Based on previous experience working in research environments during other postgraduate level research projects, combined with knowledge acquired through a taught course on Ethics in Security Research, a set of personal ethical principles were created:

1. *Be fair to colleagues, students and supervisor*: Give credit where it is due and only claim credit for what the researcher has worked on.
2. *Know and follow the rules*: Set by the university, research council and discipline-related professional bodies. When disagreeing with a rule, report it instead of breaking it.
3. *Ask for support when in doubt*: By colleagues, supervisor and any relevant resources the university provides (e.g. academics at other departments). Assuming good knowledge of issues outside the researcher's expertise and research discipline can result to costly mistakes.
4. *Avoid shortcuts when under pressure*: If it is not possible to produce quality outputs due to limited time/resources or tight deadlines, consider whether research could be improved and take the time to do so.
5. *Prevent potential for dual use and consider impact of research on individuals and society*: Take additional care when improper dissemination of research outcomes can present a danger to individuals or society; when this potential exists, devise strategies to deal with it.

3.6.2 Ethical analysis

Based on the aforementioned principles, a range of ethical issues were identified in relation to this research: (1) Need to safeguard collected information, (2) Need to preserve employee anonymity, (3)

Adherence to Non-Disclosure Agreements (NDAs) signed between the university (represented by ISRG) and the collaborating organisations, (4) Respect employee rights when suggesting solutions to identified problems, (5) Accurately report and avoid fabricating results, and (6) Accurately present sources of information. This section discusses the potential impact of these issues on the work presented in this thesis and presents potential courses of action to minimise potential unwanted consequences, while minimally affecting the ability to communicate and apply research findings.

3.6.2.1 Safeguard collected information

One of the most important challenges encountered while conducting this research was the need to safely store and transport collected datasets. This was important to ensure no unauthorised disclosure of potentially sensitive corporate information could happen while transferring or analysing the data collected.

- *Stakeholders:* Researcher, other ISRG researchers, employees and management of the organisations, university.
- *Pressures:* Need to quickly transfer interview data to transcription service. Limited time to do analysis sometimes required to work away from the university.
- *Choice of ethical actions*: Audio interview data was transferred to encrypted USB drives (2 per interview location for backup reasons). Transfer to the transcription service was done through a secure connection; same for return of the text transcripts. The transcripts were then continuously held on university servers, which are heavily firewalled and protected against unauthorised access. Transcripts were then anonymised: employee names, office locations and company names were all removed from the transcripts to avoid any possibility of someone relating back to the organisation[15]. Original manuscripts were held on encrypted drives and all subsequent analysis was performed on the anonymised versions.

3.6.2.2 Preserve employee anonymity

Respecting individual employee privacy was also an important consideration during data collection and analysis. Any potential for the partner organisations being able to link identified undesired behaviours to individuals had to be eliminated; if this happened, it could undermine potential participation in future studies and also damage employee reputation within the organisation, which is against the ethical guidelines presented by BPS.

- *Stakeholders:* Researcher, employees and management of the organisations, university.
- *Pressures:* The organisation may have asked to talk to individuals that reported to resort to behaviours deemed as risky.

[15] As previously discussed, Company A data was already available when this research commenced. As a result, it was not anonymised when the analysis processes presented in this thesis commenced, but any sensitive information that could lead to company or individuals becoming identifiable was removed during the analysis and excluded from results reporting.

- *Choice of ethical actions*: Care was taken to safeguard employee information obtained through data collection and avoid providing the organisation with information that can make any employee potentially identifiable (this is also required by the Data Protection Act, DPA, 1998, and also the BCS and the BPS codes of conduct). Consent was obtained from participating employees, who were also assured on their anonymity and confidentiality of information. Employee information was only stored on university servers and all employee identifiers were removed from subsequent reports and publications.

In the end, no significant risks arose on this. The organisations interested and participating in this research had already recognised the importance of improving understanding of employee security behaviours and the potential benefits of this research towards that. As a result, they were very willing to collaborate without following up reported outcomes with their employees.

3.6.2.3 Adhere to Non-Disclosure Agreements (NDAs)

NDAs were signed between collaborating organisations and the university. Those aimed to legally bind the university to take adequate care to prevent leaks of confidential information about internal security processes and the organisation's structure that attackers could use to attack it. Adhering to NDAs signed also protects the reputation of the university as a trustworthy institution that can help industry collaborators solve important problems. The sensitive nature of the findings of this research also run the risk to be misreported by media, damaging the reputation of any involved organisation. As a result, care had to be taken to not report information that the organisation considered to be sensitive.

- *Stakeholders*: Researcher, supervisor, university/other universities, collaborating organisations.
- *Pressures*: By the researcher's host department to advertise their relationship with industry, as that increases the impact of emerging research and knowledge, improving potential success of future funding attempts. Also by the organisation not to provide anyone with information that can be potentially used to target them. Also, as a researcher and a research group, emerging findings and knowledge needed to be published for academic reasons
- *Choice of ethical actions*: A compromise was required between publishing research outcomes and excluding sensitive information from publications. Discussing this with partner organisations, they agreed for the collected data to be used in research and publications. They did not ask to review those publications but, as an act of goodwill, draft versions of research reports were sent to them to ensure no parts of the reported findings were considered sensitive. They were also encouraged to request exclusion of anything they deemed as sensitive, but chose not to do so. This left the researcher with publishable outcomes and also benefited the relationship of ISRG with industry partners, who are still in active collaboration with it. In addition, anything included in the publications was analysed and discussed thoroughly amongst ISRG members to ensure it could not be misinterpreted in media publications.

3.6.2.4 Respect employee privacy in suggested solutions

The sensitivity of the research topic (employees reporting behaviours that deviate from organisationally-prescribed ones), also required ensuring that research outcomes would not be used by the organisations to drive implementation of more stringent security measures. The participation of UCL members in such a

research should not be linked in any way by employees to the implementation of further security restrictions; something that can lead to a negative perception and an overall loss of trust in university research.

- *Stakeholders*: Researcher, research group, university, organisations.
- *Pressures*: Organisations may be looking for ways to identify misbehaving employees and use findings to impose excessive monitoring.
- *Choice of ethical actions*: Suggested solutions to problems identified always respected employee privacy, avoiding suggesting measures that includes excessive monitoring of employees (*"Respect Rights of Third parties"*, BCS). Instead, improvements in the design, usability and applicability of existing security mechanisms and processes were recommended to improve compliance with security (*"Promote best practice in InfoSec, recognise potential for conflict of interest, take steps to avoid and resolve such conflict",* IISP).

3.6.2.5 Accurately report and avoid fabricating results

Two potential sources of pressure to produce "desirable results" existed. Firstly, organisations sometimes want research findings that justify decisions they plan to make in the near future, so they could have asked to present the data differently than what this research intended to. Secondly, the large amounts of time and effort required to collect and analyse the data for this research created pressure to "make something out of it", even if the results were not significant i.e. not improving existing knowledge on employee compliance.

- *Stakeholders*: Researcher, supervisor/colleagues, collaborating organisations.
- *Pressures*: Need to produce results both for the researcher's and ISRG's publication lists, but also for research projects that enable (and funded) data collection and analysis.
- *Choice of ethical actions*: No misrepresentation of information was done. (*"Do not misrepresent or withhold information on performance of systems or services",* BCS). Fortunately the emerging findings were useful for the collaborating organisations (and were used to implement improvements in their current security implementations), but also generated significantly important research insights that led to a number of academic publications (See related publications section in Appendix A)

3.6.2.6 Accurately present sources of information and refer to pre-existing work

The university is extremely sensitive on plagiarism issues (UCL 2011). Failure to comply with university anti-plagiarism guidelines could affect the researcher's ability to complete their degree.

- *Stakeholders*: Researcher, supervisor
- *Pressures*: Not citing or clearly presenting past research results to present emerging findings as original and unique. Avoid referring to related work published while data collection or analysis took place, in order to increase the perceived impact of this work.
- *Choice of ethical actions*: Ensured inclusion of clear reference to the sources of any information reported in this thesis. Also closely followed conferences, journals and other researchers in the field of user-centred security and security management to ensure adequate awareness on

publication of related work. When related work was published, its relation and impact to this work was well presented, analysed and the new knowledge was incorporated into the work presented in this thesis.

3.6.2.7 Conclusion

The multidisciplinary nature of this research required considering a number of ethical principles from various disciplines during data collection, analysis and reporting. The ethical actions presented to address the identified ethical issues were based on principles from professionals in computing and psychology, the university's ethical guidelines and the researcher's personal ethical values. Adhering to those often required additional time and effort investment, but it provided significant advantages: (1) it protected the researcher, supervisor and the university from potential reputation and legal problems, (2) it protected participants and the collaborating organisations, and (3) it improved the validity of the reported results, reducing the risk of other researchers challenging the validity of the findings of this research.

Chapter 4: **Security behaviour drivers**

The literature review chapter identified a significant gap in the existing understanding of security behaviours and the drivers of non-compliance and insecure behaviours in organisations. This revealed the need for deeper, exploratory investigation of employee interaction with security mechanisms, their corresponding behaviours and their effect on organisational security risk exposure. In order to improve existing knowledge on the above areas, a set of research questions were defined in section 3.3.1.1, to which the research presented in this chapter attempts to provide preliminary answers:

1. *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?*
2. *What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?*
3. *How can the improved understanding from the previous question be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?*

In order to answer the above questions, a preliminary understanding of the phenomena of interest was required, to drive the subsequent grounded theory analyses. In order to identify and describe those phenomena, an initial in-depth thematic analysis was conducted on a subset of 30 randomly selected interviews from Company A. Thematic analysis was chosen as an appropriate analysis method, as it allows enriching understanding of unknown phenomena (Braun and Clarke, 2006). This analysis aimed to understand (1) the context in which the interaction of employees with elements of organisational security takes place (mechanisms, policies and processes) and (2) employee experience of the interaction with those elements and related behaviours. The analysis process was based on the approach defined by Braun and Clarke (2006), as presented in section 3.5.1, with the interview transcripts analysed without trying to fit them into a pre-existing coding frame. This allowed extracting bottom-up devised narratives describing employee behaviours, also leading to the formulation of additional research questions. Both the emerging narratives and the updated question set allowed carrying out the subsequent grounded theory analysis on the full interview sets from both Company A and Company B, allowing for in-depth examination of the research gaps presented in section 2.8 and the validity of study propositions, presented in section 3.3.1.3.

This chapter presents the thematic analysis process followed, discusses emerging codes and themes and explains how their identification led to the two main contributions of this chapter:

1. Characterisation and categorisation of non-compliant behaviour drivers, based on the conditions that led to their emergence
2. Identification of a third category of security behaviours, extending the existing binary understanding of it (compliant or non-compliant behaviours): employees devising own security solutions outside the control of security managers.

This chapter also creates a preliminary model of employee security behaviour, discusses the implications of the improved behaviour understanding for organisational security management, and explains how the findings were used to drive the research presented later in this thesis.

4.1 Familiarising with the behaviours represented in the data

The first phase of the thematic analysis process requires identification of *start codes* to initiate the analysis. An initial set of start codes was devised based on the research questions, areas of interest to the partner organisation, organisational security policy and a preliminary reading of the 30 interviews. The start codes that emerged covered a wide range of elements of the organisational security implementation (Table 5).

Start code	Meaning	Source/Justification
Understanding of the need for security	Employee understanding of their role in security protection and how misusing information can damage the organisation	Identify employee understanding of the need for information security and their responsibility in helping the organisation to remain secure (this was included in organisational security communication)
Policy/mechanisms knowledge and awareness	Understanding of organisational measures implemented to protect information and how to use those for security risk mitigation	Assess employee ability to relate perceived need for security to existing organisational security policies and mechanisms
Screen lock	Behaviour in relation to the organisation's screen lock policy	Investigate employee experience and compliance with policy clauses requiring them to lock their computer screens when going away from their machines
Clear desk policy	Behaviour in relation to the organisation's clear desk policy	Policy states that desks should be cleared from all documents and equipment at the end of working day
File handling and sharing	Information storage, transferring, backup and sharing practices around the organisation	Need to identify and understand employee practices on information handling Policy: only share on "need to know" basis, take care with sensitive information, not export to third party sources
Laptop usage	Practices on handling of corporate laptops, information stored on them and security precautions taken	Laptops are the main work tool of most employees in the office and remotely - employees often work remotely Policy: not to install application software or programs unless they have explicit authorisation to do so for business reasons
Password behaviour	Selection of passwords, strategies to deal with multiple passwords for corporate systems and the need to change some of those over regular intervals	Policy states employees must not write passwords down or share passwords and that they will be held accountable for any actions attributed to their accounts Identify conditions that led to policy violations
Email filtering and website blocking	Employee experience and corresponding behaviours of corporate systems for website and email filtering	Policy states organisational systems should not be bypassed
Physical security	Willingness to challenge potential strangers present in the office	Policy that all visitors should have a badge and are accompanied by a member of staff
Physical document handling	Handling of physical documents (where are they stored, shared, destroyed)	Information sensitivity awareness and its effect on physical information handling
Organisational security perception	Overall assessment of the organisational security implementation	Identify employee perceptions on the state of security around the organisation (both organisational provisions to address perceived risks and colleague security related behaviours)

Table 5: Start codes for the thematic analysis

4.2 Code generation

Start codes were then assigned to parts of the text, identifying features of the data (semantic content or latent) that reflected instances of user behaviour or the organisation's security implementation related to the research questions asked. New codes were also devised when required, either as modified start codes, sub-codes of those, or new codes, to better capture the concepts represented in the data. In total,

143 codes emerged, describing the security mechanisms employees had to interact with, the various challenges they faced while doing so and corresponding behaviours. To improve code validity and ensure all instances related to the research questions were captured, an iterative analysis process was followed: after the initial code generation, a confirmatory analysis led to code refinement, also ensuring coding consistency and identification of behavioural patterns missed by the first analysis. The codes were also reviewed by another member of the Information Security Research Group[16] and their remarks and questions on the code set where addressed during the validation analysis. The final list of codes, together with themes, relationships between themes, and theme categorisation (described in the next section) can be found in Appendix F.

4.3 Combining codes into themes

Examining the final code list, 13 behavioural themes emerged, describing the narratives emerging from the data: codes referring to the same behavioural instance, mechanisms or conditions, were grouped under the same theme to provide a richer understanding of the identified conditions or behavioural patterns. To strengthen theme consistency and accurate representation of the observed behaviours, a confirmatory analysis of the 30 interviews was done to verify and fine-grain the emerging themes, based on the improved knowledge that emerged from the first analysis.

4.4 Theme review, definition and naming

Emerging themes were then assigned meaning and definitions, based on the identified instances in the data, and were also grouped in categories. For example, the *Email filtering and website blocking* theme was defined as *Problems in primary tasks created by organisational information filtering systems and corresponding employee behaviours* and was included in the *Security mechanisms* category (full code and theme list together with definitions in Appendix F).

Theme Example: Email filtering and website blocking

Codes included: Email filtering inconsistent, Website blocking causes problems, Website blocking annoying, Download information at home, Own assessment of external content security, USB use at home

4.4.1 Theme category creation and grouping

The emerging themes were then grouped in three distinct categories (Table 6):

1. *Security awareness and understanding*: Themes related to employee awareness, policy understanding, training and communication provided by the organisation and overall organisational security culture (Example theme: *Employees downplaying information security*

[16] Dr Simon Parkin provided valuable feedback on the emerging codes, their naming and grouping, and also how well they managed to capture behaviours of interest presented in the data

risks, describing instances where employees were dismissing the potential for the information they use to be misused by someone and damage the organisation).

2. *Security implementation*: Themes related to elements of the existing security implementation creating problems for employees either in their primary tasks or in their attempts to behave securely (e.g. email and website blocking discussed above).
3. *Security behaviours*: Employee behaviours emerging from the presence of insecure habits, inaccurate perceptions or restrictive security mechanisms (e.g. *Responses to inconsistent or restrictive website blocking and email filtering* describing employee behaviours like downloading information they needed for work purposes at their home computers and bringing it in the organisation using personal, unencrypted USB flash drives).

Theme category	Theme	Definition
Security awareness and understanding	Awareness of the importance of information security	Understand of the importance of organisational information Recognition of the need for mechanisms and processes to protect it Understanding their role in keeping the organisation secure
	Downplay own responsibility	Employees downplaying their role in organisational protection
	Security experience and perception	Employee experience with organisational security provisions and perceived adequacy in effective risk mitigation
Security implementation	USB stick use	Practices on the use of USB sticks to store and transfer information
	Email filtering/Website blocking	Experience of interaction with organisational systems for information filtering (email, internet traffic)
	Enforcement and sanctions	Experience with sanctions for insecure behaviour and other policy enforcement approaches
	Security helpdesk experience	Interaction and perceived usefulness of organisational security helpdesk
	Policy communication and training	Experience with communicated information Appropriateness of corresponding communication methods Perceived usefulness of the communicated information
Security behaviours	Physical security	Behaviours regarding policy requirements to challenge strangers and prevent unauthorised access
	Laptop usage	Awareness of the need to protect corporate laptop Actions taken to prevent potential laptop theft
	Screen lock	Practices regarding policy requirement to apply screen locking when away from their computers
	Password use	Behaviours regarding selection of passwords, steps taken to remember those, password sharing conditions and behaviours
	Document handling	Storage and sharing of information practices, use of personal computers to work on corporate information Physical document treatment Clear desk compliance

Table 6: Themes that emerged from the analysis

4.4.2 Theme relationships

A number of causal relationships were also identified between the emerging themes. These captured cause-and-effect relationships between security implementation elements and corresponding employee behaviours; for example where high-friction security (e.g. a mechanism difficult to use) led to behaviours

either contradicting the security policy of the organisation or increasing security risks[17]. Those relationships are represented with many examples later this chapter (section 4.6).

The remainder of this chapter presents the themes emerging from the analysis and uses those to describe how elements of the organisational security environment influence employee behaviours. It also presents a categorisation of identified insecure behaviours together with emerging risks and potential ways to alleviate those, discusses lessons learned and provides starting points for the research presented in the later chapters of this thesis.

4.5 Results: employee behaviours

This section presents employee security-related behaviours that emerged from the analysis, together with corresponding security policy clauses and examples from the interviews for each of the identified behavioural paradigms.

4.5.1 Awareness of the importance of information security

Company A's security policy asked employees to:

1. "*Be familiar with the provisions of, and process personal data in accordance with, the applicable data privacy legislation and relevant company policies and procedures*"
2. "*Keep personal data confidential and not disclose it to any person unless authorised to do so by the company*", and
3. "*Consider very carefully who needs to receive the message and do not unnecessarily copy people in. For example, send only to those who have a need to know.*"

The consequences for employees were also clear "*Failure to comply with all security policies may lead to disciplinary action and unlawful or illegal conduct may lead to separate criminal or civil proceedings.*" Examining reported employee understanding, sufficient awareness of the sensitivity of organisational information was identified amongst employees: in all the 30 interviews, employees were aware[18] about the problems that could arise from potential misuse or leak of sensitive organisational information to unauthorised sources, both from a security and a commercial perspective. They described how

[17] It is important to note here that, despite the main purpose of this thesis being to investigate drivers behind non-compliance with security policies, it was beneficial to also identify risky behaviours not captured within the examined organisations' security policy. This was based on: (1) sufficient documentation in literature examined in section 2.3 that organisational policy formulation processes are not always effective in capturing many potentially dangerous employee behaviours. Our partner organisations were open to suggestions for improvement and policy changes were a part of it. (2) This research aimed to improve understanding on many topics were knowledge is limited. Assuming effective coverage of security behaviours in policies contradicts identified research gaps

[18] When discussing interview findings the use of "were" refers to employee behaviours where sufficient evidence was provided in the interviews about their existence

information could provide advantages to competitors, damage organisational reputation and negatively affect the service providing abilities of the organisation.

P7: "*I think it's the security of information between us and other suppliers. Because it's all about our competitive environment. […] So I'd say the security of information - it's kind of commercial information, is the biggest kind of way security comes up in my day-to-day job.*"

In addition, all 30 employees mentioned that information sharing within the organisation should only be done on a "*need to know"* basis, also referring to the need to comply with regulations on information separation across different organisational divisions.

P19: "*Because we're regulated, we're not allowed to share any information with* [other business division][19]. *So we're not allowed to share any information with other parts of the business to make sure everything's fair*"

Employees also recognised potential consequences they could be subject to if their actions led to leakages or losses of sensitive information.

P26: "*I'd probably be more worried about the implications on myself. I don't think the company would be impacted that greatly, but it wouldn't be good.*"

They mentioned that potential security problems arising from their actions could negatively impact their careers, either from shaming within the organisation getting them into trouble with their colleagues or managers, or through potential sanctions imposed on them. This feeling was accentuated by the warnings given to themselves or their colleagues, or when they observed sanctions enforced around the organisation, with 9 of them (30%) mentioning the above influenced their security behaviours.

P2: "*I generally not run the risk because I think sometimes the policies can be a bit strong but I've never had any problem with this but maybe I'm over-cautious. But some of the stories that I have heard about people who have been suspended for doing something that actually sounds quite, relatively minor.*"

In general, employees understood the importance of organisational information, recognised the need for mechanisms and processes that aid protection of information within the organisation, and they understood their contribution in keeping the organisation secure.

4.5.2 Policy communication and training

Employees were aware of some parts the security policy (e.g. screen lock, clear desk), but in other areas, (e.g. use of USB sticks, password sharing) they were unaware of policy existence (P16: "*Well, I mean, common sense would say no but I've never seen a policy that says, don't write your password down, or if*

[19] Division name removed to avoid disclosing nature of organisation's operations.

I have, I can't remember having seen it, but clearly, you know I wouldn't do that anyway."), or appeared to ignore or be confused about other aspects of it (e.g. P27 discussing password policy: "*No, it says you can write them down*). 13 (43%) employees mentioned that security policy is too long to read and remember, with many clauses being irrelevant to their roles. 5 (17%) of them referred to policy as "common sense" and that they "know where to find information if needed".

Examining the reasons for the lack of policy awareness, a number of problems were identified in both organisational security training and communication:

1. Inconsistencies were identified in the way the security policy is communicated. 10 employees (33%) reported security communication is done in emails "*among other things*" (P19) and "*is not read by everyone*" (P27).
2. 15 (50%) employees reported that, from the information communicated to them, information security appears to be less important for the organisation than health and safety and physical security. "*P16: the building security is more of a concern um rather than the IT. Because obviously we want to get them into the building first off. But then we direct them to the InfoNet sites where the security pages are and we tell them to read through the documents. Um, they hand back a checklist at the end of it to say that they've done that. I mean, who knows whether they have*."
3. Training was also reported as scarce and ineffective. P29: "*apart from what their induction does, it doesn't seem like you have any other refreshers stuff, which probably would be a good idea, but I think sometimes IT security is seen as something that's a bit of a pain and most of the time rather than something that's helping you, you don't really see the end game*". In addition, they mentioned it is mostly based on employee/team initiative: P22: "*A typical first day for our contractors new in they would probably have a day with our team sort of admin person in the wider team*."

The overall comments on organisational security policy content and corresponding communication were that it is full of vague clauses (e.g. "keep information confidential" but also "share when authorised", or "use appropriate encryption"). This led to inaccurate or insufficient understanding of the purpose of information security in the organisation and a confusion on what the desired behaviours were: some said sharing passwords is acceptable, others not; same with writing those down (see section 4.5.6 below). In general, employees appeared unaware of many aspects of organisational information security policy, despite organisational security communication and some training being in place.

4.5.3 Downplay own responsibility

Despite the identified general awareness of the sensitivity of organisational information and knowledge of security policy contents, employees failed to make a connection between that awareness and knowledge and the information they dealt with as part of their day-to-day jobs:

- Only 13 (43%) employees mentioned that they consider information security as something they need to be aware of while proceeding with their primary tasks and take actions to protect the organisation.

- But a group of 7 (23%) employees mentioned that no information security implications exist in their job; P25: "*just some confidentiality issues*" that require them to be careful when working with confidential data.
- 8 employees (27%) downplayed their role in keeping organisational information secure, either by downplaying the impact from leakages of the information they handle (P7: "*I guess it's menial, but no one's gonna bring the whole country down from work I have on my computer […] security measures [are] more about regulations and commercial sensitivity of information*"), or by claiming that more than one compromises are required to get useful data (P11: "*Generally there's not a big issue in the stuff I deal with. […] You'd have to understand a bigger picture than I've got. […] you'd have to know a bit more of the jigsaw puzzle to be able to say what that piece of information meant.*").
- 17 (57%) perceived the information they handle as not commercially sensitive or of limited interest to anyone outside the organisation; P1: "*I think as far as Company's concerned everything is confidential. I personally can't see what possible use most of the stuff I deal with would be to anybody else whatsoever, outside of the Company, even outside of our department*", also referring to their corporate equipment (laptops, phones etc.) as "*not interesting*" (P18) information-wise and that someone "*would not significantly benefit from intercepting emails*" (P2). One employee even said their colleagues are "*surprised when told not to share everything with everyone else around them*." (p16)

In general, despite the identified understanding of the sensitivity of organisational information, employees downplayed their role in organisational protection: they perceived the information they handle as generically non-sensitive, which acted as a driver for a wide range of insecure behaviours, described later in this section.

4.5.4 Screen lock

The security policy mandated that employees "*ensure that the screen lock facility on your computer is engaged when leaving your desk unattended*". The majority followed this, with 20 of them (67%) mentioning they usually do it. When asked to discuss where motivation for this behaviour came from, 2 employees (7%) mentioned the open plan office space and 8 others (27%) mentioned peer pressure from their colleagues: P8: "*…I remember one of my old bosses left his screen unlocked one time, so I think his boss then sat down and started typing his resignation letter in the e-mail and then locked his screen, and let him come back to it*". Despite this, 8 employees (27%) reported they often do not lock their screens, either because they forget (4 – 13%), because the associated risks are low (2 – 7%) (P29: "*I sit at the same desk every day, around the same people. So if somebody else was to wander in and sit at my desk, it would be pretty obvious*"), or because they wait for automatic locking to kick in after a few minutes (1 – 3%) P15: "*in general, that's not bad. Plus I think the thing has a 5 or 7 minute timer, it just…automatically locks*". In general, motivation to lock screens was driven both by risk understanding and peer pressure, with policy violations stemming from either human error (forgetting to do so) or lack of appropriate risk understanding.

4.5.5 Laptop usage

Employees were given corporate laptops and are asked in the policy "*not to install application software or programs unless you have explicit authorisation to do so for business reasons*", without reference to additional need to protect those laptops. This appeared not to be a problem for employees, as their laptops were closed-built, not allowing installation of software, unless approved by technical support (6 – 20%). It was also reported as a general practice to take laptops at home 23 (76%), usually for productivity reasons (P1: "*may need to work from home during the evening*", P4: "*may not be able to come in the next morning*" or P2: "*may need to go to a different location*") and security (P3: "*feel safer taking the laptop than leaving it in the office*") reasons for this. Despite not being part of the policy, employees discussed the need to protect their laptops while on the move, and took appropriate actions to reduce the potential of physically losing or having those stolen: 16 employees (53%) mentioned that they take risk mitigating actions, with a number of different practices being reported (lock it in car boot, make sure it is not obvious they carry a laptop, hide it somewhere when leaving house). A smaller number (4 employees, 13%) mentioned that travelling with a laptop is too risky so they avoid doing so unless it is an absolute necessity (P8: "*as unregularly as possible, or as little as possible*"). Overall, employees took various self-devised actions to physically protect their company laptops, even if such actions were not mandated by the security policy.

4.5.6 Password use

4.5.6.1 Password choice and handling

The organisation has a number of different systems which employees need to access during their day-to-day tasks; with many of those requiring different user ID's and passwords. The security policy included a number of clauses on passwords: "*Keep all authentication credentials secure and must not write down or share passwords or token on their accounts – Users will be held accountable for any actions attributed to any account/uid they are responsible for*", also stating that "*not knowingly access or seek to access data using authentication credentials that they are not authorized to have, e.g. by using another user's user identifier and password*", but also including ambiguous clauses on password sharing: "*users must not access any information or system using another employee's or system's password unless explicitly authorised to do so.*" When probed to discuss authentication to organisational systems, employees reported that the number of different passwords for various organisational systems made password management (choosing them and remembering them) a challenging task. To cope with this, they developed a number of strategies:

1. 11 (37%) employees reported that they write down their passwords either (a) on paper (7 employees, 23% - P8: "*I just find there's too many to remember otherwise and we've got a different username and password most of the time for each of the logins, so […] it's written down on a bit of paper. It's locked in my desk when I've not got hold of it, probably along the laptop, which is probably not too clever thinking about it*") or (b) in electronic form (in a word document – 1 employee, or on their PDAs – 2 employees - P26: "*I've got a Microsoft Word document, which is 5 pages long now that contains passwords for everything. […] But mostly work cause I don't do a lot of stuff on the internet personally. And the amount of password-protected things…leads you to the necessity to write them down, which introduces a risk.*")

2. 7 (23%) employees reported that they use the same password for more than one system. Some do so only for rarely used ones, where remembering all required passwords is not possible; others do it for all they have to use. This was reported as a way to avoid having to write their passwords down (P25: "*I come from the school of the same password for as many things as possible rather than having them either physically written down or put into some sort of document somewhere.*")
3. One other though, reported that writing passwords down is allowed by policy! (I: "*Does it also say in the policy you're not allowed to write them down?*" P27: "*No, it says you can write them down.*")

4.5.6.2 Password changing

The organisation requires employees to change their passwords over regular time periods, which accentuates the problem of multiple password management: it imposes a large compliance overhead on employees, turning password management to a problem that requires significant time and effort investment. In some cases, it also leads to employees being locked out of systems, thus negatively impacting their ability to proceed with their primary tasks, but also creating frustration. As a response to this, employees developed different coping mechanisms:

1. 5 employees (17%) who used the same password for more than one system said they change all passwords together when one expires. I: "*And do you change them all at the same time even though they probably don't all have to be changed at the same time?*" P1: "*Yeah, change them all at the same time*".
2. 15 employees (50%) developed their own, simple password-change strategies. 9 of them for example (30%) reported that they change only one digit of the password when required (e.g. change "Password.01" to "Password.02"). Others mentioned they keep the password the same and add the existing month at the end (e.g. P15 realised that a system prevented the use of the current month as a password, so they started using *Summer01* for June, *Summer02* for July etc.)

4.5.6.3 Password sharing

As discussed earlier in this section, Company A's security policy explicitly prohibited sharing passwords, but also included contradictory clauses like: "…*unless explicitly authorised to do so*". A group of 7 (23%) employees mentioned they do not share their passwords, as they cannot be sure who to trust and they are not willing to take the risk of getting in trouble from potential credential misuse (P15: "*…from a point of view of if you're asked to give your password then really it doesn't matter who it is, whether it's senior management, the philosophy within the company is you shouldn't be asked and if you are asked you should have the right to say no without any recrimination. Um, there is a policy in place and it's there to protect you and to protect others*." or P29: "*Sometimes it comes up as a bit of any solution and I've always refused to do that actually. More for personal reasons I would say. Not because I think there's particularly a big corporate risk, for my own risk it's a significant risk to take.*")

Despite policy prohibiting password sharing, 15 employees (50%) reported that in a number of cases they needed to access systems for which they did not have an account set up (either because they were new to the organisation or because they had no need to use that specific system in the past). In those cases, the necessity for quick access meant they had to share passwords with their colleagues, as access right setups

"*take ages*" (P8) and "*colleagues have been unable to work for weeks*" (P20). This group acknowledged password sharing as a risky behaviour and, despite feeling uncomfortable, they still did it (e.g. P6: "*... sometimes people don't have access to information or systems that they need to do their job and therefore they're shared within teams. And I flagged that before that it shouldn't happen but it does, because it can take so long to get something through that they might need to do their job. So it would be, "Use somebody else's account." […] so that you can learn the process and do the process yourself*" or P12: "*Well, I've never had to but, like I said, we had a person off long-term sick and we needed to access some information that without it a £6 million contract wouldn't have been awarded so we knew the risks and we, we had to do it*"). Employees in this group also mentioned that only those who should be allowed access to a resource should be given a password (P18: *Within the small pricing team, it's giving that two or three people who would need access to those to share the password*"); none of them mentioned they were "…*explicitly authorised to do so*", as the company policy demanded though. In addition, "*generic accounts exist on rarely used systems*" (P14) that reduce potential for accountability of actions. In general password sharing appeared to be the only way to access systems when urgent access was required and no organisational provisions existed to provide that access through official channels.

4.5.6.4 General comments on password behaviour

Overall, employee password behaviours were varying and divergent from organisational policy. They set all their passwords to the same and easy to remember ones to improve memorability, changed those at the same time, wrote those on paper, stored those in documents and shared those with their colleagues when they needed quick system access. The reported practices create a number of problems and risks for the organisation:

- *Single password security*: Using a single password for all systems reduces the security provided by multiple passwords, as a compromised password can be reused to access all systems the password owner is authorised to do. The risks may be even higher if employees reuse the same password for personal purposes: potential compromises of personal accounts (combined with the fact that some may use personal email for work purposes – see section 4.5.9) can increase security risks for the organisation.
- *Simultaneous password change:* This is an effective strategy to improve employee ability to recall their passwords for various systems, but consumes significantly more employee time than a single password change, increasing the employee effort required to manage the organisation's security mechanisms.
- *Writing passwords down*: This reduces the additional security different passwords provide to a single point of failure. To gain access to a number of different organisational systems, a potential attacker only needs to gain access (either physical or electronic) to the document where the passwords are stored, which is only protected by what employees perceive to be the most appropriate way to do so.
- *Own password devising mechanisms - simple change*: e.g. "*Summer01*" example presented above. Banning words like "*Summer*" from passwords allowed could eliminate this practice, but any implementation based on banned words should not underestimate employee ability to come up with something that can pass the formal security rules, while still being severely insecure.

- *Password sharing*: Password sharing increases risks for system misuse, also leading to reduced accountability in case employee behaviours need to be followed up, especially if such sharing was authorised by managers. The risks of this practice can be amplified when passwords are shared across many systems.

In general, having many passwords that require frequent changes turns password management to a problem that requires a significant time and effort investment from employees. The emerging risks can be significant for an organisation and are also increased by slow setup of system access that encourages password sharing, for employees to be able to proceed with primary task activities.

4.5.7 Document handling

Another theme that emerged from the interview analysis was employee handling of documents containing organisational information, both in digital and physical form. This included behaviours in relation to document storage, sharing, handling of physical documents and clear desk requirements, also including the use of personal computers to store, transfer or work on corporate information.

4.5.7.1 Document storage

The security policy asked employees to: "*Keep personal data confidential and not disclose it to any other person unless authorised to do so by the Company.*" Each employee was assigned personal storage space, locally mapped on their company laptop (usually under the drive letter H://), also continuously backed-up by the organisation. That drive is only accessible when people are logged on the network, either on company sites or from other locations using VPN access. In the interviews only 3 employees (10%) reported to store data solely on the network mapped drives, providing security and automatic backup reasons for this. P6: "*Well the H drive replicates so there's an automatic mirror of that somewhere. So I guess even if the laptop got destroyed then I could probably still have my Outlook and my mail.*" All other employees stored many documents locally on their computers. Discussing the drivers behind this practice, a number of responses were received:

- 5 (17%) believed the Windows password provides adequate protection for the data stored on their laptop, P6:"*I think the laptops seem pretty well secure. That's an assumption I've made that the laptops seem pretty well password enabled. So you'd have to log on originally and you'd need to know the PIN code as well to log on as well.*"
- 5 others (17%) mentioned that sometimes remotely connecting to the corporate network can be difficult (either the service is too slow or they may not have internet access), but they may still need to access some documents for productivity purposes (e.g. prepare for a next day meeting, access from a client's site etc.). P17: "*Cause occasionally I go to [a] place where I don't have an internet connection, if we go out of site or wherever and having some of the files that I need on my laptop means that I can work, otherwise I've got to connect it to a server somewhere that's not always possible. It's not really that sensitive. I don't have any passwords on the other files, I've tried that in the past, and then I end up not being able to access the files on it, if I can't remember the passwords to the files*"
- 3 (10%) mentioned that they had run out of the allocated capacity on the network drive and they needed to store files locally to be able to keep those. P6: "*I have very little on my H drive yet the*

drive is full, that's why I can't backup my C drive to it. And it just won't let me save because there's too much information generally on the H drive."

4.5.7.2 Document sharing

The ability to share documents with colleagues was also reported as important for all employees, as a large part of their work involved collaborative working. Desired behaviours on information sharing were extensively covered in the security policy:

- "*NOT access any electronic messages or data for which they are not the intended recipient or they are not authorised to access, (unless they are permitted proxy access)"* and also "*NOT circumvent or attempt to circumvent any security controls that have been applied to prevent unauthorised access to any part of the information system.*"
- "*Bear in mind that unencrypted electronic messaging is not a secure method of communication.*" and "*Where information is confidential, price sensitive, commercially sensitive or includes personal data, first confirm with your intended recipient that the use of electronic messaging is an acceptable form of communication and should use appropriate security measures (for example, encryption technology) to ensure confidentiality.*"

The organisation provided a number of different provisions for employees to enable secure file sharing: shared drives existed for collaborators to share information and SharePoint sites were present as group document repositories. While discussing their document sharing behaviours, only 7 employees (23%) reported that they use the provided provisions for file sharing, while two (7%) of them reported they are not well-suited for their sharing needs (P6: "*I have concerns with the systems that we have because the shared drive I might only be able to get on to it twice or three times a week.*", P8: "*…we've got a guy from university who's working with us for a few weeks at the moment. And he doesn't have access to the various files that are on our actual S drive, so we're just having to e-mail backwards and forwards bits of files*". Examining employee file sharing habits, 18 (60%) reported that they mostly use USB drives to do so (encrypted and unencrypted – see section 4.5.8) while 7 others (23%) reported that it is a common practice to share documents via email. If a document contains sensitive information, 3 employees (10%) mentioned they send the password separately in another email: P16: "*Yeah, well apart from again, just password protecting it. They're probably the specialist method if we were sending it.*"

Some employees also appeared to be aware of potential risks arising from their actions: 5 (17%) explicitly acknowledged their behaviours to be potentially risky, but also mentioned that no alternative effective way to transfer or store files exists. P4: "*But there are exceptions where you need to transfer this information and you know that information is a bit sensitive, you know who you're transferring it to, and for whatever reason you can't use email so you have to use a flash stick. You should use an encrypted one but for ease and generally because I haven't got an encrypted one I just use an unencrypted one, whip it across and then just delete the copy off the flash stick which isn't perfect but it's quicker, easier than having to follow the policy.*"

4.5.7.3 Physical documents – Clear desk

As previously discussed, employees were aware on the sensitivity of corporate information and some of the corresponding policies to protect it. Many complied with clear desk requirements, with 15 (50%)

reporting not leaving sensitive documents on their desks and securely disposing information on paper once they are finished working with it. In contrast, 9 others reported not complying with clear desk, despite awareness of the need for it, due to "*information not being sensitive*" (P24) or "*lack of enforcement*" (P14).

4.5.7.4 Personal computer use

The use of personal computers to handle company information was not covered in the security policy. 4 employees (13%) reported using personal computers at home to do corporate work, for similar productivity-related reasons as having to store information locally on laptops (e.g. bad remote connection, need to work when outside the office away from internet connection). P5: "*…so if I want to work on something I have to send a document, I'll send a file to a personal email address. I don't have access [system name] in that way because of the cost of it.*"

4.5.7.5 Document handling discussion

In general, employee actions did not manage to effectively "*Keep personal data confidential and not disclose it to any other person unless authorised to do so by* [the company]". Many of the identified behaviours regarding the handling of corporate information lead to increased organisational exposure to security risks:

1. Storing documents locally means that potential loss of a laptop results in loss of the data as well. It also enables anyone who gets the laptop to recover the contents of the hard drive (even encrypted drives have been found to be insecure if someone gets physical access to a computer – Halderman et al., 2009). In addition local drives are not backed up, so no way to recover the data exists if they are deleted accidentally, or the laptop is lost or corrupted (violates *availability* principle in addition to loss of *confidentiality*).
2. Email-based sharing also increases the organisation's exposure to security risks. Confidential documents can end up being included in emails stored locally on employee laptops that move around with them, running the risk of being stolen by attackers. In addition, security policy and communication, provided no explanation to employees on how to protect the information stored on their computers.
3. Information left around in physical form can be visible to unauthorised individuals. In many cases, an attacker may not even need to remove a document of interest from an employee's desk, obtaining the required information by, for example, taking a photograph of it. Leakages of sensitive information on issues like upcoming projects can have significant consequences for an organisation trying to devise a long term strategy to stay ahead of its competition.
4. Storing organisational information on personal computers is risky, despite not explicitly prohibited by the security policy. Many modern security threats (viruses, screen capture software etc.) can lead to leakages of organisational information copied on personal home computers of employees. In addition the use of that equipment by third parties unrelated to the organisation (e.g. employee family members) can further increase the risk of unauthorised individuals getting access to information that may accidentally be left on an employee's personal computer.

In general, employee handling of organisational information was widely varying, with the security policy often failing to capture potential behaviours that could increase organisational information security risk exposure.

4.5.8 USB stick use

USB drives were commonly used amongst employees to store, transfer and share information (18 - 60%). The security policy clauses on USB sticks; ask employees to "*Ensure that they take all reasonable precautions and checks to ensure that malicious software does not enter Company Networks or systems via any means, e.g. removable media, USB drives, Internet etc.*" but also "*NOT connect any device if you are unsure of the source of the information in the device as it may contain malicious software.*"

The organisation has also provisioned for encrypted USB drive availability by providing a number of employees with encrypted ones, instructing them to use those when they need to transfer data. Not all employees were given one automatically, but the procurement process was relatively simple: they just had to file a request to the IT department. Despite this, only 10 of the interviewed employees (33%) reported using the encrypted drives: P30: "*they've said if you want to use a memory stick, then use the ones that the company is endorsing and so, for instance, in our department, one of the PAs to the senior management ordered memory sticks for the teams*". Examining employee responses on the use of USB drives a number of non-compliance practices regarding USB use were identified:

1. 3 employees (10%), who were not given an encrypted drive, assumed they were not supposed to have one. P10: "*The other point about this, the flash drive, was that they're very expensive obviously. I think what happened when the policy came out that you had to use that and nothing else, then there were lots of people that needed a portable means of carrying things around. And they were hit by and order for about 800 or something of them. And I don't think those orders were all approved, because the cost was just too much.*"
2. Those who needed to use a drive but did not have one mentioned that procurement requests take some time to be processed, so for urgent data transfers they needed to find another solution. P24: "*I have seen one or two around the place that don't meet that description. On the other hand, the method of ordering them doesn't make it easy, and one of the ways improve that adherence, would to make the process of ordering a drive simple, just make it as easy as possible, and currently, frankly it isn't. The addresses of the people who have to approve it are many years out of date*."

As a result, if they still wanted to use a recommended data transfer practice, they had to borrow a colleague's drive together with their password. P4: "*A couple of times I've had to borrow someone's encrypted one, instead of transferring it between people in the same room I've been transferring it to a different off site location. So use one of those, information has been backed up on to an encrypted one. Yeah, have to borrow the password. But, again, going on to the security of it generally, passwords are not the most secure either, it's generally a post-it note with the encrypted memory stick. So they'd have a USB encrypted with the backup of everything on and they'd have a post-it note with the packaging or next to it or on it to say what the password is.*"

16 employees (53%) reported that they use unencrypted drives, providing various reasons for this, mostly related to information availability concerns and incorrect understanding or related risks:

1. Encrypted drives were too small for their needs or the need to transfer a file was immediate; the encryption/description process required too much effort when they just needed to share a single file between them and a colleague. It was then much easier to use their own unencrypted drives and delete the data after the transfer, believing that this practice is adequate to protect the confidentiality of the data. P17: "*Sometimes, if you've got a big document, is not enough so I've struggled to get it even if you've got one gig, that's not very big. Sometimes I've got a document on to give to somebody in the office…I only need to leave there for a short period of time. And it's not really that sensitive…the encrypted one, you usually got to put it in, you got put a password in, and you got to copy it on, the document's too big to email, and you don't want to type somebody's emails in, you put it on an unencrypted disk. Walk go over to somebody else's desk, copy it onto their computer and then just delete it off the disk. Cause otherwise you've got to go to their workstation and then put your password in or tell them your password. So it's simpler just have it on an unencrypted disk.*"
2. They were afraid that they may not be able to access the drives at critical situations: P10: "*…part of it is some virtual thing where you have to log into it or something like that. And, at crucial moments you're taking this flash drive to a presentation and you need to get it to work and, the damn thing doesn't work. So what people do is that they don't use them because of the problem. Because I think people can understand the rationale behind the policy, but if the thing doesn't work in practice every time, it gets abused.*"
3. They failed to understand potential risks. P9: "*We do have password protected USB sticks, but they tend not to get used. To be honest, they just sit in the drawer, I don't know the reason why. If I've ever had to take something to a formal presentation, if I'm travelling overseas or anything, then I'll use it. Generally, if I'm in the office, I'll just use a normal USB stick and then it just sits on there until it gets deleted again."*

3 employees (10%) mentioned they did not use USB drives at all, because they found encrypted ones too cumbersome to use and unencrypted ones too risky. As a result they resorted to other ways to share/transfer files, like emailing those to their personal accounts for example (e.g. P5 example in Section 4.5.7.4).

The identified practices on employee USB drive behaviours significantly increase organisational security risk exposure:

1. The unencrypted drives used were not issued by the organisation and were often also used on their home machines, increasing the potential for malware-infected drives to be connected to corporate machines.
2. The confidentiality of the data stored on unencrypted USB drives can also be compromised if they are lost in transit to another corporate site, or if employees forget to wipe off the drive, which can then be misplaced, lost, stolen or passed on to a colleague who is not authorised to access the data on the drive. In addition, if no specialist deletion software has been used to

securely remove data from the drive, information employees perceived as deleted can be easily recovered. In general, when sensitive information ends up lying around the organisation on unencrypted USB drives, the potential of it being of being mishandled is increased.

4.5.9 Email filtering, Website blocking

The organisation operated an email filtering system and website blocking mechanism that prevented employees from visiting websites identified as potentially high-risk. In addition, in order to protect organisational systems from virus infections, employees were asked: "*NOT open electronic message attachments from unknown external sources as they may contain viruses or other malicious software. The user should alert Information Security via the helpdesk*", "*Ensure that they take all reasonable precautions and checks to ensure that malicious software does not enter Company Networks or systems via any means, e.g. removable media, USB drives, Internet etc.*" and "*NOT circumvent or attempt to circumvent any security controls that have been applied to prevent unauthorised access to any part of the communications systems, or to any electronic messages contained within those systems, or to the Internet usage facilities.*" In the interviews, employees referred to both technologies as inconsistent, not well configured, and also often blocking work-related employee tasks.

Discussing their experience with email filtering, 4 employees (13%) reported that they had work-related emails blocked and that blocking can be random and unreliable, failing to help them distinguish between legitimate emails and fraudulent ones.

P13: "*...there was one incident thinking about it whereby a friend had, got access to my email address. And they picked up a virus and I kept getting random emails through. And I found it quite ironic that some of the things that were coming through to me from this virus infected email accounts should have been blocked by the firewall and yet all of that stuff was coming through. And yes business documents were being blocked and I thought that was quite ironic at the time*."

Discussing their experience with website blocking mechanisms, 8 employees (26%) mentioned that websites they need to access for work purposes are often blocked.

P11: "*you are blocked from a lot of websites. And in my job I very often Google things, for example I was looking for big licences. And I Googled Microsoft and I got loads of access denied, for all sorts of reasons. So, you kind of think to yourself, "I don't understand what the site I can't get is." [...] But there are lots of sites blocked and you don't know whether behind it the data is useful to you or not"*

To gain access to the desired content, 4 of them (13%) downloaded the files on their home computers and transferred those on the company ones, either using USB drives or by emailing those to their corporate email accounts from their personal ones. As one employee said, if they did not cause problems to their home machines, they assumed they are safe to use on their corporate machines as well.

P3: "*So I went home and that night at home on my home PC I downloaded this formula and the instruction manual to go with it. I thought, "I'll send that to myself at work tomorrow." "And I, I can read it at work." And I send it to work and it got bounced back. [...]Um, so I put it on my USB memory stick and brought it in and then had a look at it at work the next day. On the unencrypted one. I think*

because it was an Excel macro it was a bit cautious about the fact that it was a macro and it could do things it wasn't designed to do. But doing the research I did to get to where I go to I was fairly certain it was a legitimate software tool, a legitimate bit of Excel macro that wasn't going to do any harm. It wasn't downloaded from piratesoftware.com or something like that. I think that was why the website was blocked because part of the page had a forum on it where people had commented and, and provided feedback on what was, what was available […] I couldn't access the website from work so I had to go home to do it."

In general the problems both website and email filtering systems created for employees trying to access work-related information, led to employees dismissing the usefulness of those. This, combined with inaccurate risk awareness (e.g. on virus propagation risks), provided adequate justification for their circumvention decisions.

4.5.10 Physical Security

Policy clauses on physical security stated that "*Any visitors are accompanied, ensure they have a visitors badge and ensure they comply with all Company policies. In particular visitors must not connect any third party laptop or other device to Company's computers or network infrastructure (except the guest wireless networks after appropriate authorisation).*" In the interviews, 5 (17%) employees reported they would challenge strangers walking around the office. In contrast, many reported passive physical security behaviours: 9 (30%) said that anyone in the building should have been checked at entry for authorised access, so there is no need to challenge them, while 3 others (10%) mentioned that "*Outsiders would be picked by someone else*". 8 others (27%) reported that organisational provisions for physical security were insufficient, that it was "*not hard to get into office*" (P25) and that existing security processes are not effective: P22: "*A number of times when I've certainly left this key for my desk pedestal at home or I've forgotten to bring my pass in on certain days. So I've come in before where my laptop's been locked in my pedestal but you can call facilities and they can come and open it straightway. Now from a facilities perspective I've never once had them challenge whether that is my desk and my pedestal.*" In general, as with other aspects of organisational security, employees appeared to downplay their own responsibility in preventing unauthorised physical access to the organisation's premises.

4.5.11 Enforcement and sanctions

The security policy clearly stated that sanctions could be imposed for employee non-compliance with the clauses defined in it: "*Failure to comply with all IS Security policies may lead to disciplinary action and unlawful or illegal conduct may lead to separate criminal or civil proceedings. If you are a third party user of company's information, for example a consultant or contractor to Company, misuse is likely to lead to termination of your contract*." Despite this, employees reported that sanctions appear not to be enforced. They mentioned they can get away with missent emails (P7 "*I know we can't just get away with turning a blind eye to security, but in terms of every day little slips of information, such as on a memory stick, or an e-mail which is sent wrongly, then I don't know how heavily that is monitored, to be honest*"), using unencrypted USB drives (see section 4.5.8) and sharing passwords (section 4.5.6). In addition, non-compliance appeared to be advocated by managers whenever employees had problems that slowed down or prevented completion of their primary tasks (i.e. high security-productivity friction): P6:

"*And recently I have shared a password with a senior manager because I was keeping an emergency log and it made sense to, to keep using the same log on my laptop […] as I say the reason I diverted away from policy has been driven by a business requirement. And it's one of those things that's always been discussed with seniors and it's been seen as a work around because the policy doesn't fit the business requirement*" and P30 (Manager): "*I mean, my advice to anyone wanting to use that would just be aware of what it's doing, deleting that back off that local area, and putting it on the server*"

4.5.12 Security helpdesk experience

The security policy asked employees to contact the organisational IT helpdesk whenever they were in doubt about security-related risks (e.g. "*NOT open electronic message attachments from unknown external sources as they may contain viruses or other malicious software. The user should alert Information Security via the helpdesk*"). Despite this, identified policy reliance on the helpdesk, 15 employees (50%) referred to it as unreliable, "useless", slow, also mentioning they prefer not to use it at all.

P20: "*I think it's got much worse. The outsourcing of the support is awful. I need to speak to the person that's going to mend my computer, and when they can't even understand my name, can't understand what I'm saying, until you have a real communication I'm sorry, but it's just rubbish. You know, you need to be able to say "Hi, I'm AB, you know, this is my problem, please can you fix it?*"

This lack of support for secure behaviour provided sufficient justification for breaking the rules.

4.5.13 Security experience and perception

Employees were also asked to discuss their overall experience of organisational information security. They referred to the security implementation as "about right but could be improved" and to their colleagues as "mostly compliant" that follow "most security rules most of the time", but also recognised that some rules are generally broken because there are good reasons for doing so (e.g. slowdown: P20: "*takes about 20 minutes to log on on the good days*"). They also expressed some concerns about the access allowed to contractors (e.g. P6: "*laptops given without much care taken […] not erasing data*"), who to them should be treated as potentially riskier, as they are less motivated to follow security rules; essentially hinting that the security processes were not working well. When probed to discuss potential risks emerging from their behaviours, 10 (33%) employees (e.g. P26 above) recognised risks created, but justified those as necessary (P20: "*I think we are rule-breakers when it's rubbish rules […] and they set the rule, without actually thinking about the consequences, and that's when it all becomes problematic, when you can't actually get the flash drive*"). In general, employees considered some security violations as necessary to proceed with their primary tasks, reported lack of visible enforcement for violations, and downplayed their own responsibility in keeping the organisation secure.

4.5.14 Overall security behaviour

Employee behaviours appeared to be widely varying, and in many cases deviating quite severely from the organisation's security policy, creating significant security risks for the organisation. Some of the identified insecure practices were a result of employees' lack of awareness of related policy clauses or

risks: they just based their security decisions on their own risk perceptions. In other cases though, rule-breaking was deliberate, driven by friction created by existing security policy or mechanisms being incompatible with employee primary tasks. This provided employees with justification for their behaviours, even when they acknowledged corresponding risks, as to them productivity is more important than security. Employees also appeared to make their own decisions on when policy should be followed, with those decisions often being situation-specific; in some cases they also devised their own "workable" security. They (1) chose themselves which of the clauses from policy and communicated principles applied to them and their role in the organisation, (2) put pressure on their colleagues to comply with policy clauses (e.g. screen lock), (3) devised their own approaches to protect their laptops, (4) wrote their passwords in protected documents and (5) shared their passwords only with those who, they thought, genuinely needed access. The remainder of this chapter uses the identified employee behavioural paradigms, to characterise the influence of different elements of the organisational security implementation on employee behaviours, and categorise the identified insecure behaviours, based on the factors that led to their emergence.

4.6 Security behaviour drivers

Examining the employee behaviour themes that emerged from the thematic analysis, two main categories of behavioural drivers were identified: (1) Secure behaviour drivers (elements of the security implementation or employee understanding that encouraged secure behaviour) and (2) Insecure behaviour drivers (elements of the security implementation or employee understanding that led to behaviours that increased organisational security risk exposure). This section analyses both the above categories, explaining how the employee behaviour examples presented in section 4.5 allowed identification and characterisation of the impact of a widely varying set of elements of the organisational environment on employee security behaviours. It also discusses how the perceived lack of enforcement leads to insecure security culture development and presents a preliminary model of security behaviour drivers, which is refined further in the next chapters of this thesis.

4.6.1 Secure behaviour drivers

Employee motivation for secure behaviour stemmed from both organisational security communication and employees' personal risk awareness. Security communication led to understanding of organisational security risks, with employees then complying with communicated behaviours (e.g. the need for information sharing to be done on a "*need to know*" basis). In other cases though, employees identified potential security risks that were not included in the organisation's security policy or communication (e.g. the need to protect their laptops). In order to mitigate those, they acted in ways they deemed as appropriately secure (e.g. take laptop with them).

Despite leading to secure behaviours, employee actions driven by own understanding of security risks can also increase organisational risk exposure. Long-term employee reliance on those self-devised security behaviours can lead to security habit and culture development invisible to central security management. When employees devise their own security processes, security management is less able to monitor their behaviours, which also reduces their ability to assess current levels of security protection.

4.6.2 Insecure behaviour drivers

The results presented in section 4.5 identified a number of different insecure employee practices. Analysing the relationships between the themes that emerged from the analysis, three main categories of drivers for those practices emerged:

1. *Inaccurate security understanding and risk perceptions*: Employees failing to understand security purpose, combined with their inaccurate risk perceptions, make non-compliance more attractive on a cost-benefit scale than the effort required to comply with security mechanisms (e.g. downloading files locally and bringing those in the organisation believing they pose no risk, instead of contacting the unresponsive security helpdesk to unblock access to a website).
2. *Compliance not possible*: The mechanisms required for employees to behave securely are currently not present (e.g. a network drive being full leading to employees copying files locally).
3. *Compliance too expensive*: Employees may correctly perceive the risks involved in their actions, but consciously choose not to comply due to high compliance costs (e.g. increased time-overhead of encrypted USB sticks leading to the use of personal unencrypted ones).

The remainder of this section discusses each of the above insecure behaviour drivers, analysing the conditions that led to their emergence, presenting the risks they create for the organisation, but also discussing why security management appears to be complicit to their existence.

4.6.2.1 Inaccurate security understanding and risk perceptions

The need for some of the existing information security mechanisms and policy clauses was unclear to employees. Despite possessing some awareness about the need to protect sensitive information, reports like "*just confidentiality not security*" suggest lack of understanding of what information security tries to achieve; one of the key goals of information security is to preserve confidentiality of information. This inaccurate knowledge and awareness about potential security threats, led to inaccurate risk perceptions and development of incorrect mental models[20] on the operations of the systems in place amongst employees, making non-compliance an attractive option when they encountered friction-inducing security. A few examples of this:

1. Employees rarely considered the possibility that using USB drives to copy data they downloaded at home on their corporate machines might lead to malware infections. They seemed to misunderstand how a virus may propagate though the organisation's systems (modern viruses are extremely complicated and propagate using various clever mechanisms – botnets, for example, are almost invisible to the end-user, while other viruses may be programmed to deliver their payload later in time etc.). With their simplistic understanding, employees assumed that a downloaded file that causes no harm to their home computer is safe to be used on a corporate one, adopting this practice when they could not access a file from inside the organisation.

[20] "*A mental model is the "user's belief" about a system in hand*" (Nielsen, 2010) or "*A theory people build to explain the causal behaviour of systems*" (Dix et al., 2003).

2. They also failed to consider that data deleted from unencrypted USB drives can be easily recovered; they believed that deleting all the data from a drive after a file transfer provides adequate protection in the case the drive falls in unauthorised hands.
3. Employees also stored sensitive files locally on their laptops, assuming the presence of a Windows password prevented someone from accessing those files. But a Windows password is only effective for access control purposes and, even with encryption added on top, the data on it is still vulnerable to brute force attempts, if an attacker manages to get unconstrained access to the laptop (Halderman et al. 2009).

The impact of inaccurate employee understanding of employee behaviours was often made worse by the organisational security policy not providing clear indications on what the correct risk-mitigating actions are (e.g. policy on password sharing: "*NOT access any information or system using another employee's or system's password unless explicitly authorised to do so*" – in this case no clarification existed on who is allowed to give that authorisation).

In general, most employees did not have a good understanding of what information security is, and what it tries to protect. Security aim is not just to "*prevent computers from getting infected by viruses*", as one interviewee said, but also protecting information and providing uninterrupted access to it. The presence of those misconceptions led to a reduced perceived benefit from complying with security, making non-compliance an economically attractive option for employees, when secure behaviour required significant time or effort investment (see section 4.6.2.3). They also downplayed their role in organisational protection: they perceived the information they handle as generically not-sensitive, which led to the wide range of insecure behaviours, described in section 4.5.

4.6.2.2 Compliance not possible

In many cases, compliance was not an option regardless of how much time or effort employees were willing to invest to achieve it. Employees reported inability to comply with parts of the security policy, because the mechanisms required for secure behaviour were either difficult to use or absent. A number of examples of this behaviour were identified:

1. Employees justified copying files locally to their laptops when there was insufficient space on their network drive, or to avoid problems with remote file access when working from home or while travelling.
2. They also found the encrypted USB drives provided by the organisation to be too small, which created the need for alternative file-sharing methods such as using unencrypted drives or emailing files to each other.
3. The large number of passwords required for various corporate systems resulted in employees being unable to recall those from memory. Employees then wrote their passwords down, either in electronic form on their laptop or in a document/notebook they carry with them all the time.
4. In order to cope with website blocking preventing access to information needed for work purposes, employees downloaded the required content at home and brought it in the organisation, using either USB drives or through email.

In the four examples above, the majority of employees were aware of the increased risks associated with their behaviour, but felt that the organisation failed to provide a properly working technical implementation. This forced them into workarounds, so they could keep working towards primary task completion. In addition, managers appeared happy to encourage non-compliant behaviours, as long as mitigating actions were taken (e.g. delete documents from USB drive when done); this accentuated employees' belief that the organisation would prefer security transgressions to "*letting everything grind to halt*".

4.6.2.3 Compliance too expensive

The third driver for employee insecure behaviours was the high individual resource investment (time, cognitive or physical effort) that certain security mechanisms demanded:

1. Employees shared their passwords for quick access to systems because it *"would take ages"* to get the permissions changed. They also expected their colleagues to do the same for them. Even some managers reported this as common and acceptable practice: "*employees newly-involved in a project access the system using someone else's credentials until their access is sorted out*".
2. They also used personal unencrypted USB drives to share data with their colleagues because it is faster and easier than using company-issued encrypted ones. The effort involved in using the latter was perceived to be *"not worth it for simple file transfers around the office*". Some interviewees, who understood potential risks from this practice, reported they "*immediately wiped the drives afterwards*" to prevent information from falling in the wrong hands.
3. Employees also resorted to file sharing through emails and unencrypted USBs, as the organisational file sharing solutions were either unreliable or inaccessible.

In this category of behaviours, compliance with policies was possible, but employees perceived the impact of compliant actions on their primary tasks to be higher that what they were willing to accept to protect the organisation (confirming past research suggestions that security behaviours are an economic cost-benefit decision - see section 2.7.1).

4.6.3 Lack of enforcement and security culture development

Despite security violations appearing to be widely prevalent in the organisation, employees reported minimal attempt for security policy enforcement. This perceived lack of enforcement suggested to employees that security is not part of organisational priorities. In the interviews, they mentioned that clear desk inspections were "stopped some time ago", screen lock motivation did not come from enforcement but from colleagues playing jokes on each other, while their managers advocated for password sharing whenever setting up access was perceived as "not worth it" time-wise. Long term occurrence of such behaviours, combined with perceived organisational failure to prevent those (no attempts to create security solutions that fit the primary task or enforce policy), leads to employees considering policy violations as justified. Over time, such behaviours become habitual to employees and become part of organisational security culture, leading to increased organisational exposure to security risks.

4.6.4 Security behaviour drivers model

The identified relationships between elements of the organisational security environment and related employee behaviours (Appendix F) led to the emergence of a security behaviour model, presented in Figure 9.

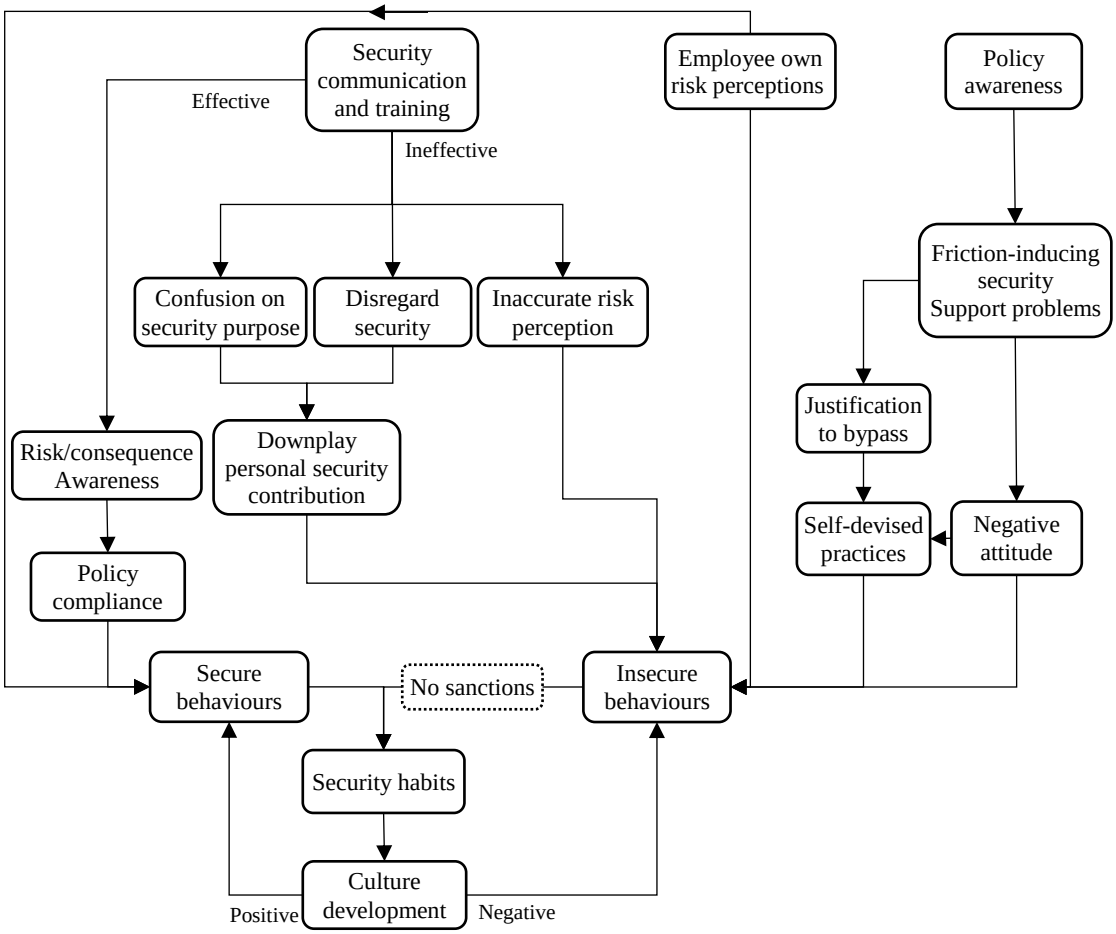

Figure 9: Security behaviour model

It is important to note here that some of the relationships presented in the model in Figure 9 were extracted from a small number of employee reports, often just one or two (e.g. support problems leading to justification to bypass). As a result, this model should be seen as a preliminary suggestion for now and is revisited and adjusted later in the thesis based on the findings emerging from chapters 5 and 6.

4.7 Lessons learned, research questions and further work

This chapter presented an analysis of 30 interviews from Company A, investigating employee interaction with organisational security implementation and corresponding behaviours. It identified drivers behind secure behaviour, elements of the security implementation that drove insecure behaviours and non-

compliance with policies[21], also devising a preliminary model of security behaviour drivers. Based on the findings that emerged, this section starts by discussing problems with current information security management approaches, revisits research questions and propositions presented in section 3.3, and also provides justification for the research presented later in this thesis.

4.7.1 Problems of current security management

The findings of this chapter demonstrate the impact of fiction-inducing security on employee behaviours. Mechanisms and processes not designed around employee primary tasks, make non-compliance an attractive option for quick primary task completion, or even the only available employee action when security is completely unusable. In both cases, employees' main goal is efficient completion of the primary task, such as manufacturing goods or delivering services. But, as Herley (2009) pointed out, it is often the case that "security people value customers' time at zero", creating security mechanisms difficult and cumbersome to use, draining employee time and effort. Productivity-focused employees then resort to insecure behaviours, as the primary task overhead leads to security being perceived as "not worth the effort". The greater the perceived urgency and importance of the primary task, the more attractive or acceptable non-compliant options appear.

In addition to friction-inducing security mechanisms, ambiguous and unclear policies (and corresponding communication) also drive insecure employee behaviours. The findings show that unrealistic or ambiguous policy clauses (e.g. "appropriate secure channels should be used") led to lack of accurate risk understanding, with employees then downplaying their participation in delivering security. Insecure behaviours then become a norm, encouraged by the presence of friction-inducing security and also advocated by line managers, whose focus is on team primary task completion rather than security. The findings also show that security solutions deployed only partially in an organisation (e.g. provisioning for encrypted USBs for only a proportion of the employees), can lead to insecure behaviours when employees are left to assume things (e.g. employees not given USB sticks assumed they should not have one, so they kept using unencrypted ones). In addition, users may devise their own secure practices when they perceive a risk that the security policy appears to have failed to capture (e.g. devising own approaches to protect corporate laptops). Over time, ineffective risk communication and high-friction security lead to insecure behaviours becoming part of organisational security culture, with organisational security being unable to control it, leaving it exposed to long-term insecure employee behaviours.

4.7.2 Revisiting research questions and subsequent PhD work

As stated at the beginning of this chapter, the purpose of the analysis presented above was to provide better understanding of the conditions surrounding employee behaviours, to provide starting points for a

[21] It is important here to underline the difference between the two terms. *Non-compliance* in this thesis refers to conditions where employees are behaving in ways prohibited by the organisation's security policy. *Insecure behaviours* refer to both non-compliant behaviours and other behaviours that can increase organisational security exposure that were not included in the organisation's security policy.

more in-depth analysis on the full available Company A dataset (and also provide guidance for data collection and analysis in Company B). Looking back at the research questions, the findings managed to improve existing understanding of employee security behaviours, partially addressing some of the research gaps identified in section 2.8 by providing some preliminary answers to the research questions. They also revealed areas that required further research. The above led to the emergence of an updated set of research questions, driven by security behaviour insights that emerged from the results.

4.7.2.1 Do employees understand the need for security mechanisms in the organisation? If yes or no, why?

The interview analysis revealed some general awareness and understanding amongst employees that organisational information needs to be protected. Despite that, many failed to explicitly relate that to information security, referring to it as "just confidentiality". The findings provided partial evidence that lack of effective communication is responsible for this (e.g. employees were unsure of policy content – some said they know where it is, but also admitted to not looking it up). In addition, some preliminary understanding emerged on employee responses when they perceive organisational security support as lacking, but understand the need for risk mitigation: they appear to modify existing security processes or mechanisms, or develop their own, believing those provide adequate protection. Both the above topics (employee understanding of the need for security and their responses to perceived lack of organisational support) need to be further investigated, to improve understanding of their effect on employee security behaviours, how they evolve over time and passed-on to new starters, and what can an organisation learn from those regarding the effectiveness of their current security deployment. In order to investigate this, a new research question was devised:

"*How do employees respond to a perceived lack of organisational security support? What are the risks from their behaviours and what can organisations learn from those?"*

4.7.2.2 What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?

Security mechanisms not designed to accommodate for employee primary tasks often make secure behaviour either expensive (requiring high time or effort investment from employees) or impossible (when they do not work as intended). The subsequent need to prioritise between compliance and primary task completion creates friction between the two. Whenever the option between secure behaviour and productivity is binary (e.g. don't share password, lock screen), employees choose the latter, behaving insecurely. But when employee options are not that clearly defined, combined with employee information security risk awareness, subsequent behaviours become more complicated: employees appeared to deviate from prescribed practices (e.g. use encrypted USB drives), using resources available to them (own drives) and then taking self-devised risk mitigating actions ("wipe the data off the drive"). This was also the case when employees identified security risks not covered in the security policy (e.g. how to protect their laptop). The need to further investigate the emerging self-devised security behaviours, led to the emergence of another research question:

When organisational security provisions appear to provide inadequate risk mitigation, what do employees do?

Another interesting aspect of the findings that required further investigation is the influence of trust on security behaviours: employees appeared to acknowledge password sharing as a risky behaviour, but still shared those, despite feeling uncomfortable about it. Violations were also encouraged by managers, who reported to trust their employees, with trust towards colleagues also being reported as a reason for not following even simple mechanisms like screen lock and clear desk (e.g. P10: "*it's a matter of degree I suppose if you are a few feet away, that's fine, but if you actually leave and go somewhere else, then certainly you should lock it. And I don't think you would have issue with your own team. If, for example, everybody goes off for a team meeting, you really should lock your screen*"). These preliminary indications of trust affecting employee security behaviours gave rise to another research question:

What trust relationships develop in an organisation and how do they influence security behaviours?

4.7.2.3 How can the improved understanding from the previous question be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?

As mentioned in section 2.8.4 of the literature review, for most modern organisations, complete redesign of their security implementations from scratch to eliminate identified problems is never an option. A more flexible approach to security design is required that will allow identification of problems in their security implementations and devise improvement approaches. The findings of this chapter create can be of significant value to attempts to create such a process. The identified non-compliance categorisation (section 4.6.2), preliminary identification of employee responses to security-productivity friction (section 4.6.2 and 4.6.3) and the security behaviour model that emerged (section 4.6.4), provide useful insights to organisations, highlighting the importance of security mechanisms designed around employee needs and priorities in delivering effective protection. Despite this, the analysis of the results presented in this chapter did not provide sufficient user behaviour insights to allow for the creation of an approach that organisations can use to identify and design out friction-inducing security mechanisms. In an attempt to create such an approach, building on the findings presented in this chapter, the remainder of this thesis presents research aiming to investigate the updated research question set and: (1) better understand employee actions when security mechanisms or communication creates problems to primary task completion (chapter 5), (2) identify the effects of trust on organisational security behaviours (chapter 6) (3) use the knowledge that emerges from both (1) and (2) to provide approaches for improvement and guidelines towards creating more effective (and less costly for employees) information security management in organisations (chapter 7), and (4) apply the emerging approach to identify and deliver potential improvements in one of the two partner organisations (chapter 8).

4.7.3 Revisiting research propositions

P1. "*Directly discussing problems of security implementations and compliance with employees can lead to improved understanding of the reasons driving employee insecure behaviours*"

As discussed in section 2.8 of the literature review, research discussing problems with security implementation in organisations has been limited and mostly focused on employee password behaviours. Using semi-structured employee interviews managed to reveal interesting insights on their security behaviours:

1. Identification of relationships between friction-inducing elements of the organisational security implementation and the emerging employee security behaviours.
2. Categorisation of the underlying conditions leading to insecure behaviours, based on specific properties of the security implementation/environment that created those.

The findings in this section provided sufficient evidence that P1 is a valid proposition, but, as discussed earlier, they only covered a subset of the available dataset. By analysing the full set of available interviews, and collecting an additional interview set in a second organisation, the research presented in the next two chapters managed to enrich and strengthen understanding of the paradigms presented in this chapter, also strengthening current findings that suggest P1 validity.

P2. "*Engagement with employees can allow falsifying current beliefs that employees can be forced to comply with security*"

In section 2.6.3 it was explained that attempts to enforce security mechanisms or processes upon employees without assessing the effect of those on their primary task completion ability can create a number of problems: (1) high cost of policy-prescribed behaviours leads to non-compliance, (2) inability to discipline when non-compliance is widespread, due to high volume of false positive alerts, (3) creation of a negative attitude towards security, (4) decreased organisational adaptability to respond to changes in the threat landscape, (5) inability to provide flexibility where required (e.g. home and remote working). The findings of this chapter revealed another problem: employees will always find a way around security restrictions, often attempting to alleviate related perceived risks through self-devised security practices (e.g. employee using Summer01 for password, downloading files at home, sharing files on unencrypted USBs and erasing those afterwards). Currently security management attempts to eliminate these behaviours through enforcement, without first taking care to remove friction-inducing elements of the security implementation. This creates further friction between employee primary task completion and security, increasing the risks from emerging insecure behaviours. Similarly to P1, the findings of the thematic analysis suggest that P2 is a valid proposition. Despite this, further in-depth examination of employee responses to organisational policy enforcement attempts was required, in order to improve understanding of the effect of those on employee attitude towards security. The follow up data collection process and analyses aiming to improve the above understanding are presented in the remainder of this thesis, together with emerging results and their implications for organisational security management.

P3. "*Engagement with employees can allow identification of employee responses to friction-inducing security*"

Past research suggested that employees respond to high-friction security by developing their own, productivity-focused coping strategies (section 2.6.2). In addition to re-organising their primary tasks to reduce exposure to high-cost security (Inglesant and Sasse, 2010) or sharing information through informal

channels (Bartsch and Sasse, 2012), the findings of this chapter suggest that, when security is perceived as inadequate or expensive, security-aware employees may take other actions that they consider as mitigating security risks (e.g. use of unencrypted USB drives, erasing the data afterwards). As this was not the focus of the analysis presented in this chapter, detailed description and understanding of those actions based on the results presented in this chapter is not possible. But the identification of their existence drove the focus of the analysis presented in chapter 5, aiming to better understand and characterise those.

P4. "*Engagement with employees can allow the identification of problems in security implementations (both policies and mechanisms) that organisations have not currently identified through other means*"

Past empirical organisational research has provided valuable insights on employee interaction with security that created problems in primary task completion (section 2.6.2). But it did not attempt to holistically explore organisational environments to identify and characterise different instances of insecure employee behaviour. The behaviours identified and discussed in this chapter provide a first step towards such an analysis, with many of the identified behaviours being impossible for Company A to identify without direct interaction with employees: despite some behaviours being easier to observe (e.g. clear desk, screen lock, employees using own USBs), other more complex ones would be much harder to capture (e.g. ineffectiveness of communication, password sharing or storing documents locally on laptops). The findings presented in this chapter provide evidence for potential validity of P4, but further analysis was required to strengthen it. This was done by the grounded theory analysis on the full interview set from the two organisations presented in chapter 5.

P5. "*Engagement with employees can improve existing organisational ability to manage current information security challenges*"

Other than identifying the need to eliminate friction-inducing security mechanisms and improve security communication and training, the analysis of the results presented in this chapter did not provide sufficient employee security behaviour insights to allow creating an approach that organisations can use to identify fiction and redesign their security implementation accordingly. As a result, no evidence for P5 validity emerged, but this proposition is revisited after the analyses presented in chapters 5 and 6, and discussion in chapter 7.

Chapter 5: **The shadow security**

The findings of the thematic analysis presented in chapter 4 improved existing understanding of the impact of friction-inducing organisational security on employee behaviours. But, as discussed at the end of the previous chapter, the findings only provided partial answers to the research questions this thesis aims to answer. Better understanding was required on (1) employee understanding of the need for security as a primary task enabler and the behaviours that emerge from it, (2) employee responses to perceived lack of organisational security support, (3) challenges to employee primary tasks created from an organisation's security mechanisms and processes, together with (4) corresponding employee behaviours emerging from those, (5) employee behaviours when deployed security is perceived as inadequate, (6) the development of trust in the organisation and its influence on employee behaviour, and (7) potential lessons information security management emerging from all the above in order to deliver less taxing and more effective security. The need to investigate the above points, led to the emergence of an updated question set, driven by the findings of chapter 4 and repeated here for the benefit of the reader:

1. *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?*
2. *What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?*
3. *When organisational security provisions appear to provide inadequate risk mitigation, what do employees do?*
4. *How do employees respond to perceived lack of organisational security support? What are the risks from their behaviours and what can organisations learn from those?*
5. *How can the improved understanding from the previous questions be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?*
6. *What trust relationships develop in an organisation and how do they influence security behaviours?*

Building on the insecure behaviour driver categorisation of section 4.6, the first half of this chapter presents a grounded theory analysis of the 118 Company A interviews, investigating employee experience with the organisation's security implementation and their emerging behaviours. This analysis led to a detailed, empirically-founded understanding of employee responses to friction-inducing security, through the emergence of a new security behaviour paradigm, the *shadow security*: employees deploying own solutions when security is perceived as not serving their primary task focus. This new paradigm characterises employee interaction with friction-inducing security elements of their work environment, using identified behavioural narratives. It then provides improved understanding of employee responses to friction-inducing security. Building on this improved understanding, the second half of this chapter analyses the drivers of shadow security development, the emerging risks and consequences for organisational security management, and the lessons security managers can draw from it in order to reduce security-productivity friction. It also explains how data and methodological triangulation approaches were used to improve the validity of the findings: a large-scale survey was used to verify the

existence of identified insecure behaviours on a scale wider than the 118 interviews. In addition, a new round of interview data collection and analysis from Company B and another large-scale survey verified the existence of identified employee practices, improving the validity and understanding of the emerging behavioural phenomena.

5.1 Grounded theory process

A grounded theory analysis was conducted on the Company A interview data set, based on the process presented in section 3.5.2. All the coding was done using the software tool atlas.ti, which was also used for code comparison and re-use across interview sets. The code list that emerged was exported and shared with other researchers who used it as a basis for future analyses of the interview set, examining behaviours different to the ones presented in this thesis. Before starting the analysis, a set of focus topics was identified, based on the results presented in chapter 4 and the updated research questions (Table 7).

Category	Description
Need for security awareness	Employee awareness about the need for security in the workplace
Potential negative consequences on individuals from insecure behaviours	Shaming, potential sanctions imposed by the organisation
Confusion on security purpose	Unaware of what security is trying to achieve, or what is security in general
Policy awareness	Awareness of security policy existence and content
Security communication	Mechanisms, perception and understanding of security communication
Security training	Training process
Security culture	Employee perception on the overall information security culture of the organisation
USB stick use	Use of USB drives (encrypted, unencrypted), purposes of use
Email filtering, Website blocking	Experience with organisational systems for filtering of emails and website content
Support Problems	Problems with organisational support for security
Laptop usage	Use of organisational laptops, awareness about the need to protect those, actions taken
Screen lock	Awareness about the need to lock screens, related behaviours
Password use	Choice and mechanisms to remember those, also potential sharing and reasons
Document handling	Handling of organisational documents – awareness about the need to protect those
Document storage	Expedience with provisions for securely storing information, usage and problems
Document sharing	Methods for sharing information (either organisation provided or ad-hoc)
Clear desk	Behaviours related to the need to prevent physical information lying around the office
Physical Security	Experience with organisational attempts to secure physical access to sites

Table 7: Staring topics for grounded theory analysis

The analysis process consisted of a combination of the three grounded theory stages presented in section 3.5.2.2 (*open*, *axial* and *selective* coding). The exploratory nature of it allowed both in-depth examination and improved understanding of employee behaviours in relation to the start codes defined above. It also led to the emergence of new topics that enriched the emerging understanding, improving the researcher's ability to answer the research questions. This section presents the analysis process followed, while the remainder of this chapter focuses on presenting and interpreting the findings.

5.1.1 Open coding

Open coding aims to exploratory investigate the available data to reveal previously unknown information. It was used at the beginning of the analysis to identify a set of themes representing employee experience and behaviour in relation to various organisational security elements (mechanisms and processes), but also employee security risk perceptions and understanding that drove their security behaviours. Those themes directed subsequent analysis steps (including additional topics of interest to the research questions missed by the thematic analysis), that led to their characterisation, refinement and identification of relationships amongst those. After the first stage of the open coding process, 47 themes emerged. Each employee discussed on average 20.35 (stddev 4.93), with the median number of themes discussed being 20.5. Example themes included *security communication*, *storage of information* and *organisational provisions for employee support* (for the full list of themes that emerged from the analysis and the number of employees that discussed each one please refer to Appendix H).

Based on the emerged theme set, the 118 interviews were revisited. During this stage, employee reported facts or behaviours on the themes of interest were identified as *concepts.* Concepts referring to similar topics were grouped together under *categories.* For example, the *security communication problems* category was characterised by the concepts *overloaded*, *vague*, *inconsistent*, *unrelated to role*, as identified in the interview analysis. In total 82 categories emerged (once again for space reasons, the full list of emerged categories, together with example extracts, is presented in Appendix I).

5.1.2 Axial coding

During the axial coding process the categories that emerged from open coding were broken down to *subcategories* denoting when, where, why and how an identified phenomenon was likely to occur. Subcategories took the form of *conditions*, *actions/interactions* and *consequences* of the phenomena described by the top level categories. During the process some categories were turned to sub-categories and vice versa. This aimed to achieve the best representation of the facts reported in the data in the emerging theories. For each category a set of *properties* were defined (characteristics or attributes) and *dimensions* (possible values of a property along a continuum) were determined (secure, insecure behaviour, defined in policy, own mechanism). After the final list of categories and subcategories emerged, related categories were grouped under four major category groups:

1. *Employee security awareness and secure behaviour drivers*: categories relating to employee understanding of security risks, their responsibility in acting to protect the organisation, and also the drivers behind their secure behaviours.
2. *Impact of burdensome security*: categories characterising the impact of friction-inducing security on employee primary tasks and related employee behaviours.
3. *Team level mediation*: categories relating to elements of security management happening at local level amongst colleagues and their line managers.
4. *Security implementation and culture perception*: categories describing employee perception of security implementation effectiveness and overall organisational security culture.

Full list of category groups with corresponding categories, properties and dimensions of those, conditions related to each category, subsequent actions/interactions and emerging consequences can be found in Appendix G.

5.1.3 Selective coding

To ensure accurate reflection of the behaviours represented in the data in the emerging paradigms, during axial coding, continual comparison of the findings with the raw data was done to confirm or refute the conclusions that were made. After ensuring consistency of the emerging categories with the raw data, a specific narrative was created based on the identified consequences from axial coding, with a *core category* emerging: *the shadow security.* A *story line* was then created, based on the emerging categories: *When employees come across unusable – not well-designed security – shadow security emerges. Shadow security consists of all self-made security measures created by productivity-focused employees when the organisation's existing security implementation does not meet their needs*.

After the selective coding stage and the emergence of the research main story line, the analysis was taken one step further by integrating *process effects*. These describe the sequences of actions/interactions which can be traced back to existing conditions and which might themselves change these structural conditions, possibly resulting in further actions/interactions. For example, shadow security leads to disregard for central security that drives the subsequent emergence of ad-hoc security culture, with employees dismissing the usefulness of centrally communicated security advice. This dismissal leads to further shadow security development.

5.2 Emerging narratives - grouping categories

In this section each of the four emerging category groups is presented and discussed together with related categories, using interview extracts identified during the analysis. A quantitative measure is also included, indicating the number of code occurrences related to each category; the aim of this is to present an estimation of the prevalence of the identified behaviours in the environment investigated[22] [23].

5.2.1 Employee security awareness and secure behaviour drivers

The first main group of emerged categories related to employee awareness about the need for security, related policies and the drivers behind secure employee behaviours identified in the interviews.

[22] It is important to note here that the numerical findings presented in this chapter are likely to underestimate the true prevalence of the identified behaviours. This is due to the open nature of the interviews, which meant that not all interviewees got to cover all the topics referred to in this chapter (as mentioned earlier each interviewee discussed on average 20.3 out of the 47 topics discussed in total).

[23] This section avoids discussing the effects of organisational trust relationships on security behaviours that emerged from the analysis, as they were significant enough to be included in a separate chapter (chapter 6)

5.2.1.1 Security awareness

Two of the emerging categories related to employee security awareness. The first concerned awareness of information security risks and the need for mechanisms or processes to mitigate those, while the second concerned awareness of the existence of the organisation's security policy and specific clauses to mitigate those risks.

5.2.1.1.1 Risk/need for security awareness

102 (86%) of the interviewed employees were aware of the existence of information security risks, recognising the need for security processes and mechanisms in the organisation (e.g. need to protect information useful to competitors, need for uninterrupted access to information, or the need to protect the organisation from malicious outsiders and potential reputation damages):

P79: "*Security implications well clearly were they to be compromised there'd be massive impact so it's very important in that respect and there are increasing reports of systems around the world being attacked*".

98 employees (83%) understood their responsibility to follow security policy when handling sensitive information, contributing to organisational attempts to mitigate information security risks and avoiding potential negative consequences for the organisation:

P36: "*So if it's HR Payroll data, make sure that we pull the employees Social Security, date of birth out and scrub the data before we publish it to whoever's asking for it.*"

In addition to awareness about the need for security, 95 employees (81%) also reported awareness about existing regulation for data protection and handling of sensitive information. This was quoted by 27 (23%) as a driver for adherence to Chinese wall requirements for information separation across organisational divisions[24], and also for information sharing within the organisation being done only on a need to know basis:

P65: "*Because they're in tune with a couple of other things like the regulatory model, separation and stuff like that, so having to do things for a reason even though it might not seem like it's a good thing*"

In addition 17 (14%) quoted the existence of confidentiality agreements as increasing their perceived need for security:

P55: "*We have a lot of confidentiality agreements between us and a customer, obviously we won't share that information and hope to God that they don't either*".

Despite the identified awareness of the need for security, a number of problems in security perceptions were identified amongst employees. They appeared to be confused on what information they should

[24] Chinese wall provisions: "internal rules designed to prevent conflicts of interest" (Anderson, 2008, p.264)

consider as sensitive, with 75 (64%) reporting that the information they personally handle as part of their job is not sensitive:

P104: "*Not at my level. There's obviously other people here, you know operational managers and things like that that might have more commercially sensitive information but at my level I wouldn't have anything that's that sensitive"*

8 (7%) of them seemed to misunderstand the purpose of security, describing security risks as *confidentiality issues* that can arise from mishandling sensitive information, but were not able to relate those risks to information security:

P51: "*So it's not strict Information Security, it's more commercial information that we have to be aware of"*

In addition 58 employees (49%) also downplayed the need to follow securty advice to challenge strangers they see in the office, as they believed they either had the right to be there or that someone else would challenge them:

P72: "*That's not something I would do as my general process…I think they have to present ID at the door, the security desk that was their name and possibly that they work for a certain company"*

27 others (23%) were confused about the purpose of some organisational security mechanisms:

P107: "*we have got firewalls and other protection, I know incoming emails are scanned for viruses, they are scanned for material that might be inappropriate, so I have got a fair degree of confidence that when things go out, when they are sent out or they come in that they are very sort of screened, and to a degree kept confidential.*"

5.2.1.1.2 Policy awareness

As discussed in the previous chapter, an information security policy was present in the organisation and all employees reported to be aware of its existence. When probed to discuss their understanding of its purpose and its content, 57 (48%) employees reported to be aware of security's importance:

P75: "*So I think this company's quite good at explaining why we need to have security in this manner*"

Policy awareness increased on role-related issues, with 38 (32%) reporting to be more likely to follow security policy clauses related to their day-to-day activities:

P66: "*You know you've got (what) you can and can't do, what you can send through your emails. You know the virus software that's going on, your security ID passwords, checklists, everything like that that goes on. So yeah little bits and bobs I suppose*"

Encrypted USB use (45 – 38%), clear desk and screen lock (52 – 44%) and password sharing (32 – 27%) were the policy clauses most known among employees. Despite the identified employee awareness and policy importance understanding, only 5 employees (4%) reported they visit the policy website to remain up to date with the information there. This suggested that some elements of organisational security

communication were happening outside official organisational channels (this is discussed in detail later in this chapter). In contrast to this, 56 (47%) others ignored organisational policy clauses regarding their role, while 51 (43%) others believed some contents of the policy do not apply to them (e.g. challenging strangers), thus did not follow recommended practices:

P89: "*I'm relatively new and there's a lot of people coming from outside reception that would come – but because everybody else is okay with them, I think it's okay*."

53 (45%) also reported that the security policy appears unimportant both to employees and the organisation (e.g. P52: "*Looking around the office and I can see lots of stuff lying around on people's desks that's been there for a long time. And I don't believe that the 'clear desk policy' is administered or audited on a regular basis. Perhaps the occasional walk but I can't recollect any signs of one recently.*"), with 32 (27%) dismissing its usefulness as a means to protect the organisation: P41: "*Well I mean, it is sort of like a very, I hate to use the word legalese, but it's a document that I've opened up the link before and I've skimmed through it and I said "I don't have a chance to read this." It seems to be very much in audit speak.*"

Perceived non-necessity of the policy led to 104 employees (88%) devising their own ad-hoc security practices (e.g. information handling/sharing strategies, password management strategies):

P95: "*So I always make a point, if I've ever had to give my ID to somebody, I reset my password as soon as I can afterwards… it minimises the risk … I trust people I work with but the point is that you still take the contingency measure.*"

P56: "*if I'm travelling overseas or anything, then I'll use it, if I'm in the office, I'll just use a normal USB stick and then it just sits on there until it gets deleted again. And normally that's not a Company USB stick, that's one that I've bought or been given or something.*"

5.2.1.2 Ineffective training and communication

The policy awareness problems amongst employees identified in the previous section (lack of awareness of policy clauses, perceived non-usefulness of the policy and own interpretation of secure behaviours), suggested a need to examine employee perceptions and understanding of information communicated through organisational security training and communication. When asked to discuss organisational attempts to communicate the need for security, outline organisational risks and potential courses of action to mitigate those, employees spoke of problematic organisational security communication (106 – 90%) and lack of effective security training (75 – 64%), both of which failed to provide risk awareness and motivation to behave securely:

P98: "*You either get lots of communication that's not necessarily relevant and sometimes I think they miss the communication that is very relevant.*"

P55: "*I've never had any formal training. Everything we've been made aware of was on the induction day, "This is your password," and you're drummed in then, "Don't share it," but there's been no formal half day workshops or anything.*"

Employees also referred to training and communication content as overloaded, with information inconsistent and unrelated to their role (44 – 37%). In addition, 14 (12%) of them referred to communicated security practices as "common sense":

P46: "*Off the top of my head it's not something I could really talk about with any authority but I know we did have a computer training that we did fairly recently. It was just things to do with confidentiality and a lot of it was common sense…a lot it's common sense.*"

5.2.1.3 Secure behaviour drivers

Despite the training and communication problems identified, in many situations employees behaved in ways that protected the organisation. Examining the drivers behind those behaviours, in addition to the already discussed awareness about the need for security, a number of other factors were identified that incentivised those. These fell under two categories: (1) *Official* (controlled by the organisation), (2) *Unofficial* (developed outside organisational control)

5.2.1.3.1 Official

These were secure behaviour incentives that depended on the organisation creating the conditions required for employees to behave securely and were related to (1) low security compliance costs for employees, (2) effective communication of related risks and recommended practices from the organisation, and (3) the presence of enforcement procedures and mechanisms.

5.2.1.3.1.1 Compliance easy/supported by environment

Low cost of compliance, stemming from easy to comply security policies, was reported by 47 employees (40%) as a secure behaviour driver. The ease of locking a screen for example was reported as a driver for doing so (P57: "*you can also just do Alt Control Delete and walk away, that's what I normally do").* Easy to use and readily available architectural elements of the security implementation also acted as drivers of secure behaviour for 29 employees (25% - e.g. P55 discussing encrypted USB drives: "*we use the security enabled ones. Well, we get a lot of gifts off suppliers that involve those and some people do use them but I bought for our team all us the security enabled flash drives.*"). In both the above examples, the low overhead of behaving securely made it easy for employees to keep the organisation in a secure state.

5.2.1.3.1.2 Effective communication

Despite the identified problems with security communication, 65 employees (55%) explicitly mentioned that one of the main drivers for their secure actions was the communication of the need for those (as discussed later this does not necessarily mean communication from the organisation's security enforcers):

P86: "*We've just been told not to mention it on social networking sites, because of the critical importance and the kind of environment we live in now, it's best not to share that kind of stuff. It's just company policy, that's the way they want it*."

5.2.1.3.1.3 Enforcement

The presence of enforcement mechanisms and potential consequences (e.g. clear desk inspections) also acted as a secure behaviour driver for 31 employees (26%):

P94: "*There's a very strong clear desk policy, it gets checked fairly regularly, we have sort of office walkabouts where people walk around…a desk that's got masses of paperwork scattered everywhere and some of that is commercially sensitive tends to get picked up as well.*"

5.2.1.3.2 Unofficial

Unofficial incentives were driven by factors elements outside of central organisational control. These were related to: (1) Peer pressure amongst colleagues, together with line manager communication and motivation to behave securely and (2) Past incidents that increased employee awareness of the need for security.

5.2.1.3.2.1 Peer and manager pressure and motivation

Peer pressure and manager pressure were reported as individual secure behaviour drivers by 87 employees (74%).

P74: "*managers will go round and check if anything's left out that's confidential after normal office hours, and people are told that you shouldn't be leaving company confidential information out you should clearly mark it if it is company confidential, and then not leave it lying around*"

P95: "*I have somebody on my team who likes to change the mouse buttons round and turn your screen upside down if you don't, so you get used to locking your screen when you leave your desk.*"

Proactive communication of the need to be secure and actions to remind colleagues about it, was also present in one participant's reports that they remind their managers about the need to lock their screen when they notice them not doing so:

P116: "*But my line manager was not until I insisted that he locked it*."

5.2.1.3.2.2 Past incidents

21 employees (18%) mentioned that awareness of past security incidents acted as a reminder for them to behave securely:

P61: "*When I saw some of the recent security breaches, people losing disks and CDs and laptops, things like that. It is something that I'm aware of and do try and minimise what's on there*."

5.2.2 Effects of friction-inducing security

Despite recognition of the need to protect the organisation, which led to the secure practices presented in the previous section, a significant number of employees spoke of security as something that creates significant friction in their attempts to proceed with their primary tasks. In employee reports, the impact of that friction was articulated in terms of (1) *time*, (2) *cognitive load* and (3) *disruption*.

5.2.2.1 Time

88 employees (75%) discussed time-related problems, emerging in situations where enacting the prescribed security behaviour led to slower completion of primary task related processes. The source of the reported problems was varying, with a number of different mechanisms being reported as friction-inducing: slow connection to the organisational network via VPN, slow encrypted USB drives slowing

down data transfers, or SharePoint setup and access taking significant amounts of time. Employees then had to find other, less taxing ways to proceed with their primary tasks. Problems in the VPN connections for instance, led to 39 employees (33%) maintaining local versions of active files or copying those on unencrypted USB drives:

P111: "*At times we do have to transfer the data to our laptops because the network is slow, response times can be really bad and some of the files are quite large so we transfer them to our laptops to work on and then transfer them back at the end of the day*."

P49: "*You should use an encrypted one but, for ease and generally because, I haven't got an encrypted one so I just use an unencrypted one, whip it across and then just delete the copy off the flash stick which isn't perfect but it's quicker, easier than having to follow the policy*."

Access control setup was also reported as slow and inconsistent by 44 employees (37%), who then resorted to USB and email file sharing:

P64: "*but people send you links to SharePoint areas, saying here's the document in a certain area you don't have access to it because it's in a different SharePoint area that the one you have access to. You have to request access, or, more commonly, they actually send you a copy of the document across. Which obviously (is) against the whole value of having SharePoint access, where you don't send documents across.*"

The slow or unresponsive nature of IT support also led to employees procuring their own access control solutions. A demonstrative example mentioned by 61 participants (52%), involved employees using the system accounts of their colleagues to afford access to information, when immediate access was required and access control setup processes took a long time:

P91: "*That does happen sometimes. It's just partly to fill a gap in IS, you know - because we use lots of systems here, and they take ages to set up, and sometimes when someone joins a team, […] he actually only obtained access to the systems about four months later, when he was going to leave, so in the interim time, he was sort of using other people's logins.*"

5.2.2.2 Disruption

In other cases, organisational security mechanisms disrupted employee primary tasks, completely blocking productivity-related activities. Problems with organisational email filtering and website blocking systems for example, often blocked employee access to work-related information (38 employees – 32%):

P101: "*Sometimes it can be quite frustrating because you are genuinely waiting for work documents to come in from external sources, and where our security's so tight, some of the documents that we're waiting for can't get into us, so sometimes that can be a hindrance as well.*"

In response to the above problems, 7 employees (6%) reported that they had to resort to other non-prescribed practices, devised by themselves and their colleagues:

P2: "*The first trick that was taught to me was you tell them to send it as a different type of file. Change the extension so you can get the file so that you can get your work done*"

P70: "*...Gmail you can't access that and the trouble is that's actually sometimes that would be useful to use as another way of sending emails. And I happen to know that someone was sending me a document that wasn't coming through because our firewall was blocking it. He sent it to my Gmail account and it's still there now. And I was planning when I get an opportunity to print it when I get a chance…At home or somewhere yeah.*"

Other examples of disruptive organisational security provisions included connectivity problems (e.g. VPN connection not being always available), limited capacity of employee's personal network drives and problems with shared drive access. These problems led to 83 employees (70%) storing files locally or on USB drives, and sharing information using USB drives and emails; often reporting to recognise potentially increased information security risks:

P62: "*I do sometimes put it on an encrypted flash drive-y thing just in case I can't log on cause there are times when it doesn't like you logging.*"

P33: "*Then I called and I got 500 more MBs. Then I called and I got 500 more MBs. So, it was, it's difficult for me because I have to call every month to get some additional space. (Easiest to do) for me is to store the work that I do on my office laptop.*"

P107: "*we try and send as much as we can via the e-mail.*" I: "*And do they customer details and things like that?*" P: "*I guess you could identify the address from the information. For that respect for support information it is whatever the supplier requests.*"

Problems were also reported in the organisational process to provide employees with encrypted USB flash drives, with 19 employees (16%) reporting that not everyone has one. As a response they started using their own personal ones:

P115: "*Yes personal USB ones so you can, instead of ordering one through the company they have already got ones they just use their own […] particularly is to move documents from one laptop or desktop to another, if they are a desktop user they might be taking it home to work on their own desktop or transferring it from their laptop onto somebody else's laptop for presentations, meetings.*"

5.2.2.3 Increased Cognitive Load

Another aspect of the organisational security implementation that created problems for employees was the cognitive overload created by friction-inducing organisational security provisions. This stemmed both from the amount of security-related information they had to recall, but also from security mechanisms that appeared to demand high cognitive effort; primarily the need to manage passwords for a large number of systems.

5.2.2.3.1 Password overload

The presence of a large number of organisational systems to which employees had to authenticate to, combined with password expiry windows that varied across those systems, led to a number of different employee responses:

- 31 employees (26%) reported they had to devise their own coping mechanisms to deal with the password expiry window:
  P77: "*I know frequent password changes force people to use a password generating mechanism that's quite easy to guess, because you have to change your password every month, people would use a football team and just add on the number of the month, for instance, if it's May, it's gonna be Arsenal 5. I think people just go round robin, because they have to change their passwords so frequently. Because it takes you probably a week to remember what you've changed your password, and you're comfortable with it, and then all of a sudden you've got to change it again.*"
- 45 (38%) reported they felt necessary to write their passwords down, either physically (e.g. P58: "*I have got a list of passwords written down somewhere unfortunately. I just find there's too many to remember otherwise, and we've got a different username and password most of the time for each of each of the logins, so it's written down on a bit of paper.*") or in digital documents (P71: "*I've got a Microsoft Word document that contains passwords for everything in my life, but mostly work, cause I don't do a lot of stuff on the internet personally…I think the amount of password-protected things leads you to the necessity to write them down, which introduces a risk.*")
- 37 (31%) also reported to recognise the risks involved with this practice and applying self-devised security practices to protect the physical artefact recording their passwords: P58: "*...it's locked in my desk when I've not got hold of it, probably along the laptop, which is probably not too clever.*" or P3: "*I keep them all on a note on my phone. And that's password protected as well*".

5.2.2.3.2 Policy content problems

The second source of cognitive overload reported by 76 employees (64%) was the volume of the contents of the security policy and security-related communication. Both were reported as generic and not role-specific, thus leaving employees having to go through large amounts of information in order to identify clauses relevant to their roles. Organisational pressure to complete primary task-related activities within tight timeframes, left employees with no choice other than completely dismissing the communicated information:

P41: "*You've got probably ten hours of work to do in an eight hour day, you come to work, you look through some kind of weekly highlights of some important email notices you should know about and in one there's a link that refers you to three pages of PC security that you need to know about as an employee. Now, are you going meet that noontime deadline or are you going to go through that?*"

As a response to this information overload, 47 employees (40%) reported they need to decide by themselves on which part of the communicated information they think is more relevant to them and adhere to it:

P64: "*I've read through the policy and try and keep to the policy. Well, I won't say I know it off by heart. I guess you tend to read it, try and get out the salient points for yourself, two or three key cues what shouldn't you be doing, things like not using, common USB sticks to pass information around and things like that which is a recent one that's been put in place and we've got special USB sticks – and never leave a laptop in the back of the car and things like that.*"

5.2.3 Security mediation at team level

A significant proportion of organisational information security management appeared to rely on line managers of local divisions. They were reported as directly responsible for managing a number of security activities within their teams, taking access control decisions, providing security decision support and prescribing behaviours to team members.

5.2.3.1 Line manager and peer support

100 interviewees (85%) reported that central security communication from the organisation is inadequate and that the current organisational setting relies on managers to do so:

P96: "*Well basically we were introduced to the security policy through my team leader. He outlined and gave us a site tour of what we can and cannot do… like you know a door being left open or your computer left being switched on or not been locked or any sensitive information lying on your desk, to be mindful of putting away security information also using a flash drive which are not company issued and stuff like that really*."

In addition to line managers communicating desired behaviours, 68 employees (58%) employees also consulted their line managers and their peers when they need support on security decisions:

P29: "*I know from my point of view being an analyst. If I were to ever share any information with any priority, even if I was not sure I would first go to my manager and ask him about it.*"

In addition, security messages were internalised at team level through discussion or manager/colleague initiative:

P14: "*One gentleman that works in my group gave us a whole workshop at one of our team meetings, on how to create secure passwords. Not to use your pet's name and your birthday, you know, simple things that people could figure out, like your phone number*."

5.2.3.2 Access control – manager authorisation

In addition to communication, 87 employees (74%) reported that their managers are responsible for managing access control within their teams, authorising and granting employee access to data and resources:

P79: "*the manager of each team is responsible for allocating permissions*"

In some cases managers also had to approve centrally-managed access:

P49: "*what would happen is, you fill in a form online saying you need this software, your manager would approve it saying, "Yes, you do need that software for this reason." It gets sent over to IS, they receive the request and send the software down to your laptop.*"

Despite their key role in managing security within their teams, three managers participating in the study reported that no security training was provided to them and they did not have security included in their responsibilities:

"*I: Are you responsible for their security awareness in any sense*?" P98: "*That's an interesting point. That's not something that has ever been particularly made clear to me. I suspect I would take that on board as a normal encompassing responsibility with regards to having people at work for me doing the right thing but I don't recall any specific guideline*".

Examining security-related manager decisions (on communication, authorisation and support), those were usually ad-hoc, based on their own understanding and perception of security risks and best mitigation practices (9 employees – 8%). One manager even explicitly reported that the advice they provide is based on their personal beliefs, not company policy:

P36: "*You know, because my responsibility is protecting the financial data. I take it upon myself to make sure that we're staying abreast of what is appropriate, what's not appropriate. What some of the new requirements may be as they're released. Not that I'm aware of*."

In addition, 16 interviewees (14%) reported that security communication and employee behaviours vary both by location and manager:

P53: "*Again, it's down to the area manager and no one else...the reason I diverted away from policy has been driven by a business requirement*".

5.2.4 Employee perception of security management

As discussed in section 5.2.1.3 employees are motivated and behave securely when easy to use security mechanisms and processes are present: employees reported that if security appears to demand reasonable time or effort and they understand existing risks, they follow recommended practices. Despite being aware on the need for security, when asked to further discuss their security perceptions, employees reported the organisational security implementation to suffer from a number of problems, relating to: (1) impact on productivity, (2) organisational adaptability problems and (3) ineffective security management.

5.2.4.1 Productivity impact

The negative impact of friction-inducing security mechanisms on their primary task, provided justification for non-compliant actions for 90 employees (76%):

P42: "*So I have huge amounts of data that I have stored multiple gigabytes of email of storage going back over 10 years. Very much contrary to the written policies, but if I'm really expected to be able to use past*

experience, I need to be able to use my records for that experience. Email's one of the most convenient ways to do that".

5.2.4.2 Organisational Adaptability

Employees reported that the failure of organisational IT systems to be adaptable and account for changing organisational conditions also caused problems to their primary task. In many cases employees did not have timely access to information necessary for their role, so they had to either wait (6 employees – 5% - P70: "*I think you can now phone them up, IS helpdesk direct and they'll do it there and then…it works in a day or so which is a bit annoying.*"), or resort to self-devised ad-hoc solutions when a problem arose (73 employees – 62%), for example sharing passwords when they encountered problems in delegation/allocation of responsibilities:

P97: "*…I was off for a month earlier this year and because of the resolutions were coming through and no-one had an idea what these resolutions or this packs were not being resolved so I gave it to one of my colleagues for him to go to my e-mail to check for the resolutions.*"

5.2.4.3 Not managed well

Management of security was also perceived as ineffective and inconsistent. When employees were probed to discuss their overall perception of organisational security approaches, 111 (94%) referred to security rules as unhelpful:

P41: "*...they tell you to do some things, but they don't really tell you how to do them*"

Housekeeping around access control, for example, was seen by employees as not being managed properly, with 19 participants (16%) expressing concerns about it:

P66: "*It sometimes takes a week, two weeks, maybe a month before they even get done and it's down to that person really more than anything chasing it to get it done. So if you've got someone who's not really bothered then they've probably still got access to it now.*"

8 employees (7%) also reported that attempts to communicate problems in the security implementation back to security management seem to go unnoticed. The organisation appears as not caring to improve, despite some employees taking action and reporting their concerns:

P53: "*I've raised security issues and you never get anywhere with them. I raised the issue of memory sticks, I also raised an issue where I had a contractor came to work for the company and he was given a laptop. And it had belonged clearly to one of the directors and it had all his information still on it. [..] you could flag your reservations up but they wouldn't be listened to*"

As one employee said, the organisation prefers to attempt to educate people instead of implementing solutions to solve the problems in security employees report:

P97: "*I think they just kept it at one level and just try and educate people instead of actually physically putting things in process*"

In general organisational security strategy was perceived as sanction-driven in theory, but with no effective enforcement in practice:

P52: "*looking around the office I can see lots of stuff lying around on people's desks that's been there for a long time. And I don't believe that the 'clear desk policy' is administered or audited on a regular basis. Perhaps the occasional walk but I can't recollect any signs of one recently.*"

80 employees (68%) also reported that security did not manage to serve their own primary-task related priorities, causing frustration (e.g. closed-built laptops - P66: "*But some of the things I want to take and use in some way that other people have done which would help me quicken my job up I can't do so yeah it can be frustrating.*")

This perceived inflexibility and inability of security management to serve employee priorities, combined with the ineffective communication and training approaches discussed earlier, and the perceived lack of enforcement, led to 68 employees (58%) perceiving security as less important than other organisational issues:

P62: "*I don't see security being driven from the top in the same way as safety and the carbon footprint.*"

5.2.4.4 Culture perception

When probed to discuss the security culture of the organisation 51 employees (43%) described their colleagues as willing to comply and stay secure, but also that everyone in the organisation is driven by productivity targets:

P50: "*But in all honesty I'm not too sure about the Security Policy, I haven't been really introduced to it and in all honesty I've not read it. I actually have not received any formal training regarding Information Security, all I've ever been taught is how to create things.*"

This, combined with the identified lack of awareness of many security issues, led to the development of an organisational security culture where oversharing of information is widespread. 24 employees (20%) reported it as common practice, also recognising the significant risks that emerge from it:

P111: "*We have a part of the site which is only for resource management staff only so only those people can see that part of the site, and then we have the different areas of the business that can only see their part of the of the site. So it is quite a big concern sometimes because we have like three, four hundred staff potentially that could have access to it.*"

Problems and concerns with contractor access were also reported as a concern by 43 employees (36%), who considered treatment of contractors as inconsistent with the security posture of the rest of the organisation:

P66: "*...but also it's not just that but it's internally as well when we have contractors coming in who are replacing people who have been here longer for the sake of saving money...for instance at the moment we've had an instance where this person's sent out a couple of documents that really aren't for private viewing but they're unprotected you know.*"

When discussing their overall perception or organisational security culture, 36 employees (31%) referred to it as static and that the organisation needs to be more proactive:

I: "*So, which way would you say the culture is moving? Is it that, security is getting tighter, or it is weakening?*" P110: "*To be honest from day to day things, I do not really see it moving to be honest.*"

5.3 The Emergence of Shadow Security

The narratives presented in the previous section revealed the existence of a previously unknown behavioural paradigm in organisational security environments; the *shadow security*. Borrowing the term from "Shadow IT" ("employees going around IT to get the IT services they want on their own", Nelson, 2013), shadow security represents "*the sum of self-made security measures created by productivity-focused, but also security-conscious, employees when the organisation's official security implementation does not meet their needs (or are unaware of relevant elements of it)"*. Rather than remaining passive, employees, peer groups, and managers who have their own understanding of security, individually or collectively devise their own adaptations to unsatisfactory security measures, introducing their own workable "secure workarounds": novel solutions, designed to fit their own primary tasks, also perceived as serving the purpose of maintaining security. These workarounds may not provide the same level of security risk mitigation as employees following the official security policy, but they reflect the best compromise employees can find between getting the job done and managing the risks to the assets they use in their day to day tasks. This section presents the drivers of shadow security development, based on narratives identified in the grounded theory interview analysis, also discussing the risks emerging from its development in an organisation. It also presents the lessons security management can learn from shadow security development to deliver more effective protection.

5.3.1 Drivers of shadow security behaviour

The conditions leading to employee deviation from prescribed security practices can be grouped under six major categories: (1) impact of friction-inducing security on employee productivity, (2) lack of organisational response to employees reporting security problems, (3) reliance on local security decision making without providing effective guidance, (4) security communication and training being generic, overloaded, and thus ineffective, (5) ineffective security management perception by employees, and (6) perceived problems in organisational culture that reduce employee motivation to follow organisational processes. This section discusses each of the above, explaining their effect on employee primary task and security perceptions, also explaining how those led to employees having to devise their own adaptations to organisational security.

5.3.1.1 Productivity impact – security-productivity friction

Contrary to the archetypal view of "lazy, ignorant and wilfully disobedient users" held by security managers (Adams and Sasse, 1999), employees appear sufficiently motivated to comply with security and demonstrate some individual capacity to do so effectively. The problems start when security starts negatively affecting productivity. Time overheads, disruption in primary task completion and increased cognitive load in order to deal with security mechanisms, all damage employee ability to proceed with productivity related activities, causing disgruntlement. Employees then come up with their own

solutions, based on their own understanding of what workable security should look like. Inflexible organisational provisions for file sharing for example, led to employees having to either wait for central IT management to approve requested access to resources, or find less taxing information sharing mechanisms. They address this by either (1) sharing information using unencrypted USB drives, deleting the information once file transfer is completed, (2) sharing files using emails (potentially leaving permanent impressions of documents on their local drives) or (3) using third party provisions for document and information sharing (e.g. DropBox), believing that careful access granting solely to their colleagues provides adequate information protection. In the majority of the examples presented in the previous section, participants recognised their chosen approaches as insecure, but provided some reasoning to legitimise their behaviour; either due to compliant behaviour creating unreasonable time overheads, or due to compliance being regarded as simply impossible. Employee self-devised practices are less demanding and less disruptive, supporting what employees believed to be more proportionate and appropriate effort for security behaviour.

5.3.1.2 Lack of feedback response

The second driver of shadow security development comes from employees perceiving the organisation as unable to respond to their reports about security creating problems to employee primary tasks. Employees report to their managers or central security on both primary task overheads created by security mechanisms and potential security risks they identify within their working environment (e.g. problems with access revoking leading to potential unauthorised access to information). In many cases, where the organisational response appears inadequate, employees believe the organisation demands security but does not listen to their feedback. This also negatively affects employees' perceived importance of security to the organisation's leadership, providing additional validation for their decisions to adapt security in their own way when productivity reasons justify this.

5.3.1.3 Communication and training problems

Based on the narratives presented in this chapter, the overall organisational security communication and training processes emerge as dysfunctional. There is limited awareness amongst employees of the existence of security policies and formal procedures that aim to mitigate organisational security risks. Employees also lack accurate knowledge of role-related risks, also perceiving information included in security communication and training as not useful to them. Confusion is also present on how to identify and protect sensitive information, but also on how organisational mechanisms (e.g. physical security desk) may be bypassed by attackers. As employees mentioned, the above problems were a result of:

1. *Lack of effective security training from the organisation*: employees reported that some security training was provided when they joined, with no follow up after that. They also referred to the content as generic and could not recall the desired behaviours described in it.
2. *Security communication emerging as dysfunctional*: sending large amounts of information to all the employees creates a negative attitude towards security managers and security in general. The communicated information is then ignored, dismissed as useless and, when employees are aware of the need for security, drives the deployment of shadow security solutions.

5.3.1.4 Ineffective security management perception

Inability of the organisation to enforce its security policy and respond to reported risks also leads to shadow security development. Non-enforcement of policy (e.g. clear desk) is perceived by some employees as lack of interest from the organisation to achieve security. They then disregard official security principles and behave in ways they know can get away with, to efficiently proceed with quick primary task completion. Their negative perception of security is accentuated by the inability of the existing processes to accommodate for organisational conditions that deviate from normal day-to-day working practices. For example, employees who find the systems in place as not supporting responsibility delegation to their colleagues when they need to go away, find it easier to just share their passwords with them. In addition, employees often identify problems and potential risks in the security implementation (e.g. leavers access not revoked promptly) and even go the extra mile to report those. But, as they said, the organisation appears not to respond to the reported problems, which further accentuates their perception that security is not a top organisational priority.

5.3.1.5 Reliance on local decision making without effective guidance

Deployment and evolution of security behaviour within organisational sub-divisions mostly relies on managers as a conduit. Managers constantly face the challenge of having to communicate behaviours that minimise work-related organisational risks, but also focus on ensuring uninterrupted completion of productivity-related tasks within their teams (e.g. how to seamlessly share information). But the organisation did not provide adequate security support or training to them, so they prescribe practices they see as best fitting (e.g. use self-procured USB drives). This invites the evolution of local, ad-hoc habits and security culture, which may significantly divert from the organisation's policy. The emerging perceived absence of a consistent organisational security position encourages independent action to manage security at team level, based on manager's own knowledge and interpretation. In addition, the lack of effective guidance and enforcement, leads to shadow security through manager recommendation and procurement of own solutions perceived as implicitly permitted by the organisation. Similarly, the procurement of employee-devised strategies is also seen as implicitly permitted by the team manager. As a result, shadow security practices become standard practice (e.g. P118: "*not policy, my own best practice*"), fostering many differing and inconsistent security behaviours within the same organisation; potentially increasing organisational exposure to security risks.

5.3.1.6 Organisational security culture problems

The widespread problems with security mechanisms led to an overall disregard for those. With their colleagues not following the recommended security practices, employees are likely to follow suit, further fostering the development of a non-compliant, ad-hoc and self-devised security culture within the organisation. Deploying self-devised security may initially start as a "one-off solution" (e.g. use an unencrypted drive to transfer data and delete the data immediately afterwards), but can eventually become standard practice amongst team members. When this happens, new joiners are also likely to mimic their more experienced colleagues' behaviours, with the emerging practices becoming part of team security cultures in an organisation.

5.3.2 Effectiveness of shadow security

Shadow security is developed as employees' response to security that creates significant friction with their primary tasks. Revisiting the definition of information security from section 2.1 (a discipline attempting to mitigate risks from identified threats by implementing appropriate controls), shadow security emerges from employees managing security themselves at the individual or team level. They assess the severity of threats and vulnerabilities based on their own risk perception and understanding, adapt existing security goals, and devise their own controls that better fit their productivity requirements. Shadow security then emerges as a realistic form of security, developed as a response to unrealistic organisational demands. The emerging employee-procured security practices may often not be as effective as behaviours and controls procured or advocated by organisational information security management. But, when employees are unwilling to comply with the latter due to high friction, shadow security provides better protection for the organisation than employee non-compliance.

5.3.3 Risks to the Organisation

Despite contributing to organisational protection, widespread deployment of shadow security solutions in an organisation negatively impacts attempts to provide effective, centrally-coordinated protection. Turning a blind eye to this "Do It Yourself" security approach harbours a number of potential risks for the organisation: (1) security develops outside organisational control, (2) shadow security consumes employee security resources (compliance budget), and (3) the perceived security self-sufficiency by employees can lead to alienation from central security.

5.3.3.1 Security development outside security management control

Significant shadow security development can lead to employee security behavioural habits that significantly deviate from official policy, thus reducing security management's ability to monitor and control security behaviour development. In addition, without assessment of the effectiveness of employee-procured security controls, the organisation is left unable to assess the effectiveness of its information security implementation. This loss of control can be accentuated by (1) line managers not accurately understanding security risks, but significantly influencing employee behaviours, (2) development of varying security "micro-cultures" within organisational subdivisions, and (3) emergence of a false sense of contribution towards organisational protection amongst employees. The three above factors are discussed in detail below.

5.3.3.1.1 Inaccurate and insufficient line manager understanding

Ineffective communication of policy and security risks to managers accentuates security development outside organisational control. Managers are the best-placed people to convey desired behaviours to employees within their teams, but without appropriate training, they lack sufficient understanding of the policies and risks that exist within the organisation. The emerging self-devised security advice, leads to the security of the organisation becoming that which managers consider to provide the best fit for their business processes. This can result in behaviours that diverge from the organisation's security policy. Security managers also lose control and understanding of security behaviours, leaving the organisation vulnerable to insecure line-manager advice that can become common practice.

5.3.3.1.2 Security "micro-culture" development

The presence of a shadow security environment can lead to the emergence of a non-compliant organisational security culture. Key stakeholders in the organisation (line managers, for instance) appear to be complicit in the development of shadow security, primarily because it moderates the negative impact of friction-inducing security on productivity: like their employees, they value productivity over security compliance. The absence of a consistent organisational security position, leads to shadow security practices devised at organisational subdivision level, which can result in divergent behaviours developing independently within those subdivisions. The emerging security "micro-cultures" provide freedom for the development of team security folk models (Wash, 2010), which are reinforced by both team managers and team members who aim to support each other in their security decisions. In addition to the immediate risks from the subsequent loss of control and inability to capture current behaviours, the presence of local "security micro-cultures" can also act as an additional level of resistance to organisational security awareness, education and training attempts.

5.3.3.1.3 Emergence of a false sense of security

When adopting shadow security practices, employees rationalise that they acting appropriately to protect the organisation, but their understanding of the risks the organisation faces can be incomplete or inaccurate. This approach could be effective if employees are significantly aware of related risks or choose actions that protect the organisation; but employees cannot be assumed to be security experts. In addition, the identified absence of accurate risk understanding (e.g. "*I delete data from unencrypted USB drive*") demonstrates that employees are not always up to date with current information security threats. In such a case, organisational willingness to let them act as they see fit can significantly increase organisational risk exposure.

Employee and manager own rationalisations also create a false sense of security existence at team level. This provides justification for shadow security behaviours, as employees believe they are contributing to organisational protection, even when they act in contrast to the security policy. When the organisation takes no action against this policy non-compliance, violations and insecure behaviours become a cultural norm. This is significantly risky, as a non-security conscious culture can lead to employees feeling disconnected from security management, perceiving it as unnecessary, thus being less likely to follow centrally-administered security advice. This can act as an additional level of resistance to organisational behavioural change attempts, providing further justification for divergence from prescribed behaviours or current mechanisms.

5.3.3.2 Reducing employee resources available for security

Employee resources expended on friction-inducing security, together with related shadow security behaviours reduce their ability to comply with well-designed centrally-administered security mechanisms and processes. In some increased cognitive load conditions where compliance with official security policy clauses is impossible (e.g. multiple password management without writing those down), the chosen "shadow" employee actions consume their time and effort available to security (e.g. having to maintain a password protected document with their password list, regularly updating it when different systems require a password change). This can quickly exhaust the employee's compliance budget (Beautement at al., 2008), reducing their willingness to comply even with well-designed security mechanisms.

5.3.3.3 Alienation from central security

Friction-inducing technical solutions that the organisation refuses to change or replace cause disgruntlement amongst employees. This can create alienation between employees and central security management, accentuating the existing user-security divide (Albrechtsen and Hovden, 2009), and compounding resistance to centrally-dictated security expectations. This divide can be further accentuated when employee reports of potential concerns (as in 5.2.4) appear to remain unaddressed by central security. Not responding to employee feedback about identified security shortcomings is seen to validate their decisions to adapt security when they believe an alternative solution is needed. When central security support appears inadequate, shadow security practices may indirectly serve to reduce their frustration with security. In addition, attempts to enforce compliance by putting restrictions in place (e.g. blocking certain types of documents from corporate email systems) may partially prevent shadow security practices from developing, but they negatively affect employee productivity, create disgruntlement and can lead to further alienation of employees, who will eventually still manage to find ways around restrictions (e.g. change file extension to get an attachment past the organisational firewall). In general, the development of shadow security signifies the presence of significant problems in organisational security management, with shadow security offering a less taxing alternative to employees. Attempts to suppress this without improving organisational security systems only manage to disengage employees from security management attempts to protect an organisation.

5.3.4 Lessons from Shadow Security

The risks identified in the previous section suggest that the potential for shadow security development should not be ignored by organisational security managers when designing, or attempting to improve existing security mechanisms or processes. As discussed in the previous section, in many cases the presence of shadow security can be a positive sign: instead of staying away from unworkable security completely, employees act in ways they perceive as providing at least some protection. But the emerging practices often do not manage organisational risks adequately. Despite that, shadow security behaviours presented in this chapter revealed a number of insights on employee security behaviours that can be useful to organisational security management, which are discussed in this section.

5.3.4.1 Employees want easy to use security

In general, employees appeared motivated to invest some proportion of their time to keep the organisation secure. The development of shadow security confirms the existence of employee capacity to behave securely. It also suggests that employees are able to relate security consequences to personal practices, which can act as a motivator to improve their security behaviour. They appeared willing to take action to address potential risks when insecure conditions or behaviours were identified (i.e. take care to protect information in transit or behave securely when the overhead is minimal). They also encouraged their colleagues and superiors to act in a secure way, implying that if security enforcers manage to instil appropriate behaviours in employees, these can then be reinforced across the employee base. In addition, the findings of this section reinforce past research and previous chapter reports that security mechanisms imposing minimal additional workload have positive effect on employee compliance behaviours (Beautement et al, 2008). The findings also contradict Pallas' (2009) findings that "an increase of opportunistic behaviour is exactly what can be expected to happen within strongly decentralized settings".

There is sufficient evidence in the emerging behavioural paradigms that employees want security and, what Pallas presents as opportunistic behaviour, is actually their attempt to deploy the required workable solutions that security management failed to deliver. In addition, the results suggest that the value misalignments between security management and employees (principal-agent problem - section 2.6.1) are not as severe as previous research suggested (Gurbaxani and Kemerer, 1999; Holmstrom, 1989; Pallas, 2009): employees felt they were responsible for keeping the organisation risk-free. They even went the extra mile of devising their own "affordable" security provisions when the productivity overhead created by the friction-inducing official security and their primary task activities was perceived as uneconomic.

5.3.4.2 Usable security is still not available to users

Many drivers of shadow security development were a result of the organisational security design not providing employees with workable security solutions. Organisations would do well to consider that shadow security happens naturally and is a valuable indicator that security solutions are not serving the business. When the organisation fails to align security with productivity goals, employees take action, rather than doing nothing or passively relying on the organisation to remediate. For an organisation, ignoring the presence of unusable and friction-inducing security mechanisms and processes is dangerous: errors and workarounds create vulnerabilities (Adams and Sasse, 1999), people ignore security advice that requires high effort for little benefit (Herley, 2009), and systemic non-compliance creates noise that makes precursors of even severe attacks hard to detect.

5.3.4.3 Employees can participate in security

While shadow security practices persist, the organisation has an inconsistent security posture which does not align with its productivity goals. However, the existence of shadow security also suggests the presence of a latent capacity for employees to appreciate and play an active part in the provision of security, albeit driven by their internalised sense of what security should achieve for the primary task. Employees deploy their own security solutions when they believe an easy to follow policy or infrastructure is missing, instead of doing nothing or passively relying on the organisation to remediate. Security management should not encourage shadow security development simply through ignorance. Security experts should be aware of this individual capacity and the potential for employees to consciously consider well-designed and low cost security in their activities. Security management needs to listen and learn from shadow security development

In many ways, perceptions of the organisation's existing security implementations, as elicited from employees, indicate where they believe the organisation has failed to provide them with workable security, adequate security support, or indeed failed to keep the organisation secure. User reaction to an organisation's security implementation needs to be heard, lest it weaken the organisation's security posture: learning from, and not ignoring, employees can enhance security, aligning it with organisational goals and increasing its effectiveness. If users are not heard, they can become disenfranchised, and should they have a legitimate concern about security, they will not remain passive in the face of ill-fitting solutions: they will engineer their own shadow security environment, either individually or collectively. Organisations must be able to recognise when and where shadow security is created, factors that contribute to its development, and in turn how to adapt security provisions to respond to user needs. In order to achieve this there needs to be: (1) recognition of individual employee capacity for consciously

considering security as part of work activities (2) a strategy for engaging with employee security needs, and (3) two-way channels implemented within the organisation that support engagement and dialogue. The emerging employee participation in security design can allow for better alignment of security with organisational productivity priorities, thus improving employee compliance.

5.3.5 Shadow security as a learning opportunity

The above lessons suggest that shadow security development comes as a result of employee attempts to achieve workable security. Its development does not necessarily mean that security as a notion is disregarded, but that productivity-focused employees perceive the provisioned approach to one or more security elements as either inadequate or too expensive. They then solve the emerging productivity-security conflict that the organisation failed to resolve, as best as they know for their specific tasks and risks: rather than remaining passive, employees, peer groups and managers use their own understanding of security, individually or collectively, to devise adaptations of unsatisfactory security or introduce their own novel solutions. Shadow security emerges as the realisation of employee attempts to behave securely, even when provisioned security appears incompatible with their primary task, or dysfunctional security communication provides very limited awareness of security policies and formal procedures.

Effective security management should treat shadow security behaviours as a learning opportunity. Its development and identification can improve understanding of how the existing security mechanisms and processes create security-productivity friction. The emerging employee responses can then provide valuable insights that security management can use to drive security improvements. Further discussion and analysis of how shadow security can be identified and leveraged to deliver effective security are presented in Chapter 7.

5.4 Results validation

As explained in section 3.4 of the methodology chapter, the validity of case study findings can be improved by using different triangulation approaches. To improve the findings presented in this chapter, additional data collection and analysis were conducted in Company A and a second organisation, Company B. This aimed to provide both methodological and data triangulation, improve the validity of the findings and provide better characterisation and understanding of the identified phenomena. This section presents the process and emerging findings of additional data collection and analysis. It also discusses the contribution of this additional research on understanding the evolution of shadow security in organisations and the opportunities it presents for organisational security management.

5.4.1 Methodological triangulation - Survey

As explained in section 3.4.1, a large set of survey data with 1488 employees of Company A was available for secondary analysis. The data was not used to confirm the presence of shadow security, as data collection was already completed before commencing this research; instead, it was used to demonstrate that the behaviours which lead to shadow security identification and definition were widely prevalent in the organisational environments examined.

5.4.1.1 Analysis of results

In order to provide validation for the insecure behaviours identified in the interviews, the analysis of the survey results focused on: (1) verification of employee propensity to act in a secure way and (2) identification of the existence and prevalence in Company A of friction-related insecure behaviours on a wider scale than the 118 interviewed employees.

5.4.1.1.1 Attitude

5 security attitude-related scenarios were analysed to verify the validity of the suggestions presented in section 5.2, stating that employees are aware of the need for security, motivated to protect the organisation, willing to report potential security risks, able to identify insecure practices, and willing to challenge those. This section presents the attitude scenarios included in the interviews, together with the number of employees that responded to each one and the numbers that chose each of the available actions.

1. In a scenario of unsupervised people without a visible visitor's badge waiting near the barrier door and occasionally 'tailgating' to get into the main building, answered by 359 employees.
    a. 123 (34%): Notify security that you have observed visitors tailgating past the barrier.
    b. 206 (57%): Confront the people tailgating, ask them to show you some ID (if they are not known) and supervise them back to reception.
    c. 16 (5%): Assume the people have access and have been checked by the reception staff and continue with your work so as not to disrupt their work or yours.
    d. 14 (4%): Confront the people and then report their names to either your manager or security.
2. Identification of access to information and sharing with others by people not gone through vetting process to handle sensitive data (796 employees)
    a. 581 (73%): Report observations to manager, and urge them to take action.
    b. 107 (13%): Send violators an informal email, reminding that sharing sensitive documents with non-cleared employees is not allowed.
    c. 107 (13%): Initiate an audit of other department to attempt to track the use and distribution of the sensitive documents.
    d. 1 (1%): Do nothing - If something goes wrong, the Senior Manager in charge of the department that is sharing the information will be held responsible.
3. Colleague often prints out confidential documents to work whilst travelling on the train to/from home - not always using the Confidential, but normal recycle bin as the paper will be destroyed when it is recycled anyway (133)
    a. 0: working practises are acceptable; recycling the paper is good for the environment and destroys any sensitive information at the same time.
    b. 95 (71%): Should ensure any paper copies are disposed of specifically in a confidential recycle bin to ensure secure shredding once finished with them – hard copies are a major source of information leaks.
    c. 0: Is right to work in the way that suits him best – without access to the company systems even if someone did get hold of a few bits of information they couldn't damage the company anyway.

d. 38 (28%): Employee is totally reckless with customer's information – should stop printing out work unless it is absolutely necessary.

4. Notice a blue van parked outside the entrance gates - several times over the last couple of weeks. Inside are two individuals who appear to take pictures of the building/people around the building. As soon as the individuals are noticed, the van pulls away in a hurry. (347)
    a. 1 (1%): Ignore it. The van was there several times and nothing has happened at the site so it probably isn't a threat.
    b. 53 (15%): Report the incident to line manager; it is better to report such incidents even if no obvious breach is noticed.
    c. 292 (84%): Report suspicions directly to security so they can take the appropriate action.
    d. 1 (1%): Do nothing now but keep an eye out for the van in the future to confirm his suspicions. Report if it shows up again.
5. Employee notices that several confidential documents/records were missing and there was no audit trail of who had used them last. Colleague behaves weirdly and objects to being challenged (877)
    a. 8 (1%): Do nothing, colleague has always been eccentric
    b. 581 (66%): Discuss colleague's behaviour with the department manager – it isn't acceptable for an individual in the department to have their own methods.
    c. 8 (1%): Accommodate their work practises by adjusting their own.
    d. 280 (32%): Call the Business Conduct helpline and make a report about colleague's behaviour – it is suspicious that there appears to be no proper audit of his work.

The above results confirm the identified employee awareness of the need to protect the organisation: the majority of employees chose actions that indicate an understanding of the risks related to potentially insecure behaviours. They were also willing to take action when they observed such behaviours, either directly or, most of the time, by reporting potential concerns to appropriate authorities.

5.4.1.1.2 Behaviour

After confirming the existence of employee awareness of the need for security, 5 behaviour scenarios were analysed to identify employee chosen courses of action when security requirements created primary task overheads.

6. Problematic SharePoint setup scenario (slow approval, need for urgent access - 877).
    a. 74 (8%): Request that those with access share their (main log-in) account details and passwords with others to allow them access to the information.
    b. 261 (30%): Burn a copy of the files onto a CD/DVD and distribute to the work group.
    c. 412 (47%): Email the document archive directly to the general work group mailing list using your company email address.
    d. 130 (15%): Move the files to an unrestricted folder on the internal network to allow the work group to have continued access to it.
7. Problems in delegating access-granting responsibilities when going away. In addition, guidelines for granting access are not always clear and require some degree of discretion (865)

a. 154 (18%): Leave password with secretary who, although temporary, is a trusted employee, with instructions to use account to resolve "emergency situations".
b. 454 (53%): Leave password with a trusted member of the department and ask them to handle "all decision making" while they are away.
c. 64 (7%): Grant blanket access rights to the whole department for the duration of absence.
d. 193 (22%): Give out login details of a range of access permissions (used by temporary workers) with instructions that they be used where existing permissions do not allow access.

8. Unavailable encrypted USB stick, client presentation includes embedded media too large to email, problems accessing internal network from outside (133)
    a. 49 (37%) Take the required data on an unencrypted USB stick they have available.
    b. 61 (46%) Borrow an encrypted stick from a colleague - make a note of their password. Colleague asked not to share / erase the confidential data already on the stick.
    c. 13 (10%) Use the available unencrypted stick to put a copy of the data on a colleague laptop and ask them to take it to the client's site.
    d. 10 (7%) Upload the files to a public online storage service and recover at client's site.
9. Occasionally works from home in the evening, gets there by train. Leave laptop at work - recently had it stolen. Backup all work files on personal computer to access without having to connect to the company system - home network connection is not always reliable. Knows this is against policy, but lives in a safe neighbourhood. To transfer files to home computer, uses a variety of methods (278).
    a. 60 (22%) Use own USB sticks to carry current work on the train.
    b. 15 (5%) Email files to your personal email account and download at home.
    c. 11 (4%) Use an online storage service such as DropBox, deleting files once you have made a local copy.
    d. 192 (69%) Log in to the company VPN and make local copies via that connection.
10. Contractor asks for some commercially sensitive information not publicly available through the company's web site without following request procedure 3rd-parties need to go through. Contractor becomes persistent, reminds that they used to be colleagues, mentioning the names of several senior people in both companies that would be extremely unhappy if she does not get this information that day. Also says she is still in contact with line manager and will explain everything to him later, so it should be ok to provide this information today. (359)
    a. 28 (8%): Accede to the request for information to ensure that senior personnel are satisfied and contractor' productivity isn't hampered.
    b. 18 (5%): Send the information requested but immediately inform line manager of what information has been provided.
    c. 29 (8%): Ask specifically which pieces of information contractor needs - send through a redacted or edited version of the documents.
    d. 284 (79%): Send the information through but password protect the file and wait until they have spoken to line manager before releasing the password.

5.4.1.2 Survey discussion

The attitude scenarios provided additional evidence of employee goodwill and understanding of the need to take action and contribute to delivering organisational security. The majority of employees were willing to act when they identified potential security risks, challenge insecure behaviours of their colleagues, report violations to central security, securely dispose confidential information, and discuss security concerns with their line managers. Despite the identified willingness to act securely, the behaviour scenarios demonstrated that when security created problems in proceeding with their primary task activities, a large proportion of employees chose to proceed with insecure options (e.g. sharing credentials, using unencrypted drives, emailing sensitive documents). These findings strengthen the results of the interview analysis, suggesting that employees consider non-compliant behaviours as acceptable when they encounter friction-inducing security.

5.4.2 Data triangulation - Company B

The survey results from Company A verified the identified employee willingness to bend security rules and bypass mechanisms that create significant overheads or disrupt their primary task. Despite that, they provided little evidence to support the emergence of shadow security as a response to this productivity impact. In order to improve the validity of the identified paradigms on shadow security development discussed earlier in this chapter, data triangulation was also required. As discussed in section 3.4, cross-case data triangulation can significantly improve the validity of paradigms emerging from case study research. In order to do so, a similar interview set from the second partner organisation, Company B was collected and analysed, with a second survey also taking place to confirm identified behaviours (details on the interview data collection process are presented in 3.2.1). The remainder of this section summarises the results of the interview analysis from 82 Company B interviews and uses the narratives identified in the new analysis to revisit the shadow security paradigms identified in Company A. It then explains how the new analysis allowed confirmation of the presence of shadow security in organisations and its impact on employee behaviours or the organisational environment.

5.4.2.1 Interviews

The question set for the semi-structured interviews was very similar to Company A, with small adaptations to reflect identified differences in the organisational environment between the two organisations. The analysis process followed was also the same as Company A (section 5.1), using the grounded theory process of open, axial and selective coding (the emergent grounded theory categories can be found in Appendix I).

5.4.2.1.1 Security awareness and compliance

The majority of employees in Company B (78 – 95%) reported that they see value in security and the benefits it can provide to the organisation. As a result, when mechanisms or recommended behaviours demanded reasonable time or effort, secure practices were present (e.g. taking care to protect their corporate laptops to protect both company property and the information stored on those). Employees were also willing to challenge their colleagues and reported to actively do so (77 - 94%).

5.4.2.1.2 Secure behaviour drivers

The presence of supporting mechanisms and procedures (mostly absent from company A) was reported to encourage secure behaviour. Employees mentioned, for example, that quick access control setup (43 – 52%) and easy password resets (29 – 35%), reduced the need for password sharing. In addition, the presence of a usable password manager, reduced employee need to write passwords down (38 – 46%). 55 others (67%) reported that the presence of Non-Disclosure Agreements on some projects led to taking more care when dealing with project-related information. Perceived responsibility, peer and manager pressure were also reported as drivers for secure behaviour for the majority of Company B employees (70 – 85%).

5.4.2.1.3 Effects of burdensome security

A number of friction-inducing elements of the organisational security implementation were identified that affected employee primary task completion ability, or increased the perceived effort required to follow secure practices. This led to a negative attitude towards security and provided justification for insecure employee behaviours. The identified friction-inducing mechanisms and processes were categorised based on the workload impact categorisation devised during company A interview analysis, presented in 5.2.2: (1) Disruption, (2) Time and (3) Increased cognitive load[25].

5.4.2.1.3.1 Disruption

When systems in place prevented completion of primary-task related activities, employees devised their own procedures. For example: in order to help employees manage their credentials for different systems, the organisation deployed a password manager that stored employee username and passwords on their computers. 52 employees (63%) mentioned that the provided software did not work for all systems they had to authenticate to. As a result, they resorted to writing their passwords down (either in physical or electronic form) and then took self-devised measures to protect the password storage location (e.g. encrypting password holding document, or carrying notebook with passwords with them all the time)

5.4.2.1.3.2 Time

Employees also reported that they avoid mechanisms that slowed down their primary task completion, choosing to adopt other less-disruptive practices. Problems with setting up team access to organisational data sharing systems for example, led 64 employees (78%) to use email or other external third party services (e.g. DropBox) to share files; they assumed those provide adequate protection for their corporate information. As one employee (PB40) explained, fine-graining access within DropBox to only include colleagues' accounts is a "secure enough" approach.

5.4.2.1.3.3 Increased cognitive load

The interviews also revealed that, when the amount of information employees had to memorise in order to behave securely became unmanageable, they resorted to other, less strenuous activities. The large amount

[25] For space and readability reasons I will not present the full list of the narratives that emerged from the analysis at this point, but they can be found, together with related interview extracts in Appendix I

of information included in the organisational security policy, together with training and communication content appearing irrelevant to their day to day activities, led to employees perceiving policy, training and communication as "tickboxing" exercises required just to pass organisational audits or comply with regulatory requirements. 66 employees (80%) dismissed policies as irrelevant, interpreted desired secure behaviours in their own way, and sought support from their line managers and colleagues when in doubt on what a secure course of action would be.

5.4.2.1.4 Team level security mediation

Similarly to Company A, a large proportion of security mediation in Company B happened at team level. Employees sought support from their line managers when they encountered problems with security, or when they were uncertain on the actions required to keep the organisation safe. In addition to providing support, line managers were often also responsible for authorising access to information, systems and resources. This reliance on managers was not formalised in their responsibilities or the security policy though, and the lack of accurate policy and security understanding led to managers adopting approaches they themselves deemed as more appropriate to protect the organisation (65 employees - 79%). These approaches were often devised outside of central security control, giving rise to a number of shadow security practices, this increasing organisational exposure to potential risks (e.g. the example in the previous section about DropBox use when corporate file-sharing systems created problems – for more examples please refer to Appendix I).

5.4.2.1.5 Security perceived as ineffective

The identified problems in the security implementation, combined with weaknesses employees saw in organisational security management (e.g. access revoking for people leaving the company being slow or using CBT completion rates as an indicator for security), and the observation of various insecure behaviours around them (e.g. over-sharing of information), led to them perceiving the organisation as unable to provide effective and usable security. As a response, 67 employees (82%) reported they devise their own security solutions. Problems with organisational back-up systems for example, combined with limited network storage space, led to employees deploying their own backup solutions by using personal (or team) drives, outside of central information systems controls; in some cases those drives were even reported to be unencrypted.

5.4.2.1.6 Culture perception

As with Company A, employees reported that organisational culture is mostly productivity driven. The variation in behaviours across different organisational locations and the perceived need for the organisation to be more proactive, led to the belief that it is OK to bypass security (or procure own solutions) when it created primary task problems. This led to the emergence of varying norms and security micro-cultures across different organisational subdivisions (clear desk behaviour for example, differed significantly between employees based in two different organisational sites).

5.4.2.2 Survey

Aiming to confirm the identified employee willingness to bypass security when it created excessive primary task friction, a survey was also conducted in Company B, confirming the results in a similar way to the findings of the survey in Company A: employees appeared security risk-aware and willing to

challenge insecure behaviours of colleagues or outsiders, but also willing to bypass security when it created significant negative impact on their ability to proceed with their primary tasks (for the full survey analysis and data please refer to Appendix J).

5.4.3 Revisiting shadow security

5.4.3.1 Drivers of shadow security development

The drivers behind shadow security development in Company B were based on the same elements of the organisational security environment as Company A: (1) productivity impact of friction-inducing mechanisms, (2) problems in security training and communication, (3) lack of feedback response, (4) problematic security management perception, (5) reliance on local decision making without effective guidance, and (6) insecure culture development.

5.4.3.2 Lessons learned from Company B

In addition to verifying the drivers of shadow security behaviour, the Company B analysis led to identification of an additional property of shadow security development: ill-though organisational attempts to address some of the emerging insecure behaviours can only alter the nature of the problem, without fixing it. For example:

- Company B deployed a password manager, aiming to help employees manage the many passwords they had. But problems in its operation (did not work with all systems employees needed to use), turned a cognitive load problem (having to remember the passwords) to a disruption one (a security mechanism not working). This still leaves employees having to manage the emerging security-productivity friction, justifying potential decisions for deployment of shadow security solutions.
- Connectivity to organisational systems from outside the organisation through VPN was reported as very good, preventing the emergence of disruption identified in Company A analysis from problematic network connections. The lack of available individual network storage for employees though, ended up changing the nature of the disruption employees faced from lack of connection to lack of storage. Consequently, employees had to use other means to store and backup information (local storage on laptops and personal external drives for backup), and deploy their own security on those (e.g. take initiative to encrypt external drives).

5.5 Revisiting Research Questions

1. Do employees understand the need for security mechanisms in the organisation? If yes or no, why?

The interview analyses revealed some general awareness and understanding amongst employees about the need to protect organisational information. Despite that, they appeared to ignore many of the security policy clauses explaining how to act in order to achieve that protection. The findings presented in this chapter suggest that the main reason for this was the ineffectiveness of organisational security communication and training (scarce, not followed up, and mostly based on generic content that provided no visible benefit to employees). This led to employees dismissing the communicated information, turning to their line managers for support or selectively applying the principles they themselves identified as relevant to their roles (section 5.2)

2. *What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?*

Security causes disruption and slowdown to employee primary tasks, or unmanageable cognitive load. They respond to this by devising their own, or adapting existing security solutions, to achieve the level of security they perceive as necessary, while minimising its impact on their primary task activities. This shadow security development process can happen both at an individual level (employee devising own low cost solution to a security challenge) or team level (solutions are devised by colleagues collectively and/or also advocated by their line managers). Employees also take additional actions to report the existence of disruptive security mechanisms to their managers or central security.

3. *When organisational security provisions appear to provide inadequate risk mitigation, what do employees do?*

Employees find themselves in situations where they identify potential security risks (e.g. the need to protect their laptop) for which an official policy did not exist, or they were unaware of it. As a result, they devised their own solutions, often advocated by their managers in team meetings (e.g. don't leave laptop in car).

4. *How do employees respond to a perceived lack of organisational security support? What are the risks from their behaviours and what can organisations learn from those?*

Lack of organisational support (e.g. not responding to employee reports of problems with security mechanisms or potential risks that are left unaddressed) leads to employees justifying their decisions to procure self-/team-devised solutions. This increases the risk of security behaviours developing outside central security control, suggesting the need for an organisation to improve its security implementation, based on lessons learned from employee behaviours. Organisations need to recognise that if they appear not to care about security, employees will have minimal incentive to follow the practices prescribed in security policies.

5. *How can the improved understanding from the previous questions be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?*

Employees respond to friction-inducing security mechanisms using the resources they have available (e.g. lack of connectivity leading to storing files locally), deploying shadow security solutions to deliver some security protection. When these solutions become common practice, the organisation loses control of security management, reducing alignment of deployed security approaches with organisational security risk appetite. This calls for a security management approach that will allow adapting friction-inducing elements of the existing organisational environment to ones that can provide effective security protection; as discussed in section 2.8.4, for most organisations redesigning security from scratch is not an option.

The definition of shadow security as the "*sum of self-made security measures created by productivity-focused, but also security-conscious, employees when the organisation's official security implementation does not meet their needs (or are unaware of relevant elements of it)"* provides a good starting point to

deliver workable and secure approaches. Organisations can use shadow security as an indication of what mechanisms create friction between security and primary tasks, but also to identify employee awareness and current security behaviours; shadow security can act as a starting point for workable security, providing the basis for effective organisational protection (for further discussion on how this can be done please refer to Chapter 7)

6. What trust relationships develop in an organisation and how do they influence security behaviours?

A number of the identified paradigms presented in this chapter suggest that trust relationships exist in the organisation that also influence employee security behaviours. For example, the action of employees to share passwords with colleagues despite security policy prohibition, suggests the presence of mutual understanding that their colleagues will not report their policy-violating action. To identify, understand and characterise those relationships and their effect on employee security behaviour, an additional grounded theory analysis on both the Company A and B interview sets was conducted, presented in the next chapter.

Chapter 6: Trust and security behaviours

The findings of the analysis presented in chapter 5 provided preliminary evidence for the existence of trust in the organisational environments examined, together with its influence on employee security behaviours. A number of different situations were identified where the organisation did not attempt to enforce the content of the security policy through assurance. Instead of implementing mechanisms to enforce or detect non-compliance, the organisation relied on its employees to behave as instructed. In Company A for example, employees were given the freedom to manage access rights for their documents, while in Company B information classification requirements relied on employees assessing the sensitivity of information and marking documents appropriately. The findings also identified instances where employees showed trust towards their colleagues: they shared their credentials with them to aid quick system or information access (an action prohibited by the security policy) and shared sensitive information outside official organisational channels. Employees considered both these behaviours as necessary to proceed with their primary task-related activities, when they came across friction-inducing security. In other cases, they left their screens unlocked because they knew the people physically present around them, so the perceived risk of not following the policy appeared to be lower. As discussed in sections 5.2 and 5.3, employees often recognised the above practices as potentially increasing organisational risk exposure, but provided efficient primary task completion as a justification for their actions.

Despite the identified indicators on the presence of trust and its influence on employee security behaviours, the findings presented in chapter 5 were insufficient to provide solid conclusions: the focus of the grounded theory analysis was not to examine the role of trust on security behaviours, but the drivers behind insecure behaviours and the impact of friction-inducing security on employee security practices. As a result, further analysis of the available dataset was required, to examine the existence and the prevalence of trust relationships in organisational environments, characterise those and identify their impact on employee security behaviours. Aiming to deliver this understanding, this chapter discusses security-related trust development in organisations based on a secondary trust-focused analysis of the available interview sets. It starts by presenting related literature on trust in organisational environments, together with a framework of trust interactions developed by Riegelsberger et al. (2005) and its application to organisational security behaviours by Fléchais et al. (2005). The chapter then presents a new grounded theory analysis, examining the development and impact of trust relationships in Companies A and B. Using the results, it then identifies two different security-related trust relationships in organisational environments: (1) *organisation-employee trust* and (2) *inter-employee trust*. The chapter also explains how the two relationships often come to conflict, with employees having to choose between keeping the organisation secure or preserving already established trust relationships. It also presents the impact of trust on shadow security development and the risks from the emerging behaviours that organisations need to address.

6.1 Trust, risk and uncertainty

Trust plays a vital role in the modern world: most economic, political and societal agreements strongly rely on the ability of two or more parties to trust each other, enabling collaboration to achieve mutual

benefits. The presence of trust allows parties to engage in transactions where increased *risk* and *uncertainty* exist (Giddens, 2013). *Risk* arises for a *trustor* (the transaction partner who moves first) when they cannot control the actions of the *trustee* (the person on which the trust is placed). By making the first move in the transaction, the trustor then stands to lose something of value (valuable information, time or money). The less information a trustor possesses about the *ability* and *motivation* of the trustee to hold up their part of the commitments made, the higher the *uncertainty* they face on the outcome of the transaction (Deutsch, 1958). Based on this risky and uncertain nature of trust placement, Mayer et al., (1995) define trust in social interactions as: "*the willingness to be vulnerable based on positive expectation about the behaviour of others*", or, as Clark (2014) put it, "*to assume that the other party will act in my best interest*".

6.2 Trust-warranting properties

Despite the existence of risk and uncertainty, a trustor may consciously decide to expose themselves to the trustee's actions, due to potential benefits they may receive from the trustee's later fulfilment. On a single transaction basis, a trustee would be better off defecting after receiving the benefits of the trusting action: they have already received all the potential rewards from the transaction, so they are at a point of maximum gain, having invested minimal effort. Any attempt to fulfil their part, honouring the trust shown towards them, requires investment of additional resources that will reduce their net benefit compared to the pre-fulfilment state (Sasse and Kirlappos, 2014 – Figure 10).

$$Trustee's\ net\ benefit = Transaction\ Rewards - Effort\ invested\ for\ fulfilment$$

Figure 10: Trustee benefit equation (Sasse and Kirlappos, 2014)

Fulfilment motivation for the trustee comes from the existence of *trust-warranting properties* (Bacharach and Gambetta, 2001): properties of the environment or the parties involved, the long-term effects of which outweigh immediate non-fulfilment gains. These trust-warranting properties can be distinguished between *intrinsic* and *contextual*, based on the factors that drive their development (Figure 11).

6.2.1.1 Intrinsic properties

Intrinsic properties are relatively stable attributes of the trustee that affect their *ability* and *motivation* for fulfilment in the trust transaction. *Ability* of a trustee characterises the possession of the resources or knowledge required for fulfilment of the trustor's requirements. *Motivation* on the other hand stems from existence of factors internal to the trustee that provide incentives for trustworthy behaviour (e.g. propensity to do good, personal costs of breaking trust). It is driven by internalised norms or benevolence that dictate doing what a trustee perceives to be "the right thing" and provide non-monetary fulfilment rewards to the trustee, like personal satisfaction. Essentially, intrinsic properties provide motivation for a trustee to behave as the trustor expects, without any immediate gain from fulfilment.

6.2.1.2 Contextual properties

Contextual properties are attributes of the context of the interaction that provide motivation for trustworthy behaviour by dis-incentivising non-fulfilment. Their presence creates incentives for self-interested trustees to fulfil in a transaction, in order to gain potential short and long term benefits, also

avoiding potential negative consequences. Depending on the conditions that drive their development, contextual properties can be *temporal*, *social* or *institutional*:

- *Temporal embeddedness*: Non-fulfilment can damage the potential of future trust shown towards the trustee. The prospect of benefitting from future interactions becomes an incentive for fulfilment (Axelrod, 1980).
- *Social embeddedness*: Performance information about a trustee's past behaviour may be shared amongst trustors. The potential for reputational damage from fulfilment failure leading to reduced future trust placement can act as a fulfilment incentive for a trustee (Corritore et al., 2003).
- *Institutional embeddedness*: The presence of external enforcement authorities penalising non-compliance also acts as a non-fulfilment deterrent for a trustee (Schneier, 2012).

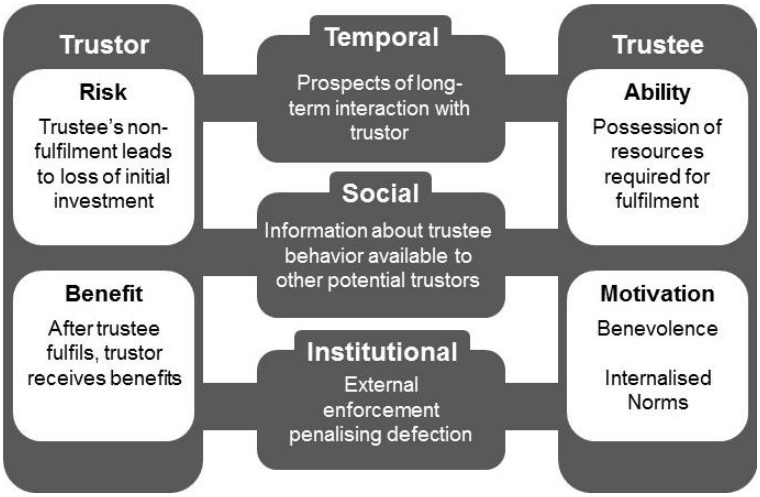

Figure 11: Model of a trust interaction (adapted from Riegelsberger at al., 2005)

6.2.1.3 Intrinsic vs Contextual properties

The important distinction between intrinsic and contextual properties is to whom the trustor's trust is placed. Intrinsic properties lead to the development of *party trust*: trusting the other party's (trustee) internal ability and values. Contextual properties on the other hand lead to *control trust*: the trustor relies on the existence of mechanisms that dis-incentivise non-fulfilment by the trustee (Tan and Thoen, 2000). Fulfilment due to control trust does not imply a trustee is intrinsically trustworthy, as trustworthy behaviour is a result of external factors and motivation for long-term personal benefit, but in most cases it is "*good enough*", as it still allows for successful transactions (Riegelsberger et al, 2005).

6.3 Trust and organisational security

Examining the available literature on information security in organisations, limited previous research was identified on the development of trust relationships in organisations and their effect on employee security behaviours. To the best of the researcher's knowledge, the only past attempt to do so was the work of Fléchais et al. (2005), where they adapted a model of trust in technology mediated interactions by Riegelsberger et al. (2005) to discuss how trust affects security behaviour in organisations, also providing some suggestions for improving trust management by security managers (presented and discussed later in

this chapter). This section presents the rationale behind conducting further research on the relationship between trust and security, presented later in this chapter. It starts by bringing together research on the impact of trust in organisations and past research on information security behaviours. It then revisits the drivers behind insecure employee behaviours identified and discussed in chapter 5, presents the economic impact of trust and assurance in security implementations, discusses the strengths and limitations of Fléchais et al.'s suggestions, and explains why further research was required.

6.3.1 Trust and security management

In an organisation, security management is part of a wider socio-technical environment, where the primary target is effective and efficient completion of production tasks (Brostoff and Sasse, 2001; Weirich and Sasse, 2001). The existence of trust in that environment significantly contributes in realising organisational goals: it aids the development of social norms amongst employees, improving collaboration and leading to more effective production task completion (Mayer et al., 1995). Despite this important role, the term *trust* is currently heavily misused in information security management; it is primarily used to describe what security experts call *trusted components*: *"systems or components whose failure can break the security policy"* (Anderson, 2008). This definition refers to system components (hardware or software), certified to exhibit a specific behaviour under specific conditions. Essentially, by referring to trusted components, security experts refer to assurance mechanisms that have been rigorously tested, often accompanied by appropriate "certifications of trustworthiness". Revisiting the definition of trust presented in section 6.1 ("*…vulnerable based on positive expectation about the behaviour of others*"), the current use of the term by security managers needs to be reconsidered: the only element in a security implementation that can potentially break the security policy is the people who use the systems in place. In addition, positive expectations exist by the organisation on employee values and corresponding behaviours, as total control over their actions is both impossible and impractical. Trust then emerges in the organisation when the impossibility of controlling what employees can do leads to security managers choosing to trust and encourage them to behave in a secure manner, instead of attempting to enforce stringent security (Fléchais et al., 2005).

6.3.2 Employee trustworthiness and security violations

Organisational research has already proven that employees are emotionally attached to the organisations they work for (Love and Singh, 2011; Rousseau, 1989). The findings from the research presented in chapters 4 and 5 of this thesis also showed that, when employees understand related risks and the need for security protection, they are sufficiently motivated and capable to act appropriately to protect the organisation and its information. Despite this, current organisational security approaches, often treat employees as untrustworthy, implementing excessive restrictions, mostly driven by "just in case" security management attitude (Silowash et al., 2012), or regulatory requirements for such restrictions (section 2.5.3). Chapter 5 identified many instances of this: security communication, for example, was overloaded with information that was irrelevant to many employees' day-to-day tasks (section 5.2.1.2), while systems or information access granting decisions administered by central security made the approval process slow (5.2.2.1). These excessive restrictions leave security-aware employees having to deal with strict policies and disruptive mechanisms that are either impossible to use or comply with, or that negatively affect their

ability to proceed with their primary tasks. So, as section 5.3.3 explained in more detail, they end up having to choose between:

1. *Accepting the primary task impact of friction-inducing security*. An employee, and their colleagues and managers, accepting the delay in completion of a productivity-related task caused by high-cost security mechanisms (e.g. waiting for formal request for information access to be approved).
2. *Ignore recommended practices*. Employees resorting to actions explicitly prohibited by the organisation's policy in order to proceed with their primary tasks (e.g. use unencrypted USB drives to share data with colleagues when encrypted ones are slow and take too much time – section 5.2.2.1).
3. *Adapt existing security solutions, or create their own*. This leads to employees creating and deploying *ad-hoc* security deployments outside security management's control (either individually or collectively at team level), leading to the development of *shadow security* practices described in sections 5.2 and 5.3. Password sharing, for example, is used when an employee's colleague needs urgent system access, often impossible to achieve through official organisational processes (section 5.2.4.2). Recognising the need to maintain security, some employees take the additional step of changing the shared password afterwards, considering this a sufficient action to mitigate potential risks emerging from their policy violations.

The shadow security behaviours presented and discussed in Chapter 5 suggest that productivity-focused employees often resort to (2) and (3) when they come across friction-inducing security: they ignore or bypass official security and devise their own ad-hoc solutions that better serve their productivity needs. This leads to security spinning out of organisational control, with the emerging protection being based on employee-devised practices, potentially increasing organisational risk exposure due to inaccurate employee risk awareness. Any attempts to eliminate such behaviours by threatening employees with sanctions essentially weaken organisational defences. They also fail to include employee propensity to behave securely in information security management; especially when the organisation is unable to enforce those sanctions, due to widespread non-compliance making effective monitoring, detection and punishment impossible (section 2.6.3).

6.3.3 The economics of assurance and trust

For an information security manager, the definition of trust presented in section 6.1 ("*willingness to be vulnerable…"*) may sound unacceptable, given their role in protecting the organisation: protection of organisational information requires identifying security vulnerabilities and applying appropriate risk mitigation actions. But the need for trust development in a security implementation needs to be seen in the context of expected benefits. Trust-related risks are taken because the risk taker (the trustor) hopes to gain some benefit from a trustee's fulfilment; in the organisation's case an economic one: the economic benefit of trust-based transactions lies in the resource savings emerging from the reduced need for legal frameworks, policies, and technical controls required to detect and enforce violations (Fléchais et al., 2005). Organisational security management not only pays a cost for the operation of excessive controls (Pallas, 2009), but also creates constraints for honest employees that end up negatively affecting organisational productivity (e.g. the need to file requests to let legitimate websites through the corporate

firewall and subsequent slow response from the organisation described in section 5.2.2.2 – for more examples on security controls negatively impacting employee productivity see section 5.2). In addition, security implementations based primarily on rules and enforcement may deliver effective risk mitigation, albeit at a higher cost, but they prevent trust from developing in the organisation (Clark, 2014). This prevents the organisation, its employees, and its security managers from reaping the second-order benefits of trust development; those include enhanced cooperation, goodwill, adaptability, and creativity to address new problems (Handy, 1999). In order to enjoy the potential benefits of trust, information security management requires better understanding of its role in security behaviours. The need for this understanding acted as a motivator for the research presented later in this chapter.

6.3.4 Using trust to manage security behaviours

As explained in the previous section, security management currently neither recognises, nor attempts to manage the effect of trust on employee behaviours. In an attempt to aid the development of an approach that allows for better security-related trust understanding and management, Fléchais et al. (2005) adapted Riegelsberger et al.'s model of trust interactions, examining the impact of trust-warranting properties on employee behaviours.

6.3.4.1 Secure behaviour drivers

Fléchais et al. start by suggesting that an organisation should not aim to achieve total assurance, if employees exhibit the intrinsic properties required to behave securely. Well-trained employees (*ability*) that understand the risk mitigation effects of trustworthy behaviour (*motivation*) are likely to act in ways that protect the organisation, even with minimal assurance in place. This was also discussed in section 5.3.4: employees do want security, it just needs to be affordable.

In addition to intrinsic motivation, Fléchais et al. also suggest that existence of contextual incentives can also affect security behaviours:

- *Social embeddedness*: (Weirich and Sasse, 2001) report that newcomers' security behaviour follows that of members of their immediate work team, even after receiving security training as part of their induction. Their desire to "fit in" with their colleagues is usually stronger. As a result, when the team culture is security aware, employees are more likely to behave in a secure way.
- *Temporal embeddedness*: This is used by organisations to reduce risks from employee behaviour when they have minimal incentives to expect future interaction and associated benefits. Disgruntled employees ready to leave a company, for example, may be willing to cause damage to systems they have access to, since they lack expectation of future benefit from their employer and their colleagues. If they are leaving to join a competitor, they may even have incentives for violations, like stealing sensitive intellectual property information to provide their new employer with competitive advantage. This is why many organisations today have "exit protocols" aiming to eliminate this risk, making sure that people who are leaving the organisation cannot exploit trust that was extended to them as employees.
- *Institutional embeddedness*: The presence of legislation or institutions with power to sanction untrustworthy behaviour (e.g. ethics committees of professional bodies) acts as a deterrent for an

employee considering a trust violation. The emerging level of deterrence, and thus the effect of institutional embeddedness on behaviours, usually depends on the type, strictness and severity of punishment (e.g. the threat of being excluded from a professional group).

6.3.4.2 Trust and security violations

Fléchais et al. also discuss how, in addition to incentivising secure behaviour, the presence of trust-warranting properties in an organisation can also lead to policy violations. The presence of intrinsic properties (benevolence and social norms) and contextual properties (social acceptability, expectation of future relationships) can lead to security violations that aim to preserve trust developed between employees. For example, an employee's willingness to help a colleague locked out of a system by sharing their password may be stronger than their motivation to adhere to the security policy, also further incentivised by contextual pressure (be part of the group, potential of needing a colleague to do the same for them in the future). After a number of successful trust violations to help their colleagues, a non-compliant security culture amongst employees can emerge over time, increasing the organisation's risk exposure. Social engineering attackers for example, can exploit this by pretending to be a colleague that needs help when attempting to get hold of sensitive organisational information (e.g. asking their colleagues to provide them with information while being "snowed in" – section 2.4).

6.3.4.3 Improving security

Based on their aforementioned analysis, Fléchais et al. presented a number of potential trust-aware courses of action organisational security management can take to improve security:

1. *Simplify security*: When a degree of flexibility is required, rigid policies cannot work because they are too complex, constraining or expensive, eventually exhausting employees' security compliance budget. In such cases, the only effective approach is to encourage and trust employees to behave in a secure manner, complementing this with effective monitoring to detect whether employees are actually complying with the policy.
2. *Improve education*: Security awareness and training should be given continuously to all employees, as opposed to just giving it to newcomers, in order to improve motivation and ability for secure behaviour.
3. *Promote security culture*: Ensure the security policy is neither excessive nor unfair, so that minimal circumventions are required.
4. *Adopt participative security*: Involve various stakeholders in security design to increase perceived responsibility.
5. *Foster group cohesion*: Group people into security groups, to improve their perceived social responsibility to collectively contribute to security.

6.3.5 The need for further trust-driven security research

Despite their potential usefulness (and consistency with the problems that lead to shadow security evolution presented in chapter 5), the above suggestions are only based on the findings of past security research, discussed in the context of Riegelsberger et al.'s framework. The suggested effects of contextual and intrinsic properties on employee security behaviours, together with the proposed improvements emerging from those, were not grounded to any empirical data collection and analysis.

Combined with the suggestions that trust affects employee security behaviours, presented in chapters 4 and 5, the need for further research to investigate the effects of trust in security implementations was identified. This was required both to verify the suggestions made by Fléchais et al., but also to further examine the existence of security-related trust relationships in organisations, their effect on employee behaviours, and potential lessons for security management. In an attempt to do so, the remainder of this chapter presents the analysis of the complete available dataset of 200 interviews from both Company A and B, and discusses the importance of the findings for security management.

6.4 Interview analysis

The secondary analysis on the available interview sets presented in this chapter aimed to answer the final research question that emerged in section 4.7.2, which could not be answered by the findings presented in chapter 5: "*What trust relationships develop in an organisation and how do they influence security behaviours?*" The analysis presented in this section followed a grounded theory process, in a similar way as in chapter 5, as presented in section 3.5.2 of the methodology chapter, adapted to reflect the research question examined. The process was done concurrently on both Company A and B interview sets. Coding was done using the software tool atlas.ti and the full list of the grounded theories categories that emerged from the analysis can be found in Appendix G.

6.5 Understanding organisational trust relationships

Two main paradigms emerged from the trust-focused grounded theory analysis: (1) employee understanding and acceptance of the need for some assurance in order to deliver security, and (2) the presence of two different security-related trust relationships that influence the design, implementation and evolution of security behaviours in an organisation: *organisation-employee trust* (willingness of the organisation to remain exposed to the actions of its employees, expecting them to behave securely) and *inter-employee trust* (willingness of employees to act in a way that renders themselves or the organisation vulnerable to the actions of another member of the organisation). This section discusses both the above paradigms, based on narratives identified in the analysis, presents the effect of those on employee security behaviour, explains the long term implications for organisational security, and also discusses how the findings contribute to the development of shadow security in the organisation.

6.5.1 Understanding the need for assurance

The first main narrative emerging from the analysis was the identification of employee understanding of the need for security. The majority (92%) of employees in both companies discussed potential consequences of a security breach for the organisation and recognised the need to implement security mechanisms in order to limit those. A significant proportion (88%) also showed understanding of their own contribution and responsibilities to deliver that protection:

PA60: "*Certainly from financial information we have a lot of knowledge and information that could affect stock market value of the company. You know we hear about recent things that maybe in advance to the public.*"

Employees also reported that the actions they need to take to deliver that protection are outlined in the organisation's security policy (48%):

PB11: "*There's also pages on the intranet so the security team have their own section on the intranet where you can go and look for specific information if you're unsure of what the policy might be around a particular type of access.*"

18% also mentioned that sanctions were in place for those caught bypassing security:

PB14: "*It could be dismissal and potential prosecution I would imagine, dependant on the sensitivity of the data, I mean we're not allowed to talk about products to other peers in other companies, so we wouldn't do that. Obviously that's breaching data protection Act, it's breaching copyright, it can be breaching all sorts of security risks. So it's certainly not something I'd do.*"

6.5.2 Organisation-employee trust

Despite the presence of some assurance to limit potentially harmful employee actions (e.g. website blocking mechanisms, access control for information-handling systems), in many cases employees reported that the organisational security implementation was based on a security policy that defined desired behaviours, with no assurance mechanisms in place to enforce those (e.g. don't share passwords, use encrypted USB drives etc., 37%):

PB56: "*I think it's encouraged, whenever you talk to the right people it's encouraged, but it's not enforced…So there was a notice came round driven by security, saying these things were available, so if you must use sticks, we recommend you use these one. So that was kind of the information and I actually proactively went and ordered it. It was up to the individual to take action.*"

The access control procedures in both organisations highlighted this lack of control over employee actions. In many cases the organisation appeared to be reliant on employees to manage access control: Employees reported minimal central coordination of access granting procedures, shared information as they saw fit for business cases, and managers authorised access to information and systems for their team members. They also reported a lack of oversight after they were granted access to a repository, set of documents, or physical location:

PA57: "*somebody said "Oh, I'll set you up on this, I'll set you up on this" […] that's just because they were sitting next to me, that wasn't just their job, or anything, it's no one's particular job to set people up on different systems.*"

PB67: "*I guess it's judgement and what you're working on and whether the data is sensitive (inaudible) so head count, people's name and grades and stuff are obviously sensitive so I would put a password protection on that. But if it's just an overall (inaudible) that everybody can see then probably not. If it's budgets that need to be seen by everybody then probably not.*"

In general, both organisations appeared to accept some exposure of their systems and information to employee misbehaviours by trusting them to behave in a secure way. This lack of strict assurance and

trust towards employees to behave securely, is defined as *organisation-employee trust*: "*the willingness of the organisation to remain exposed to the actions of its employees, expecting them to behave securely".* In many cases, employees reported they understand the existence of organisational trust towards their behaviours (72%), and the potential for their behaviours to increase organisational risk exposure:

PB23: "*We tend culturally to be allowed more freedom and responsibility than some people might do…It's almost impossible in security terms to stop a human actually attaching a document when they shouldn't it's very difficult to get round that.*"

PA99: "*…I think there's a balance to be struck between giving people trust and appreciating their common sense and their intelligence and also protecting one's system from the occasional stranger who walks through the area.*"

Examining employee behaviours, both intrinsic and contextual motives encouraging employees to behave securely were identified (Figure 12):

1. *Intrinsic*: Employees exhibited both knowledge and risk awareness (*ability*) to protect the organisation (88%):
   PB69: (talking about USB drives) "*No, they're more trouble than they're worth because you could potentially get into trouble with those things, leaving stuff on them that you shouldn't do, and leaving them lying around, they're just too easy to lose, so I don't use them."*
   They also demonstrated propensity to do good and contribute to organisational protection (*motivation*) (41%):
   PA83: "*I think all the data I work with is very sensitive. And, from what I've seen, you know, the company is quite serious about securing its financial information and all the applications I deal with are password-protected*"
   PB58: "*So maybe I'm not the right person to take those risks and make those choices, but I think we all have to share that that's part of the ethos of the company.*"
2. *Contextual compliance*: In other cases, employees reported a need to comply with organisational policies to avoid potential sanctions (*temporal incentives*); 32% reported to understand the consequences of breaking security rules and that sanction avoidance acted as a secure behaviour driver:
   PA4: "*…They do it only because "Oh, I might get into trouble if I don't do it"*.
   PB71: "*The trust has always been there, but the consequences are also there if it's broken.*"

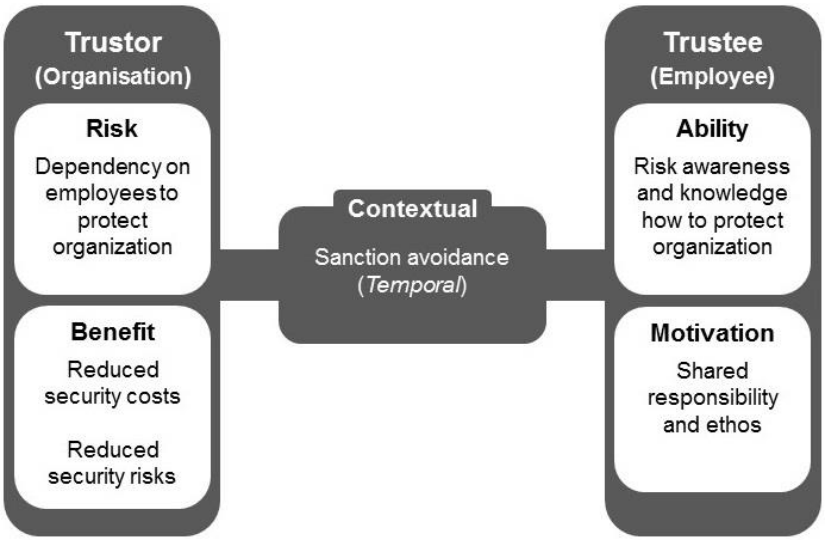

Figure 12: Organisation – employee trust development incentives

Despite the existence of both intrinsic (*ability, motivation*) and contextual (*temporal*) incentives to comply with security, 90% of interviewed employees reported they occasionally deviate from policy-prescribed behaviours due to friction-inducing security mechanisms, with 66% explicitly acknowledging this was a violation of the trust shown to them by the organisation:

PA53: "*the reason I diverted away from policy has been driven by a business requirement. And it's, it's one of those things that's always been discussed with seniors and it's been seen as a work around because the policy doesn't fit the business requirement.*"

The range of employee insecure behaviours identified, was grouped in three categories, based on the drivers behind identified behaviours: (1) friction-inducing security mechanisms and processes creating high primary task overheads, (2) inaccurate user risk perception and awareness, and (3) the need to develop or preserve existing inter-employee trust relationships prevailing over the need to preserve organisation-employee trust. As (1) and (2) were extensively discussed in chapters 4 and 5, the next section focuses on the third driver of insecure employee behaviour: attempting to preserve inter-employee trust, when the actions required to preserve organisation-employee could end up damaging it.

6.5.3 Inter-employee trust

40% of the interviewed employees reported they have close relationships with their colleagues, also explaining how those relationships act as enablers to productivity:

PB2: "*You work with them so much. God, the engineers that I work with for our company I spent hours with them on a daily basis, so you do get to know them very well.*"

Despite that, 94% of the interviewed employees reported instances where organisational security requirements demanded not showing inter-employee trust (e.g. no password sharing, no information sharing, challenge your colleagues). In the majority of those cases (85%), employees reported that inter-employee trust relationships prevail over policy clauses, either explicitly reporting trust presence as a

driver for non-compliance, or discussing how the close relationship they have with their colleagues lead to them not following the prescribed security practices:

PA12: "*…as far as "Oh, this contractor wants to get something done quick, here use my ID for doing that. You know, and then I'll switch the password after. Okay, he's sort of protected it, but really is, you've just shared your ID, you just shared a password, and with a non-company person, you know, violation, but you need to get your work done.*"

Employees also reported that trust acts as an enabler to productivity when security creates friction (30%):

I: "*So if someone asked you to share your password with them, you'd have no problem with that?*" PB5: "*No, as long as it's a trusted colleague.*"

Based on the above behaviours, *inter-employee trust* is defined as: "*The willingness of employees to act in a way that renders themselves or the organisation vulnerable to the actions of another member of the organisation".* It can be developed both inside and outside the security domain, and leads to behaviours that diverge from the security policy. A few examples:

PB18 (on sharing documents through non-official communication channels): "W*ell if someone's into the company and they need a certain document they know where to find it then pass it on.*"

PA116 (on not locking their screens): "*…because when you comment on it and say "Well you should actually be locking your screen when you walk away", the comment you get back is the fact that "Well you know we should be able to trust people around.*"

Similarly to the drivers of employee secure behaviours, the development of inter-employee trust is also based on both intrinsic and contextual properties (Figure 13):

1. *Contextual*: Successful employee collaboration leads to social capital development (7%), based on both social embeddedness (increased feeling that collaborators are members of the same social group I: "*So if someone asked you to share your password with them, you'd have no problem with that?*" PB6: "*No, as long as it's a trusted colleague*") and temporal embeddedness (increased willingness to collaborate in the future PB3: "*I spent hours with them on a daily basis, so you do get to know them very well*."). Temporal incentives also lead to inter-employee trust turning to reliance over time, with employee work processes ending up relying on collective trust violations (e.g. PA2"*…a lot of times the field guys, they won't tend to trust you initially you've got to be there for a while. Like now that I've been here three years, "Oh, I've worked with him a lot. Not a problem, I like working with him*."")
2. *Intrinsic*: Employees feel the need to be helpful to someone within their social environment (7%) (PA31: "*…there's a policy that, shortly after we moved to this building they made a big deal out of "Don't allow following access through doorways." […] it seems kind of impolite to say, Sorry, I can't let you through, I'm going to have to slam the door in your face. Human nature tends to be I'll hold the door for you"* (*motivation*). In addition, employees assumed their colleagues are as motivated as themselves to protect the organisation, and that they are also familiar with the security policy, so the risks from policy deviations to help a colleague were

minimal (PA78: "*So when you're an employee and I speak to another employee, it's not a problem, because everybody knows what the security policies are with the company*"). They also appeared to assess their colleagues' *ability* to protect the organisation before resorting to trust-driven violations: PA30: "*…But it was quicker sometimes to just throw it on a flash drive and chuck it over the cube wall. We just didn't really see the point in needing to buy an $80 flash drive to do that. The people that I work with, I'm speaking from my experience, they're all a lot smarter than me. They all have grad degrees and PHDs and stuff, and they write really good programmes, I would trust them to take some information off their computers.*")

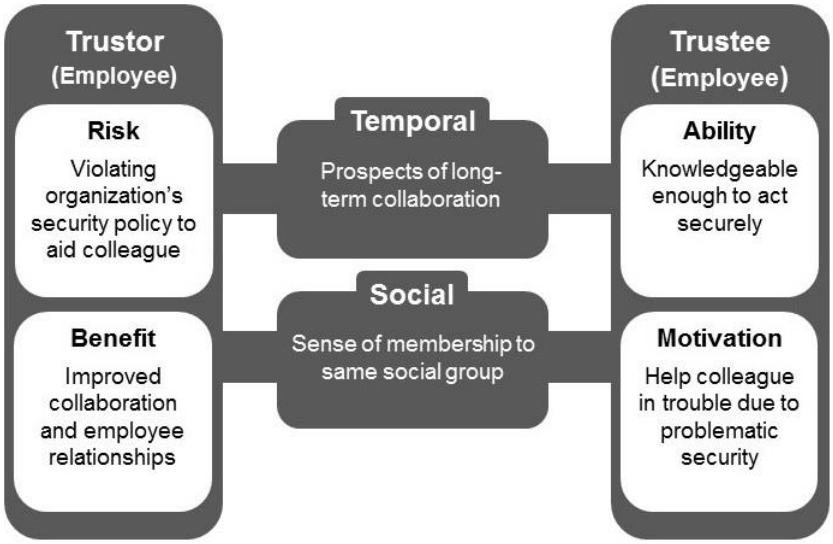

Figure 13: Inter–employee trust development incentives

6.5.4 Trust leading to shadow security development

As discussed in chapter 5, when employees need to bypass or modify a friction-inducing security process or mechanism (thus breaking organisation-employee trust), shadow security emerges. For example, the following self-devised security mechanism of an employee when working with contractors that needed wider access than what their permissions allowed:

PA12: "*…as far as "Oh, this contractor wants to get something done quick, here use my ID for doing that. You know, and then I'll switch the password after. Okay, he's sort of protected it, but really is, you've just shared your ID, you just shared a password, and with a non-company person, you know, violation, but you need to get your work done.*"

In such security-productivity friction situations, employees use their own understanding and available resources to deploy self, or team-devised solutions. The presence of inter-employee trust then acts as a readily-available resource, encouraging shadow security development; employees use inter-employee trust to deploy their own workable security solutions, addressing policy gaps or excessive burden from friction-inducing organisational security mechanisms:

PB3: *"… if we've had to give temporary passwords to an engineer, or someone like that, we will change the password, give them their own password, and once they're done we will change them back, so nobody ever actually has the official passwords except the engineers themselves."*

6.6 The impact of trust on organisational security behaviours

The findings of this chapter lead to the emergence of two trust-related paradigms in security management: (1) organisations place a significant level of trust towards their employees, even if they do not explicitly acknowledge it in their security strategy or policy; employees also understand this, together with the increased organisational exposure to their behaviour, and attempt to honour the trust shown towards them, (2) inter-employee trust acts as a readily available resource when security creates friction with primary tasks: in some cases employees need to break organisation-employee trust to avoid emerging overheads on primary task completion, and resort to trust they have developed amongst them to do so. This section discusses both paradigms, together with their impact on shadow security development, the risks that emerge and the challenges they create for information security management.

6.6.1 Employees understand and want to honour organisation-employee trust

Many elements of the security implementation in both organisations suggested the presence of organisational trust towards employees through the identification of organisation-employee trust. Employees recognise that in many cases no assurance exists to ensure they behave securely, thus the organisation remains exposed to security risks if they do not act as required. An example comes from organisational access control policies: employees are allowed to share information and grant access to their colleagues, with minimal organisation oversight of their decisions. Despite this lack of control, the presence of *contextual* (temporal) and *intrinsic* incentives (motivation and ability), motivates employees to behave in a secure way, confirming the suggestions by Fléchais et al. that the presence of trust-warranting properties in the organisational environment can incentivise secure behaviour. This understanding of the need for security, also leads to employee acceptance of some productivity overheads, in order to protect the organisation. They essentially appear willing to tolerate some friction caused by security, if they see a clear need for the mechanisms that caused it. Employees also understand and accept the need for reprimands for people who violate organisation-employee trust.

6.6.2 Inter-employee trust prevails over security

When employees encounter friction-inducing security, inter-employee trust prevails over organisation-employee trust, acting as a coping mechanism to minimise the emerging primary task overhead. As the analysis findings demonstrated, employees knowingly diverge from recommended practices, disclosing information or performing actions for which they could be held accountable, either because they want to help a colleague in need (e.g. share a password or information), or because they trust people around them (e.g. leaving their laptops unlocked or letting them tailgate). The identified drivers behind these trust violations are:

1. *Preservation of good relationship with colleagues*: Employees are willing to break the *organisation-employee* trust relationship to help develop, improve or maintain *inter-employee trust* that appears to be important and widely prevalent amongst them. Many of the non-compliance scenarios identified were related to security policies essentially asking employees to distrust their colleagues (e.g. no password sharing, lock screen, no tailgating). But relationships between employees develop both inside and outside the security domain, as they collaborate on a day-to-day basis for effective and efficient primary task completion. As a result, the *social* and

temporal elements of inter-employee trust, combined with intrinsic employee *motivation* to help their colleagues, lead to insecure behaviours. Preserving or improving their existing relationship with their colleagues, eventually prevails over the need for security.

2. *Minimise overhead of friction-inducing security on primary* tasks: As discussed in chapter 5, the presence of friction-inducing mechanisms and processes in organisational implementations leaves employees having to resort to other, less taxing actions for efficient primary task completion. In those cases, they turn to their trusted colleagues for support. They use a resource readily available (inter-employee trust) to cope with over-restrictive mechanisms that hinder their ability to do their job, while also improving their ability to collaborate with their colleagues. For example, an employee who was locked out of a system by entering their infrequently used password incorrectly, and who cannot get it reset by the helpdesk immediately, can easily borrow a trusted colleague's password to fetch some urgently required information. Willingness to help a colleague (*motivation*), recognition that they may end up in the same situation in the future (*temporal*), and the overall desire to be part of the overall organisational environment (*social*) provide enough incentives for their colleagues to help them, even if that means breaking the security policy, thus failing to honour organisation-employee trust.

In general, when security and productivity came to conflict, employees often chose to break organisation-employee trust, in order to proceed with their productive activities and preserve inter-employee trust.

6.6.3 Risks from security-related trust conflicts

Collaborative violations of organisation-employee trust, combined with shadow security development presented in chapter 5, lead to the emergence of two different types of organisational security: one defined in the policy, and one devised by employees on an ad-hoc basis, while they attempt to balance their own perception of how security should look like, their primary task focus and the need to be helpful to their colleagues. The emergent security environment inevitably spins out of organisational control, leaving the organisation vulnerable to behaviours out of sight of security managers. The risks emerging from this are: (1) development of an organisational security culture where breaking security is justified, (2) long-term reliance on trust violations, and (3) draining of existing employee capacity to behave securely.

6.6.3.1 Culture where breaking security is justified

The long-term development of employee belief that policy violations are necessary, can lead to the emergence of a corporate security culture reliant on security violations. The benefits of breaking security (preserve colleague relationships, efficient primary task completion), combined with the reported lack of consequences and manager approval of violations (e.g. 6.5.2, PA53), lead to the development of a security culture where breaking organisation-employee trust for the benefit of inter-employee trust and productivity is considered acceptable. The reported lack of follow-up enforcement accentuates this, as it reduces the impact of contextual incentives to preserve organisation-employee trust. The emerging security behaviours, may not manage risks effectively, due to inaccurate employee understanding of security risks and countermeasures, but are the best available actions for employees to proceed with their primary tasks. Collaborative non-compliance also encourages disregard for security in general, with non-compliance eventually becoming the habitual behaviour amongst employees. Once a security culture is

developed based on collaborative security violations, new employees that try to "fit in" and participate in inter-employee trust development are more likely to follow suit to their colleagues' non-compliance.

6.6.3.2 Long-term reliance on collective trust violations

An insecure culture also develops from long term collaborative security violations. Regular reliance on violations leads to the development of insecure behavioural norms that can then evolve to long-term information security culture (Da Veiga and Eloff, 2010). It also leads to the development of social capital (Schneier, 2012) amongst employees, grounded on collective security violations, and also increases organisational exposure to social engineering: employees willing to violate security to help their colleagues can be more vulnerable to attacks by impostors that rely on their willingness to share information through informal channels.

6.6.3.3 Drains employee capacity to behave securely

Employees appear sufficiently aware of the need for security, related risks and potential actions required to mitigate those risks, also possessing both *ability* and *motivation* to behave securely. Friction-inducing security mechanisms fail to take advantage of this, damaging employee ability and motivation to comply with security: any attempts to enforce security end up alienating employees from security management, draining existing employee capacity to behave securely, thus decreasing their motivation in conditions where the organisation relies on their actions to address security risks. The emerging low appreciation for security can accentuate the development of a non-compliant security culture, discussed in section 5.3.3 (Pfleeger et al., 2014). It also encourages further shadow security development, leading to the organisation losing track of employee actions, thus increasing the security risks it is exposed to.

When the organisation demands security behaviours that employees consider unrealistic, employees may perceive this as lack of organisation-employee trust. This creates resentment amongst them, increasing incentives for trust-driven collaborative non-compliance. In addition, long-term resentment can have dangerous effects, as it damages psychological contracts between employees and the organisation (Morrison and Robinson, 1997). This increases the risk for insider attacks and loss of valuable human capital, with disgruntled employees ending up leaving the organisation.

6.6.4 Trust and shadow security development

Employee decision to prioritise inter-employee trust over security adds an additional element to the complexity of modern information security management. Past user-centred security research extensively discussed the *usability-security* trade-off, often suggesting that effective security management can achieve both (sections 2.5, 2.6 and 2.7). The findings of this chapter demonstrate that the presence of trust in organisational environments also affects employee security behaviours: they break organisation-employee trust to both strengthen and preserve their relationships with their colleagues, but also to minimise the impact of friction-inducing security mechanisms and processes on their primary tasks. In both the above scenarios, trust acts as an additional driver for the development of shadow security, increasing organisational exposure to the risks presented in section 5.3.3 (security development outside organisational control, reduction of employee resources available for security, and alienation from central security). To reduce this exposure, security management needs to understand the impact of inter-employee trust on employee security behaviours, and take that into account in future attempts to design

security processes and mechanisms (in-depth analysis of how trust can be leveraged to improve security protection is presented in chapter 7).

6.7 Revisiting research questions

The main aim of this chapter was to investigate and answer research question number 6: *What trust relationships develop in an organisation and how do they influence security behaviours?* The findings also improved the ability to answer question 1 as well: *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?*

1. *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?* Employees understand both the need for security and organisational reliance on them to participate in security risk mitigation. They also understand the need for assurance mechanisms required to protect the organisation, but they also believe that they cannot be implemented to exhaustively cover all security risks an organisation faces. As a result, a large proportion of security management relies on trusting employees to exhibit behaviours that protect the organisation, despite this not being formalised in organisational security strategies.
6. *What trust relationships develop in an organisation and how do they influence security behaviours?* Employee trust relationships with their colleagues and managers develop though interactions both inside and outside the security domain. Inter-employee trust then acts as a readily available resource to deal with friction-inducing security. It also prevails over organisation-employee trust, when security policies demand from employees not to trust their colleagues. This leads to non-compliance with official security and shadow security development.

The findings of this chapter suggest that both organisational productivity and security can benefit from a shift in security management: rather than restricting and controlling employee actions, security should aim to understand organisational trust relationships and incentivise trustworthy behaviour. It also needs to accommodate for the fact that, for their employees, security is of lower priority to both productivity (primary task completion) and the need to develop and preserve a collaborative social environment (inter-employee trust). Further analysis and discussion of how the to combine the improved understanding emerging from this chapter with the shadow security findings of chapter 5 to deliver effective security protection is presented in the next chapter (chapter 7).

Chapter 7: Using shadow security to improve security management

The findings of the analyses presented in chapters 4, 5 and 6 identified three previously unknown employee behavioural phenomena, together with their impact on organisational security management:

1. *Employee propensity to behave securely*. Employees understand the value of security to the organisation, which motivates them to participate in organisational efforts to deliver it. But, despite this understanding and motivation, three categories of behaviours that increase organisational risk exposure were identified: (1) when organisational security communication is inconsistent with employee priorities, they fail to recognise some risks, and behave insecurely. (2) When friction-inducing security creates overheads for their primary tasks, employees passively bypass those, ignore policies and avoid organisational security mechanisms. They then (3) use other resources available to them, actively taking initiative to protect the organisation, by adapting existing mechanisms and policies, or by devising their own "secure practices".
2. *The shadow security*. When the organisation's existing security implementation creates friction between security and productive activities, employee productivity focus and their awareness about the need for security leads to them adapting official security or procuring self-devised security practices, both at an individual and a collective level. The emerging practices reduce security-productivity friction to acceptable levels for employees, while also serving their understanding of the need for security and contribution in organisational protection. But shadow security also leads to security management losing control of security culture and habits development, exposing the organisation to risks employees cannot understand or mitigate. This eventually leads to security practices around the organisation being widely varying and out of security management control.
3. *Trust relationships and their impact on security*. Two security-related trust relationships develop in the organisational environment, influencing security management decisions and employee behaviours: (1) *organisation-employee trust*, allowing for flexibility in security implementation and reduced control over employee actions, with its visible presence also acting as a motivator for secure behaviour for employees, and (2) *inter-employee trust*, developed through activities both inside and outside security, acting as a readily available resource for employees to cope with friction-inducing security, also serving their need to preserve or improve their relationships with their colleagues.

In-depth examination of the above phenomena led to the identification and characterisation of a number of different employee behaviour narratives, providing valuable insights to organisational information security management:

1. Employees understand and accept the need for security, together with their responsibility and contribution in achieving it. They also understand organisational reliance on their behaviour and the trust shown towards them by security management, realised through reduced controls

(*organisation-employee trust*). They are also willing to invest some of their time and effort to keep the organisation secure.

2. Friction-inducing elements of the security implementation cause disgruntlement: employees refuse to accept the resulting primary task overheads, which can often cripple their productive capabilities. Subsequent security management attempts to enforce desired behaviours isolate employees from security managers, creating disgruntlement and a negative attitude towards security in general (perceived to be badly designed, implemented and managed, also creating overheads in their productive activities)
3. Rather than remaining passive, either ignoring official security or working their way around it to avoid related overheads, employees, peer groups, and managers who have their own understanding of security, individually or collectively adapt unsatisfactory security measures to what they consider manageable (in terms of the corresponding primary task overhead) or introduce their own novel solutions. These solutions are perceived by employees as serving the purpose of maintaining security, but at the same time reducing friction and corresponding primary task overheads to levels acceptable to them.
4. The emerging employee-devised shadow security practices often do not manage the organisation's risks adequately: isolated from security management and without guidance on the actual organisational security risks, the alternative solutions are deployed based on employees' own risk perceptions and understanding of what the security experience should be like.
5. The existence of trust amongst employees (*inter-employee trust*) also affects their security behaviours: the need to preserve or improve their relationships with their colleagues, together with their belief in the ability and motivation of those to behave securely, leads to the perception that trust-driven security policy violations are a low risk option to reduce security overheads and proceed with primary task related activities. As a result, inter-employee trust prevails over policy-prescribed behaviours when the two come into conflict: it becomes a readily available resource to cope with the overheads of friction-inducing security, further encouraging security violations and contributing to shadow security development.
6. The development of shadow security, together with organisational inability (or perceived inability) to enforce policy-prescribed behaviours (or identify employee deviations from prescribed practices), leads to security behaviours and culture evolution spinning out of central security management control: employee-devised practices can often be inconsistent with organisational risk appetite, with trust-driven violations becoming the only way to preserve good relationships amongst colleagues. When shadow security practices become part of organisational security culture, or varying micro-cultures developed within organisational divisions and sub-divisions, security behaviours become invisible to official security management, failing to deliver the required protection for the organisation.

This chapter uses the lessons learned from chapters 4, 5 and 6 to provide guidelines that help organisations manage employee security behaviour, but also leverage it to align security management with organisational productivity targets. The suggestions for improvements presented in this chapter focus on five distinct, but also interdependent, areas: (1) The need for security management to move away from its current binary understanding of user behaviour (compliant vs non-compliant), also (2)

understanding that friction-inducing "unusable" elements of security implementations need to be removed before attempting to influence employee behaviours, (3) the need to leverage shadow security as a learning tool to engage employees and line managers in security management and design, also (4) building on the presence of trust in the organisation, using it as an additional defence layer, and (5) deploying measurements using readily available or easy to collect data to identify areas for improvement, and use those to deploy improvements and assess their effectiveness and overall impact on employee behaviours. All the findings discussed and suggestions made in this chapter are related closely to the experiences of individuals within both Companies A and B, focusing specifically on examples where friction-inducing security and the emerging primary task impact led to the development of shadow security activities or trust-driven security violations.

7.1 Using employee behaviour to drive security management

As discussed in section 2.8, there is a strong need for a process that will improve security management's ability to accurately identify current employee behaviours and use those to drive subsequent security management decisions. This section uses the paradigms that emerged from the research presented earlier in this thesis to: (1) revisit and enrich existing understanding of employee security behaviours, (2) use the improved understanding to update the security behaviour model of section 4.6.4 to reflect the presence of shadow security in the organisation, and (3) Explain how shadow security can be used to improve existing security management implementations.

7.1.1 Revisiting security behaviour drivers

Chapter 4 identified employee propensity for secure behaviour, but also conditions that lead to policy violations. Employees followed policy-prescribed behaviours when the impact on their primary task was minimal, but also bypassed security when it disrupted or slowed down their primary tasks, even when they were aware of the need to behave securely. Evidence of their awareness of the need for security was accentuated by chapter 5 findings: they even adapted friction-inducing policies and mechanisms to deliver some organisational protection. The findings from chapters 4 and 5 suggest that employee awareness does not always lead to compliance; it is only the first step towards achieving it. To improve on employee compliance, it needs to be encouraged by an organisation's security implementation. This can only happen if employee security behaviours are well understood and accommodated in information security management. As discussed in section 2.8.3 of the literature review, employees were up to now considered as either behaving securely or insecurely, with insecure practices also seen as opportunistic behaviour:

- Pallas (2009) claimed that employees will always go for low cost, opportunistic behaviour when no control is in place.
- Weirich (2005) stated that users structure discourse about password security issues in a manner that makes it possible to justify malpractice.
- Ashenden (2015) suggests that the presence of cognitive dissonance when employee behaviours were inconsistent with their attitudes, led to them changing attitudes to be consistent with their actions, thus rationalising their insecure behaviours.

Shadow security challenges the above suggestions. Even when employees have perfectly valid productivity reasons to bypass security mechanisms, they take additional care to mitigate potential risks emerging from their malpractice (e.g. encrypting personal drives on which corporate data is backed up due to lack of sufficient backed-up network storage in company B). The presence of shadow security suggests that policy-prescribed practices are not the only way to achieve security, especially if they give rise to significant security-productivity friction. Security managers need to understand the presence of *in-between* behaviours and leverage their presence to enhance both learning and better management.

The identification of shadow security suggests a need to revisit Alfawaz et al.'s (2010) model of security awareness and behaviour presented in section 2.7.3. In that model, non-compliance with policies is attributed to lack of awareness, with "doing" referring to acting in accordance to the policy. But, given the development of shadow security, and insecure behaviours being used as a coping mechanisms for high-friction security, the "knowing" stages of the model need to be modified in order to: (1) distinguish between malicious acts and employees choosing to do something else due to friction-inducing security in the "knowing-not doing" condition, and (2) distinguish between compliance with well-designed security and compliance with high-friction security that is unsustainable in the long-run (due to productivity overheads) for "knowing-doing". Using the shadow security findings to modify the Alfawaz model, led to the identification of six security behaviour levels (Table 8).

Alfawaz state	**Revised security behaviour**	**Description**	**Related Findings**
Not knowing – not doing	Unaware of security	Lack of awareness from ineffective communication and training	None of the employees was in this state
Not knowing – doing	Awareness from other sources (both personal, organisation, colleagues)	Employee understanding is a combination of their own risk awareness and responsibility towards the organisation	Lack of policy awareness, but secure behaviour die to peer-pressure
Knowing – not doing	Malicious, careless non-compliance	Maliciously choosing to ignore/no interest in protection	Sanctions exist to deter this, but currently impossible to enforce
	Productivity-driven non-compliance	High friction security – employees choosing to do something else	Trust – shadow security evolution, majority of examples discussed in chapters 5 and 6
Knowing – doing	Compliant but expensive	Employees "do" because they have to	Both due to enforcement and lack of alternative perceived as secure
	Well-designed security	Policy compliance	E.g. clear desk compliance when secure on-site lockers exist – employees only need to invest minimal effort

Table 8: Security behaviour levels

The above classification comes can be challenging for security managers attempting to rank these steps on an "insecure to secure" scale. From a security point of view the security level would be 1 to 6 (from insecure to secure). If productivity impact was calculated as part of a holistic risk management approach, 4 and 5 may need to be swapped: shadow security behaviours may offer adequate cost-effective risk mitigation compared to expending employee resources to comply with friction-inducing mechanisms. In addition, potential unsustainable long term compliance with resource-demanding mechanisms (level 5 in the above model) can easily exhaust employee's compliance budget, influencing their ability to behave securely when interacting with other policies or mechanisms.

7.1.2 Updated security behaviour model

The improved understanding of employee behaviours that emerged from shadow security identification and the factors that lead to its development, created the need to adapt the security behaviour model presented in section 4.6.4. The new model (

Figure 14) incorporates the enriched understanding of employee responses to friction-inducing security, together with the effect of long term employee reliance on shadow security behaviours on organisational security culture development. The emerging culture and habits cycle is where security management needs to act to (1) identify current shadow security behaviours and the specific elements of the security implementation that drive those, (2) disrupt the culture cycle by reducing the drivers of shadow security and communicate the changes to employees, in order to aid the development of new security behavioural norms and culture.

7.1.3 Incorporating shadow security in security management

Security managers need to consider the development of shadow security as an opportunity for improvements. It suggests the presence of a latent capacity for users to appreciate and play an active part in the provision of security, driven by their internalised understanding of the need for security and their focus on their primary task. Employees deploy their own security solutions when they believe a required "affordable" policy or infrastructure is missing, instead of doing nothing or passively relying on the organisation to remediate. They take self-devised actions, still aiming to preserve security, both at the individual and the collective (team) level, often managed locally by their line managers. In addition, the presence of inter-employee trust acts as an additional driver for shadow security development: it provides employees with a readily available resource to resolve the productivity impact of high-friction security. The perceived justification for security violations in order to preserve their relationships with their colleagues, leads to loss of control of security behaviours by security management, with employees essentially becoming "partners in crime". Attempting to reduce or eliminate the emerging shadow security practices through increased assurance, without attempting to reduce high-friction security in organisational production tasks, creates additional burden for employees: assurance mechanisms accentuate primary task impact, which leads to further non-compliance, shadow security emergence and insecure culture development. Shadow security should be used as a tool to intervene and improve existing security implementations, to inspire more workable security that aligns with organisational productivity objectives, provides effective protection, and minimises security overheads.

The development of shadow security suggests the need for security management to rethink organisational security practices, processes and mechanisms, and attempt to better align security with employee primary tasks. Without actively soliciting feedback from employees to identify security-productivity friction points and their subsequent responses, the security of the organisation becomes that which managers and employees, assumed non-experts in security, consider as best fitting their business processes. Despite potential risks, shadow security presents the only workable security for the organisation; its presence indicates that the organisation has an inconsistent security posture, which does not align with its productivity goals. In order to eliminate this problem, security managers should aim to learn from employees and line managers, take advantage of their capacity to consciously consider security in their activities and use the emerging shadow security practices as a driver for improvements. In order to

provide security managers with a research-inspired approach to identify shadow security and improve their security implementations, the remainder of this chapter discusses how shadow security and trust can be incorporated in attempts to holistically rethink organisational security management.

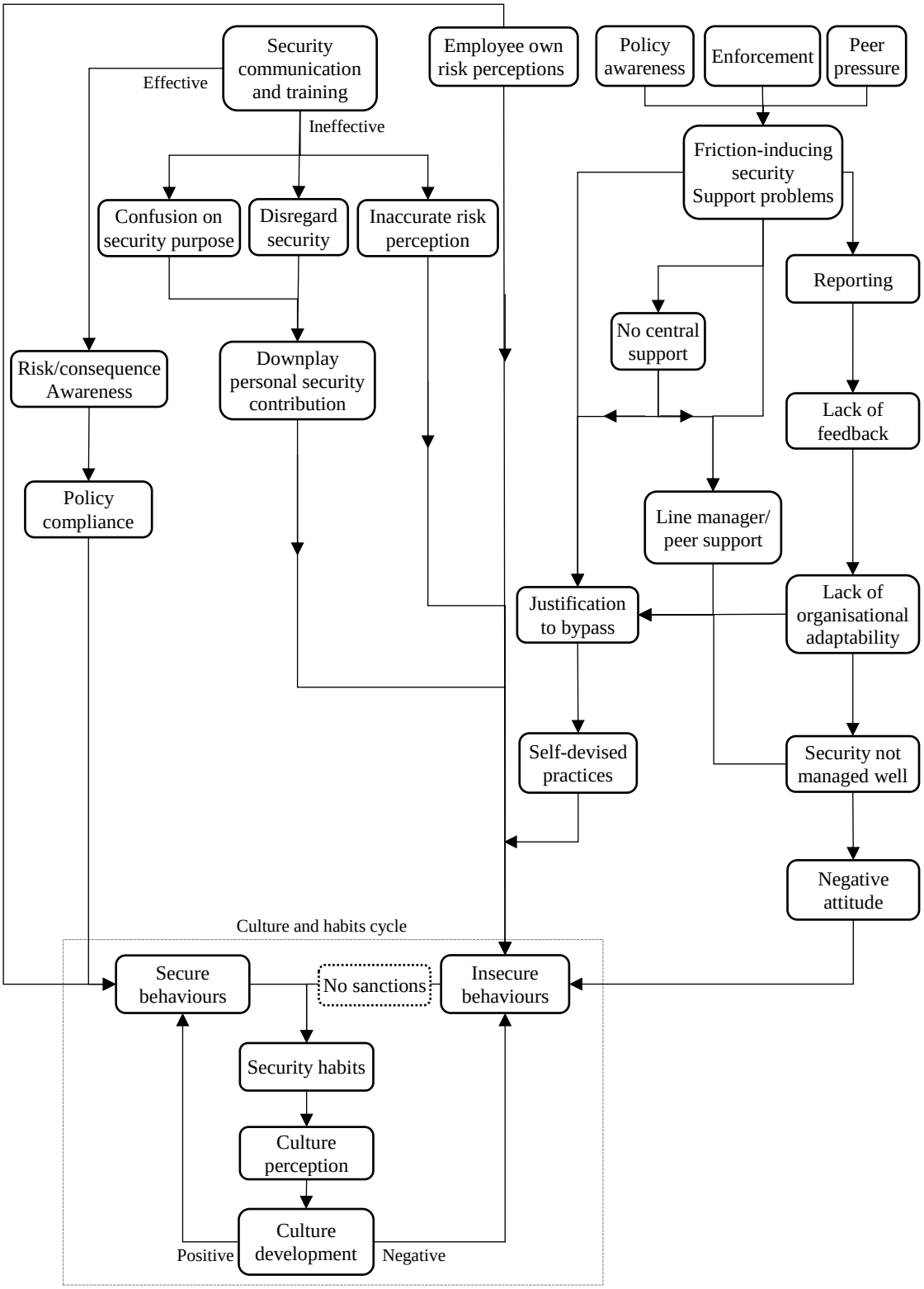

Figure 14: Secure behaviour model

7.2 Improving security-productivity alignment

The results presented in chapters 4, 5 and 6 show there has been little progress in identifying and removing ill-fitting security policies and mechanisms from organisational security implementations: organisations still do not track the effort that individuals have to expend on security and many elements of existing security implementations create significant friction between security and employee primary tasks. Consequently, there exists no evaluation of policies and mechanisms in terms of fitness-for-purpose in the real working environment. As section 7.1 discussed, burdensome or disruptive security implementations promote shadow security as the only workable security, even for risk-aware employees. Security experts need to acknowledge that effective security can only be achieved if it fits and supports productive activity. As a result, fitting security to the primary task should be in the centre of any security intervention, whether that aims to improve existing security elements or design new ones. This section discusses the need to better align security with organisational production tasks, focusing on (1) the importance of usability, (2) careful planning of interventions to ensure primary task compatibility, (3) the need for effective security communication and training, and (4) the need to align employee security efforts with organisational risk appetite.

7.2.1 The importance of security hygiene

Usability of security implementations is still a major hurdle to employees trying to behave securely: the findings presented in this thesis show that current security approaches do not manage to effectively reduce friction between security and productivity. Organisational security management appears to ignore user-centred security research findings that high friction security leads to errors and workarounds that create vulnerabilities (e.g. Sasse et al., 2001). Organisations still seek to mitigate information security risks by implementing policies and technical mechanisms that specify and restrict employee behaviour, often also threatening sanctions in case of non-compliance. This "comply-or-die" approach increases the cost for security mechanism operation, but also creates constraints for honest employees seeking to perform well in their primary tasks. Security mechanisms and processes not designed around employee needs and priorities slow them down, sometimes even completely preventing primary task completion. They also increase the cognitive load required for employees to participate in organisational protection, eventually causing frustration and disgruntlement. As a result, employees choose to ignore security that requires high effort for little benefit (Beautement et al., 2008), or use readily available resources (e.g. inter-employee trust or line manager support) to resolve the emerging conflict, which encourages the evolution of shadow security in the organisation. This leaves security managers unable to manage the emerging organisational security environment, reducing their ability to effectively manage organisational risks. The resulting high levels of security behaviours deviating from security policies, also increase the noise in organisational attempts to detect signs of malicious attacks (von Solms, 2006). All the above call for a significant rethink of the way information security is implemented and managed, demonstrating the need for information security management approaches that put employee understanding and priorities at the centre of their risk mitigation strategy and actions.

The first step for any user-centred security management approach is to realise that with high productivity impact security will never deliver effective protection. Many security experts still talk (and think) that usability and security create a trade-off: that usability is nice, but security is more important, so asking

users to make extra effort is acceptable. Usability is considered as an afterthought and a luxury security management can only afford to consider once security is assured. But the findings presented in this thesis demonstrated that usability problems can lead to security mechanisms being perceived as incompatible with employee primary tasks. Looking back at the definition of usability ("*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use*", ISO 9241), any mechanism not designed to fit employees' primary tasks will end up not being used, leading to further security violations and shadow security development.

Security design should treat usability as a *hygiene factor* for security (Kirlappos and Sasse, 2014): solutions that are not usable disrupt and divert effort from employee primary tasks, thus will inevitably be circumvented. Risk-aware employees, who understand their role in protecting the organisation will then resort to shadow security practices at best. At worst they will become disgruntled and see security as an obstacle that they need to get around, resorting to high-risk behaviours, increasing potential organisational risk exposure. The emerging employee disgruntlement can create serious risks for an organisation: it hinders the development of social capital and shared values (Moore et al., 2011), resulting in minimal incentive for secure behaviour, while increasing the probability of insider attacks (Vroom and von Solms, 2004). It also impacts the ability of an organisation to retain its valuable human capital; dissatisfaction can lead to employees eventually leaving the organisation (Fléchais et al., 2005). Consequently, delivering security hygiene should be a key requirement for any security management approach; security rules should not need to be broken to maintain productivity.

Security mechanisms need to be designed around employee primary tasks to reduce the need for productivity-driven trust violations, but also reflecting the trustworthiness an organisation should show towards its employees. To eliminate the need for password sharing for example, an organisation should create mechanisms that provide quick account creation for employees that need access to new systems (e.g. through easy to use one time tokens). This can be achieved by using human factors expertise and usability design methodologies in security system design process. The resulting user-centred security design will allow designers to move away from the current "deploy, if too much noise, remove" approach that makes security implementations expensive to implement, difficult to use, ineffective and unsustainable in the long term. Examples in the interviews have shown that parts of the security implementation can be integrated with productivity, essentially "piggybacking" security on other organisational needs (e.g. the use of personal network allocated storage for employees that provides automatic backups as well – see security hygiene example below).

Security hygiene example: Employees in Company B stored significant amounts of information locally on laptops due to problems in network storage capacity and connectivity issues. They also recognised the importance of that information and the need for backups. The lack of easy access to organisational drives (that are automatically backed up) led to employees having to devise own backup approaches: they used their own drives, either at team level or individually (both encrypted and unencrypted, with practices differing significantly across different groups).

Secure behaviour (storing data on automatically backed-up network drives) can only exist if:

a. Adequate network capacity is put in place
b. Communication of the benefits it provides, also emphasising its productivity benefit (backup)
c. Employees are provided with uninterrupted access to their personal network drives
d. Any reported connectivity problems are quickly addressed

Another important lesson for shadow security management emerging from the results in chapters 4, 5 and 6 is that improvements required to eliminate shadow security cannot be limited to security mechanisms. In a number of shadow security practices, security-productivity friction that created those did not emerge from problems in the security mechanisms, but to reliability issues of organisational IT provisions (e.g. lack of easy to use collaboration platforms within the organisation leading to use of third party ones). In order to eliminate such problems, security management needs to identify situations where functional requirements are missing and consider the impact of those non-security-related mechanisms on employee security behaviour. As the results have shown, effective security protection requires IT in its entirety to be free from problems; any element of the organisational environment that can affect security behaviours needs to be designed around employee priorities, also ensuring its proper function. Failure to achieve this can create a negative attitude towards organisational systems in their entirety, further encouraging trust-driven security violations and shadow security development.

7.2.2 Interventions need careful planning

Attempts to disrupt current employee practices require careful pre-deployment suitability assessments. Current security intervention attempts fail to assess the impact of attempted improvements on employees, with security management not tracking the effort that they have to expend in order to comply with existing or proposed security mechanisms and policies (Albrechtsen and Hovden, 2009). In addition, changes and attempted security implementation improvements are currently delivered reactively and impulsively. When a security mechanism is causing friction, with employees often voicing their concerns, it may be removed or disabled, but the risks it aimed to address can remain unmitigated until another solution is found. The new solutions are also deployed without proper design, testing and deployment, essentially only managing to modify the type of security-productivity friction employees have to incur (section 5.4.3.2). As discussed in section 7.1, shadow security indicates an employee-devised *balance point* to manage this friction. Any attempts to alter that balance need to be well planned, otherwise they risk draining employee capacity for secure behaviour. Effective protection can only be achieved with user-centred policy and mechanism design, taking into account the subsequent impact on an organisation's existing production tasks. To achieve this, security management needs to move towards

a participative security design approach that works with users to understand where and how security can align with the productive activity to protect valuable organisation assets.

An example of the need for pre-deployment assessment of security improvements was identified in organisational attempts to provide password management solutions to employees. The large number of systems to which employees had to authenticate themselves in both the organisations studied, led to writing down their account passwords being the only way to guarantee uninterrupted access to password-protected systems. This managed to reduce the increased cognitive load problem created by multiple password management. Company B's security management attempts to address this by providing employees with password managers failed when those tools were incompatible with some of the systems/websites employees had to authenticate to. Employees were left with a security mechanism not working as intended, turning the cognitive load problem to a disruption one, with the burden of resolving the conflict between security and productivity being once again cast on themselves. Employees then resorted to shadow security behaviours to solve the "too many passwords" problem (section 5.4.2). As the above example suggests, if attempted security improvements are not well-designed to eliminate usability problems, and no continuous evaluation of their effectiveness and "goodness-of-fit" with the primary task exists, they run the risk of just changing the nature of the security-productivity friction instead of removing it.

7.2.3 Importance of communication and training

The findings also call for a change in current security communication and training approaches. Lack of accurate knowledge on role-related risks, and lack of role-specific communication based on employee tasks, led to employees dismissing the usefulness of security communication and training. This acted as another driver for shadow security development, with security communication done through line managers and colleagues. To avoid this, formulation of communication content should aim to accurately represent everyday employee tasks. User-centred security approaches like requirements gathering and understanding should be used, to ensure the communicated information is fit for purpose and in-line with the challenges employees face, also formalising current line managers' role in delivering more context-specific communication. The emerging training and communication should be role-specific, with regular refreshing, ensuring employees understand role-related security risks, taking advantage of their identified propensity to behave securely.

7.2.4 Align security effort with risk appetite

Security management should also aim to align user resources required to bring security in line with organisational risk appetite; currently no formalisation exists on how much of employees' time and effort should be spent on security. Given that organisational risk management should be based on identification, assessment, and prioritisation of risks (ISO 31000 on risk management), the presence of shadow security suggests a potential mismatch between organisational risk appetite and current allocation of available employee resources towards delivering effective organisational protection. Current organisational attempts to exhaustively eliminate all potential risks, lead to the implementation of a significant number of risk-mitigating mechanisms or policies (often required to meet the demands of relevant regulation or international standards). But, when some of those lead to security-productivity

friction, security management adopts a post-deployment "ignorance is bliss" approach: they know some risks are left unmitigated, but are often left with inadequate resources to address those. Openly admitting to this approach is often impossible due to regulatory requirements or pressure by the organisation's top management to deliver the required protection without requesting additional resources, thus security management often chooses to ignore (and not report) the presence of some of the unmitigated risks. In addition, the mere presence of too many security mechanisms or policies, even well-designed, context-specific ones, can exhaust employee compliance budget, eventually leading to shadow security in the form of self-selection of mechanisms and policies to comply with. This leaves little or no resources to mitigate more severe organisational risks that employees may perceive as less important. It also prevents the organisation from accurately assessing the amount of employee resources currently invested towards implementing and sustaining the current security state: unless employee time and effort are invested in a centrally managed way, the organisation runs the risk of employee resources being allocated towards potentially insignificant security risks. It is also important to understand that in risk management it is acceptable to do nothing about some risks if available resources can deliver higher risk mitigation in other areas. In general, organisational security risk management needs to direct employee time and effort towards addressing most important risks first, minimising shadow-security-driven resource allocation by employees, thus ensuring available resources are invested towards maximal risk mitigation (a process of how to deploy a shadow security-driven risk management process is presented later in section 7.5).

7.3 Using shadow security as a learning and diagnostic tool

Understanding shadow security and its drivers can become a powerful tool for security management, providing a unique opportunity to deliver user-centred security improvements. Shadow security should be treated as a learning opportunity, as it can help the organisation identify where employees are putting to practice what the organisation should be doing but refusing. As Taleb (2010) notes, identification of problematic events within an environment can be used both to build robustness around negative ones and exploit positive ones. Shadow security provides such an opportunity: it allows for engagement with employees to increase their participation in attempts to deliver the security improvements presented in the previous section, and implement new or adapt existing security controls to better fit employee productivity tasks, while still delivering organisational security goals.

In order to take advantage of shadow security, security managers working within organisations need to understand the drivers behind its evolution and, as Schein (2010) puts it, aim to become *perpetual learners*. Modern corporate environments are fast-paced and unpredictable: the nature of organisational operations and technologies change constantly, together with security threats becoming more complex (e.g. effective security management of BYOD and home working were amongst the challenges Companies A and B had to deal with). Security managers can learn from shadow security in a number of ways: (1) engaging users to identify security problems and design appropriate solutions, (2) measuring the effectiveness of security mechanisms after deployment, and (3) leveraging the position of team managers as both a mediator for security and a conduit for feedback, as to the appropriateness of security solutions in supporting productive tasks. In order to effectively develop this learning process, security managers need to start by accepting that employee responses to friction-inducing security happen naturally. They are the first indicator of security solutions not serving the business, and security management must

engage with employees to identify security needs, perceived risks, impact of current implementation on their productivity, and the emerging shadow security behaviours. Essentially, as the remainder of this chapter explains, shadow security should be treated as a diagnostic tool and an opportunity to identify shortfalls in current security implementations, their impact on the organisational environment, and leverage those to provide more effective security solutions for organisations.

7.3.1 Involving employees in security management

The development of shadow security suggests that employees are motivated to help the organisation and willing to suggest potential ways to improve existing security practices. Their lack of accurate security risk awareness though, often leads to insecure behaviours. Security management can leverage this employee goodwill to participate in security, by engaging with them in the design and operation of security controls. Such an approach requires moving away from current solutions for mitigating security risks, towards a more participative approach that works with employees to understand where and how security can fit in the productive activities.

7.3.1.1 User engagement and participatory security management

The importance of involving users in systems design is well documented in approaches like Soft Systems Methodology (SSM - Checkland and Poulter, 2006), and the value of participatory and contextual design is widely accepted among developers. As Checkland and Poulter explain, a real-world system undergoing change to improve on a problematic situation needs to be understood in its entirety (or as much as possible) before attempting to deliver that change, but also during delivery as part of a continuous learning cycle (Figure 15). Otherwise, deployed changes will fail to capture the tasks and priorities of different stakeholders and the impact of attempted changes on those. Unfortunately, participatory approaches are currently not adopted by security design, with very limited research attempting to apply those in information security: Bartsch and Sasse (2013) used a participatory approach to provide guidance on improving the formulation of authorisation policies, while James (1996) demonstrated the potential of participatory design as a security management tool. Creating a continuous, participatory design-based security management process using the lessons learned from shadow security (together with the metrics presented later in this chapter), can allow building more accurate employee activity models, improving the effectiveness of proposed improvements and their alignment with organisational productivity priorities.

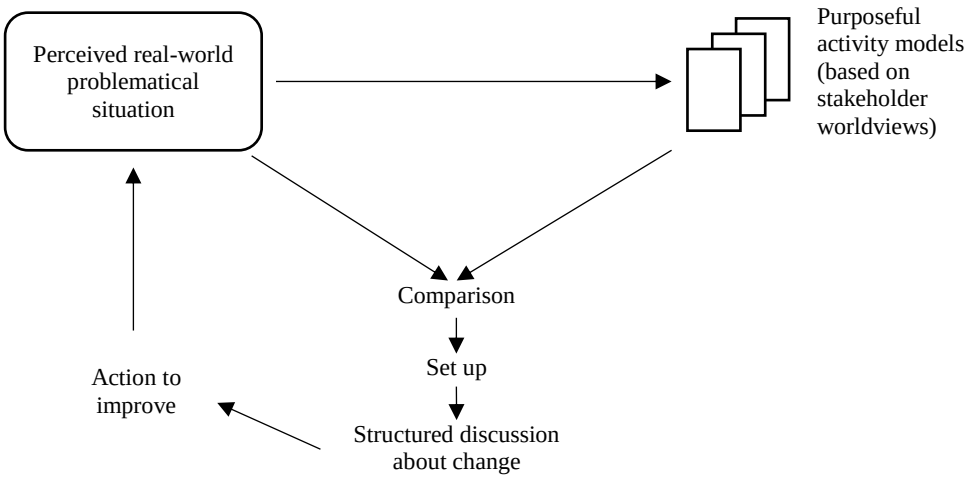

Figure 15: The SSM learning Cycle (Checkland and Poulter, 2006, p13)

7.3.1.2 Incorporating feedback-driven security design

Security management should aim to use employees as a resource for learning to identify specific points of friction and candidate improvements. As previously discussed, users do not dismiss security, but devise "more appropriate" shadow security solutions when they encounter unworkable security. The emerging practices may not necessarily be those that the security experts expect, but employee rationalisations dictate how they interact with security, and the value they see in compliance. This capacity of users to participate in security can provide leverage to create new, seamless security solutions that are better aligned with their primary tasks. To take advantage of this capacity, two-way communication between security and employees needs to be implemented, repurposing user feedback to improve the organisation's security approach. This can also bridge the divide often observed between security and productivity-focused organisational divisions (Ashenden and Sasse, 2013). The purpose of feedback solicitation is to learn something from users that security implementers could neither predict nor detect from their position outside of the primary task. Security managers do not see security from the perspective of employees, and so cannot assume they have designed security that fits their primary task, unless they have otherwise engaged with them in the design and deployment of security solutions. This learning and communication approach can be achieved through:

1. Persistent and readily-accessible feedback channels as part of the organisation's structure and culture (e.g. a "we've just upgraded your email client, is it working well for you?" pop-up that "gobbles up" any post-deployment frustration). If an employee reports a security concern, there should be a visible response that describes the impact their feedback has made.
2. Security enforcement among team members should be scaled to cover the wider organisation: employees can champion secure behaviour within their teams, situating security practices in primary roles in a more meaningful way than sanctioned security communications.
3. By advertising a capacity to listen, security managers can leverage employee experiences as an additional layer of assurance that security mechanisms are serving the business. In addition to receiving feedback for improvements on security mechanisms and policies, advertising organisational capacity to listen can increase employee positive attitude towards security, increasing their propensity for secure behaviour.

4. This approach also makes it possible to improve communication and training, by logging employee misunderstandings or reported insecure behaviours, identifying areas where actions are most urgently required.

To conclude, engagement with employees should aim to reframe security in the organisation as a collaborative activity, not as a barrier to work, taking advantage of internal employee propensity to participate in security risk mitigation, and use it to deliver security implementations that accommodate for employee primary task priorities.

7.3.1.3 Employee participation does not mean delegation of responsibility

Adopting a participatory approach to security management should not be misinterpreted as delegation of responsibility for organisational protection to employees. Pallas (2009) argues that the increasing decentralisation of modern IT implementations means that security challenges need to be solved in a decentralised, cooperative way, arguing that hierarchical security management leads to suboptimal outcomes. He then argues for more autonomy, explaining that coordination costs for centrally-administered security can be too high, and that formal rules are more expensive than delegating responsibility to employees. But, despite the identified motivation for secure behaviour, delegating responsibility to employees also requires accurate risk awareness, which employees often do not possess, as the findings of this thesis suggest. Information security is complex and quickly changing, with effective security risk mitigation being a challenge even for experts; delegation of more responsibilities to employees cannot provide effective protection. Herley (2014) echoes this by also explaining that directing more responsibility towards users is not an effective way to manage security: employees should not be expected to incur additional costs due to the failure of security management to identify other solutions. This cost can be prohibitive if no formal procedures exist to identify and eliminate friction-inducing security: employee attempts to behave securely can consume a significant proportion of their resources, and thus the total organisational resources invested to deliver security. In addition, the emerging primary task disruption can lead to further user alienation from security, reducing their propensity to contribute to organisational protection.

Organisational security management should not try to shift responsibility for protection towards employees, but learn from them and improve its practices. As the findings of chapters 4 and 5 demonstrated, well-designed security acts as a secure behaviour driver. Deploying a learning-based security management approach, reduces the coordination costs of security management, a factor that Pallas considered prohibitive to centrally managing security. It is a cheaper approach to implement and much easier to control, while at the same time using employee understanding and behaviours to drive centralised security management decisions. Well-designed security based on collaborative, participatory management can provide effective risk mitigation, leading to what Camp (2011) described as a "community based production of security". This can lead to the development of a security-conscious organisational culture, and enable better coordination and employee participation in security protection and improvements.

7.3.2 Management Training – Engage with Low- and Middle-Management

A decentralised and collaborative approach to security management also requires effective low-to-middle management engagement. As explained in chapter 5, line managers are in a powerful position to act as motivators for effective security behaviours. Thus, it is important to ensure they possess adequate and accurate security awareness and understanding amongst them, in order to promote secure behaviours and culture development amongst employees. Security managers need to be aware of this, and (1) understand manager role in shadow security development and that any security awareness or education they broadcast will be interpreted and mediated locally, (2) listen to managers' questions, problems and concerns, incorporating those as another source of information in participatory security design, and (3) help them develop correct and consistent security advice for their teams through tailored training.

7.3.2.1 Role in shadow security development

Security is a collective achievement and line managers play a central role in shaping security decisions and behaviours within organisational sub-divisions. In both companies examined, employees often turned to their managers for security support when existing security mechanisms created significant primary task friction (e.g. slow access control), or when policies did not provide comprehensive, role-specific answers to security challenges (e.g. what to do under emergency need for access conditions). In those cases managers had to prescribe actions that address the emerging friction, but also preserve team productivity. They ended up making local, and often ad-hoc, decisions about security, like access control granting and recommending information sharing practices. The emerging security practices lead to shadow security evolution, varying security behaviours, and micro-culture development across organisational sub-divisions, eventually leading to security behaviour spinning out of central control. But the impact managers have on their teams also means that when individuals consult their managers, they are more likely to design novel solutions that better address the risks faced by team members, also preserving productive capabilities. Their significant role in managing security at local level, together with their understanding of role-specific challenges, suggests that line managers are well-placed to help security management accurately capture security behaviours and learn from shadow security development.

7.3.2.2 Provide role-specific training

Security-specific training should be tailored for managers to acknowledge their role as mediators of security. Rather than overloading them with security information, communication to managers should focus on role-specific goals and related security principles. It should also formalise and communicate their team-level security management responsibilities, also providing them with adequate resources, support and knowledge to respond to those. In this way, when managers need to support their team members, they will be more likely to come up with novel solutions that effectively address their role-specific risks.

7.3.2.3 Include managers in security improvements

The importance of line managers in shaping organisational security behaviours, calls for inclusion of them as an integral part of organisational security improvements. They frequently interact with employees and have a unique perspective of the friction between security and productivity tasks.

Soliciting feedback from them can contribute to an effective amalgamation of shadow and prescribed security practices. Communication also needs to be two-way, extending participatory security design to include line managers: in addition to influencing their staff's security decisions, they can also elicit feedback from them on the challenges creates for their primary tasks. Security management should liaise with them to deliver role-specific and consistent security advice to different organisational divisions, also using manager feedback to drive security improvements. Essentially managers need to act as a bottom-to-top feedback channel for identification of friction-inducing security. They can also communicate to security management on the evolution of informal rules (Pallas, 2009) at team level, which can then be formalised, if they are consistent with organisational risk appetite. If organisations neglect to do so, managers and their teams will continue to create their own rationalisations as to what their interactions with information security mean, and how to balance their perceived need for security with their main goal of primary task completion.

7.3.3 Employee involvement improves motivation

Involving employees and managers in security improvements creates a participatory security environment that can improve employee security behaviours. Pallas argues that, given lack of control, employees will always act opportunistically, which then increases non-cooperative behaviour and corresponding secure behaviour motivation costs for security management. But the findings presented in chapters 4, 5 and 6 of this thesis suggest that, if employees understand the need for security, and security mechanisms and processes are well-designed (minimal cost), employees are sufficiently motivated to invest some resources (time and effort) to protect the organisation instead of behaving opportunistically. This willingness to participate in security needs to be further encouraged by security management, through visible communication of the positive impact of employee participation and inclusion of security in group meeting agendas. This can lead to increased employee awareness about the actions required to keep the organisation secure and improve employee ability to connect with the risks presented by their managers or colleagues. This increase in their perceived contribution and ownership of security implementation amongst employees, can further trigger internalised norms and benevolence-related compliance identified in chapter 6, further discussed in the next section of this chapter.

7.4 Trust as a security risk management tool

Security management also needs to understand and allow for the effects of organisational trust relationships on security behaviours. As discussed in chapter 6, in a highly social environment like a large organisation, inter-employee trust is often more important to employees than complying with security. This should not be used as a pretext to treat employees as untrustworthy though: employees possess both the ability and motivation to exhibit trustworthy behaviour as long as their ability to complete their primary tasks is not significantly hindered by security. Using the improved understanding of trust relationships and their impact on security behaviours emerging from chapter 6, this section discusses what organisational security management can do in order to accommodate for organisational security trust relationships in security implementations.

7.4.1 Ignoring trust creates problems

Many organisational operations depend on the presence of trust (chapter 6), thus security cannot silently accept its presence but refuse to account for it. Security management should aim to formalise trust presence, understand its impact on security behaviours, and manage it to deliver more effective risk mitigation. The results of chapters 5 and 6 demonstrated that organisational insistence on using technical mechanisms and sanctions to eliminate or reduce the need to trust employees has a number of negative effects:

1. *Friction between security and productivity*: Attempts to restrict employee actions within pre-defined domains often lead to high security-primary task friction, encouraging shadow security development. Attempts to eliminate this through excessive assurance lead to a negative attitude towards security. The emerging disgruntlement drains identified employee capacity to behave securely and can damage employee emotional connections with the organisation, increasing the risk for insider attacks and loss of human capital.
2. *Increased security violations and shadow security development*: Assurance often asks employees to treat their colleagues as untrustworthy (e.g. "don't share your password"). But employees prioritise inter-employee trust relationships from security compliance, with temporal and contextual incentives to develop and preserve relationships with their colleagues leading to violations of security policy (password sharing, information sharing through unofficial channels, tailgating etc.). In the end, assurance ends up turning inter-employee trust to a readily-available, low cost resource for collaboration and enabler of productive activity when employees need to minimise the impact of friction-inducing security.
3. *Insecure culture development*: Lack of enforcement (e.g. password sharing not penalised when detected) leads to the development of a culture where breaking security is justified. Long-term reliance on collective trust violations leads to security spinning out of organisational control, with security behaviours significantly deviating from security policies.

The above points suggest that, in order to effectively manage security, the presence of trust relationships needs to be acknowledged and leveraged by security management in the organisational security implementation.

7.4.2 Formalise trust presence in security management

Organisations trust their employees, but currently there is no formalisation of this trust in security management. Current approaches to organisational security implicitly trust employees: many of the policy clauses in the organisations examined were not accompanied by mechanisms to enforce those or identify policy violations. Information handling for example, was significantly dependent on employee actions, with employees being free to copy information to external drives and share it with their colleagues. The trust shown by the organisation towards employees has been defined in chapter 6 as *organisation-employee trust*. This needs to be formalised and leveraged by security management to take advantage of both users and technology to achieve effective protection. To deliver this, security management needs to (1) understand the importance of security hygiene as a trust prerequisite, (2) formalise a "when to trust" and "when to assure approach", (3) support correct trust development through

inclusion of trust in security communication, (4) avoid over-enforcement where trust develops, but also (5) enforce assurance when required to mitigate risks where trust is not an acceptable risk mitigation approach.

7.4.2.1 Understand the importance of security hygiene on trust incentives

User-centred security is a pre-requisite to trusting employees. Employee secure behaviour requires removal of unusable elements of the security implementation, with security communication and training providing sufficient *motivation* for secure behaviour. As a result, user-centred security design and communication principles, discussed earlier in this chapter, should be treated as a prerequisite (or hygiene requirement) of any attempt to include trust in organisational security management.

7.4.2.2 Formalise trust and assurance in risk management

As previously discussed, implementing assurance mechanisms for all possible employee behaviours is prohibitively expensive. The productivity benefits of trust have been identified in non-security related contexts: trust between members of an organisation leads to highly cooperative behaviours, acting as a substitute for control (Costa et al., 2001). In addition, employees that feel connected to an organisation are more committed and involved with it (Bussing, 2002). Organisations should aim to achieve similar benefits in a security context, leveraging already existing trust relationships to provide effective protection. They need to take advantage of the intrinsic incentives driving employee secure behaviours, taking advantage of second-order trust benefits (goodwill, positive culture development and reduced assurance costs). Ability to solve security challenges through goodwill and improved awareness also allows for efficient reallocation of resources available to security, to address other risks.

Trust should also be part of organisational security risk management. Formal decisions need to be made on where assurance is necessary and where trust is required. Trust should be present when employees have adequate incentives (both contextual and intrinsic) to behave securely (e.g. when organisational provisions for sharing of information allow effective and efficient primary task activity). Assurance on the other hand is required when the rewards from not playing by the rules are significantly higher than the consequences of not doing so. In such cases an organisation needs to take actions to reduce potential exposure to malicious behaviours (e.g. block potential for leavers to access sensitive information, or monitor and audit access and copying of data from sensitive corporate fileservers from where employees should not be downloading vast amounts of information). Some of the actions in question may not constitute an offence on their own, but can provide sufficient grounds for further investigation; where the line is drawn depends on organisational risk appetite. Where an organisation decides to implement assurance instead of trust, the "business, not personal" nature of the controls put in place needs to be made clear to employees through security communication. Employees are not deemed as untrustworthy; controls are required in order to protect the organisation from malicious outsiders and insiders. Finally, where organisational reliance on employees exists, it should be formalised in order to be better reflected in information security management strategies: after identification of security-related risks the mitigation method (assurance vs trust), together with the related organisational actions required (mechanisms implemented, communication sent, training module content updates) should be recorded as a formal risk management decision and revisited over regular intervals to assess potential need to reconsider it.

7.4.2.3 Include trust in security communication

Where security management decides trust is required and can be beneficial to the organisation, its presence should be made explicit. After security mechanisms are implemented in a way that encourages trustworthy behaviour, Security Awareness, Education and Training campaigns (SAET) should be used to enable employees to better understand the actual risks the organisation faces. For example, in Company B, home working is quite prevalent, with many employees being either full time home workers or working from home two or three times a week. This makes it impossible for the organisation to restrict employee actions: if no trust is shown on their ability to protect the information they carry with them, they will be unable to proceed with their primary tasks. This organisational dependency on employee behaviour should be communicated to employees, to explain their responsibility and contribution in keeping the organisation secure. The emerging SAET approaches should: (1) make it clear to employees that they are trusted and supported in their security decisions (to improve motivation), also explaining the "it's business, not personal" need for security vigilance, and (2) include information on current threats and how real-world trust development signals break down when using computer systems (improving ability).

7.4.2.4 Once developed - don't enforce it!

If an organisation considers its employees as trustworthy, this decision needs to be formalised and honoured. The first assessment of an employee's trustworthiness comes even before they join the organisation, through recruitment background checks and vetting procedures. This process uses past employee behaviour as an indicator of potential future actions. When the organisation establishes that ability and motivation for trustworthy behaviour are present, there's no need to over-assure. Employees that pass the screening process should be considered trustworthy and treated as such instead of being subject to continuous restrictions. Visible presence of trust towards employees can further increase employee trustworthiness, by injecting secure behaviour in the organisation-employee psychological contracts that dictate organisational employee behaviour. The emerging cooperation can benefit all stakeholders (employees, top management and security management), providing three major advantages:

1. People in an organisation develop shared values and a shared-sense of responsibility for the well-being of the organisation, based on shared formal or informal norms promoting cooperation (Fukuyama, 2001; Resnick, 2001), which also affect their security behaviour (Pfleeger et al., 2014). Secure behaviour should be driven by a feeling of contribution to common organisational interests, rather than rule-driven actions to avoid sanctions.
2. Organisational attempts to enforce friction-inducing security will be reduced. This will reduce both productivity-driven and trust-driven policy violations, lowering the levels of "noise" the above introduce in security monitoring; precursors of serious attacks (e.g. intellectual property theft[26]) can be lost in false-positive alarms if employees frequently violate security for

[26] Intellectual property theft accounts for a small percentage of all cybercrimes, but results to the majority of the resulting monetary losses, Rantala, 2008)

productivity or collaboration reasons. As a result, organisational ability to monitor, detect and enforce its security policy will improve, improving the overall efficiency of the organisation's security implementation. The resources saved from reduced noise can be reinvested in implementing other more effective security mechanisms, enabling the implementation of clever monitoring to identify serious malicious activity (insider or outsider attacks - Caputo et al., 2009).

3. Flexibility strengthens employee ability to defend the organisation. Attackers are likely to adapt to new technologies, but attacks are much harder to succeed with suspicious employees, motivated to protect the organisation and a culture that favours secure behaviour. This is not uncommon in other security implementations: for example biometrics at passport control points are considered to be more effective than individuals, but when a problem is identified, a human can take over and use a much richer and broader set of factors from the context of the environment to assess a passenger's trustworthiness (Fléchais et al., 2005). The presence and formalisation of trust, together with the emerging perceived responsibility, acts as an additional motivator for employees to behave securely.

7.4.2.5 Enforce assurance through contextual incentives when necessary

Trust should never be perceived by employees as inability of security management to enforce security rules. Security management needs to accept that formal rules left unenforced are ineffective, especially if lack of enforcement is visible. Risk-aware employees, interacting with well-designed security mechanisms, no longer have reasons to violate security. As a result, when the rewards from not playing by the rules (benefits from malicious actions) are significantly higher than the consequences of not doing so, assurance mechanisms need to exist to change the risk-reward structure, thus dis-incentivising untrustworthy behaviour. In such cases, violations can be detected by improving current monitoring implementations to include contextual information on user behaviours, which can be used to detect employee trust abuse and precursors of insider attacks. Malicious actions should then be followed up with serious consequences that are visibly enforced. Visible enforcement can act both as a deterrence for future misbehaviour and as a motivation improver, reminding employees that they are trusted and responsible to keep the organisation safe. On the other hand, organisational inability or unwillingness to enforce the policy (as identified in the interviews) is seen as weakness, leading to security appearing as less important to employees, reducing compliance incentives (reduced motivation and perceived contextual incentives). By making contextual incentives visibly enforceable through assurance and enforcement, security management deters potentially malicious behaviours or other actions that put the organisation at risk, but also reduces shadow security development stemming from perceived ineffectiveness of official security.

7.4.3 Accommodate urgency, encourage self-reporting and follow it up

Security management also needs to implement formalised processes for unusual circumstances where security may need to be bypassed. Employees may, under *rare* and *unusual* conditions, have to circumvent security for productivity reasons. In such cases mechanisms should be in place for employees to report their non-compliant behaviours (Bartsch, 2014). Clear instructions should then exist for employees and security management on how to deal with emerging vulnerabilities. For example, an

employee who shared their password with a colleague in an emergency situation should recognise this as a violation, then login to a "violation logging" system and report the behaviour. The same should apply to physical access control: an employee who forgot their access pass should be easily able to get a daily pass through a simple verification process. In both cases, the organisation should encourage self-reporting by communicating that no action will be taken against employees who self-report, while those who do not should be susceptible to sanctions. The organisation should also ensure adequate measures were taken to close any resulting loopholes (e.g. forcing the employee who shared their password to change it within two hours). Accommodating for urgency should not be implemented as a substitute to usable systems though. Violations, even reported ones, need to be infrequent enough to avoid non-compliance becoming part of organisational security culture, also avoiding introducing significant resource overheads to address the loopholes created by frequent circumventions. Insecure behaviour cannot be totally eliminated, as this is both uneconomical and prohibitive for productivity, but enhancement of the organisation-employee trust relationship can ensure that it happens rarely and employees take appropriate mitigating actions.

7.5 Measuring shadow security

Measurement plays a key role in modern security management, but current attempts to devise behaviour-related security metrics are ineffective, expensive and also fail to accurately capture employee security practices. Key Performance Indicators (KPIs) are widely deployed by organisations to benchmark their performance against set targets and competitors, often also driving security strategy decisions (Cai et al., 2009). The need for effective security metrics to aid security management decision making and risk assessment is widely accepted in information security (ISO 27004; Johnson and Goetz, 2007). Currently information security uses metrics mostly focused on technical aspects; security managers have access and monitor detailed technical information on intrusion attempts, virus logs, access requests, traffic information and many more (Brotby et al., 2013; Payne, 2009; Wong, 2011). An international standard on information security metrics also exists (ISO27004), defining a measurement processes for assessing the effectiveness of Information Security Management Systems. Unfortunately, current use of metrics to measure security behaviour is of limited scope and expensive. Metrics defined in the latest edition of ISO27004 consist largely of "tickboxing" elements (e.g. *count of logs/registries with annual information security awareness training field/row filled as "Completed"*) or require the organisation to manually collect information from its employees (*ask each user about the number of their passwords that satisfy organisation's password policy*). Other attempts to measure security behaviour in the form of empirical guidelines from commercial security organisations, present no scientific justification for the measurements they recommend. They also demand excessive effort for data collection, asking organisations to conduct surveys and phishing exercises to determine user awareness and benchmark the organisation (e.g. Bond et al., 2014), or manually collect the information required to assess employee behaviours (e.g. Rudolph, 2006).

Security management needs to observe real usage data and user feedback to learn how to adapt security provisions to achieve both productivity and security. Bartsch (2012) argues that organisations need to examine the presence of precise knowledge to guide authorisation decisions and reuse it to drive the deployment of those. An attempt to achieve this is documented by Smetters and Good (2009), who

conducted an in-depth examination of access control in organisations. Their findings revealed interesting insights on the state of access control in organisations, but only managed to capture a snapshot of the state of access control at a specific point in time. Given the quick pace with which technologies and emerging security risks undergo change, conducting one-off work can be of limited usefulness to attempts to continuously monitor behaviour-related metrics. Easy-to-collect security behaviour metrics that allow for a more accurate representation of employee behaviours than existing ones, can be a powerful tool for security managers. They provide them with the ability to understand how security fits with productive tasks in practice, thus improving their security management decisions. Shadow security provides the opportunity to collect such information. This section discusses how shadow security indicators can be used to devise security behaviour metrics, using information that is mostly, readily available in an organisation. It also explains how those metrics can be used to drive subsequent security management decisions for improvements, assess the effectiveness of those improvements, and allow for continuous monitoring to detect insecure behaviours and react before they become threatening to the organisation.

7.5.1 Shadow security and measurement

The presence of shadow security presents a good starting point for measuring employee behaviours in organisations. The identified problems of current behavioural metrics suggest a need to look deeper into readily available, or easy to collect, information to develop more effective ones. Security managers ought to consider how to identify the indicators and drivers of shadow security and develop a capacity to analyse and adapt, in cooperation with other functions in the organisation. Unfortunately, periodic repetitions of the methodology presented in this thesis can be prohibitively expensive. But many of the behaviours presented in chapters 5 and 6 can be identified through information that exists in abundance in modern organisational IT systems. As Hubbard (2010, p. 48) puts it, “anything detectable at different amounts is measurable”. Using readily available information signifying shadow security behaviours allows better understanding of the prevalence of those in the organisation, enabling more effective resource allocation for future organisational security improvements.

In order to take advantage of the emerging ability to identify and measure shadow security, organisations need to adopt a risk-oriented behaviour measurement process. This should aim to, identify target employee behaviours using the improved understanding emerging from shadow security, devise required metrics and identify sources of information, arrange access to those, and then adopt an iterative monitoring approach, as presented in Figure 16:

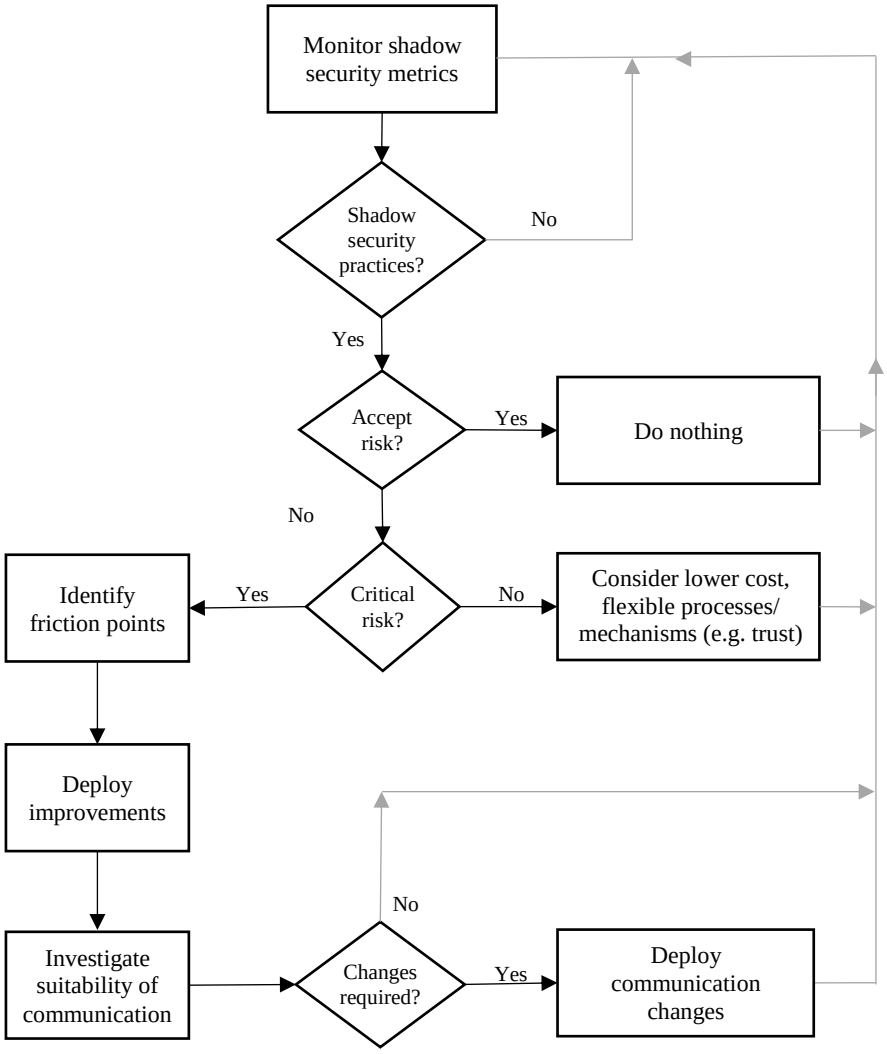

Figure 16: Risk-driven intervention process

The above process allows security managers to continuously monitor their implemented shadow security metrics, assess the emerging risks and then take appropriate risk-mitigating actions, based on organisational security risk appetite. The above process is also consistent with the security metrics process presented in the ISO27004 international standard for information security metrics.

7.5.2 Sources of measurement

In order to identify available information that could be used to develop shadow security metrics, the researcher worked closely with Company B, identifying a number of potential sources of behavioural indicators. Information on a number of different shadow security topics was readily available through various organisational systems: network access logs, access control data, leavers' process statistics, data on usage and availability of organisational systems for information storage and sharing, logs from clear desk checks, and statistics from IT support and employee feedback mechanisms. All these can be used to identify elements of the security implementation that encourage shadow security development and quantify mechanism and process-specific behaviours. The remainder of this section combines the improved understanding of employee behaviours that emerged from shadow security and trust development, together with information that is readily available in large organisations (or can be easily

collected), to (1) devise a set of security metrics that accurately capture shadow security presence, and (2) drive organisational security risk management and decision making to more effectively manage employee security behaviours.

7.5.2.1 Information handling, flow, sharing and storage

For large organisations like the ones investigated in this research, it is common for employees to engage with colleagues situated in various locations around the country, or even overseas. Combined with the increasing prevalence of home working, remote collaboration results in sensitive organisational information being present at various locations and on many devices, increasing the potential points of failure that could lead to security compromises. Both the organisations studied had implemented internal file storage and sharing systems that employees could remotely access, so in theory, provision for secure behaviour was in place. But problems in capacity, slowdown in accessing the organisational systems and lack of flexibility (no access provisions for various types of devices) led to employees using other ad hoc practices to share information. Employees resorted to using third-party cloud storage solutions for sharing sensitive information, due to a perceived lack of organisational support for effective file sharing, thus exposing the organisation to potential security risks. To detect such behaviours, which also suggest problems in the usability, availability and effectiveness of the systems in place, an organisation's security management needs to observe the following:

1. *Metrics generated by agents on managed organisational computers* (e.g. Data Loss Prevention agents - DLP). This software can provide quantitative data on the volume of information shared through emails or sensitive information stored locally on corporate machines, allowing deducing data handling information. Security managers can track the number of attachments or pattern-matched text excerpts being sent, or information sent to out-of-company email addresses. As Smetters and Good (2009) identified, email mailing lists (and the dynamic groups generated in the "to" and "cc" lists of each message) are in fact the most commonly used access control lists encountered by users.
2. *Check volume of traffic to third-party cloud storage servers* (from inside the corporate network and company computers). This aims to identify the use of third-party storage to store and share corporate information. It may be difficult to distinguish with absolute certainty on which parts of cloud storage traffic relate to corporate information, as opposed to employees accessing personal files while carrying out personal tasks on corporate machines, but extensive use of cloud providers can indicate a need to investigate current use of organisational systems.
3. *Check utilisation of internal file-sharing systems*. Does it make sense if an employee has not accessed their personal file space in two or three working days? If network storage provisions are not used, can the organisation identify organisational information stored locally on employee computers? If excessive use of and reliance on local storage is identified, the organisation should investigate organisational storage and connectivity problems, also gauging employee awareness of the existence of organisational storage provisions, together with feedback on usage experience.
4. *Monitoring external drive use (encrypted and unencrypted)*. The results also suggested that some backups and sharing of information within the organisation was done using non-approved unencrypted hard drives and USB sticks. Monitoring the use of those (e.g. through the use of

locally-installed software) can also allow the organisation to identify potential issues with organisational provisions. It can also gauge potential employee policy awareness of the need to use encrypted drives.

5. *Clear desk logs*. Company B has clear desk checks that occur every night, after employees have left the office. Those currently record the number of documents found on employee desks and potential classification markings on those. By comparing the number of documents found during clear desk checks before and after clear-desk related communication has gone out, an organisation can assess its effectiveness. In addition, close examination of some of the documents can reveal the understanding amongst employees of the organisational classification scheme. This can drive both improvements in communication and training, but also attempts to improve the comprehensiveness and context-specific applicability of organisational data classification approaches.

The metrics defined above can raise a number of questions that security management will need to address through a risk-driven intervention process: (1) if staff avoid using organisational systems, consider sending files to personal accounts via email easier, share information through third parties and unencrypted drives, and avoid classifying the information they use, what does this mean for the organisation? Is the nature of the information mishandled sensitive? If yes, is the organisation willing to accept potential risks? If no, security management should then (2) consider where organisational information storage/sharing systems create problems in employee workflow (e.g. lack of adequate storage, problems in setting up file sharing mechanisms, problematic connectivity). Where related risks may be considered less threatening, security management may choose to (3) consider providing employees with more flexible solutions (e.g. encrypting laptops to allow local storage of information and providing easy to use encrypted email communications), while for more severe risks it should (4) invest in improvements to reduce those disruptions. In addition, security management should (5) investigate whether organisational training and communication effectively communicates the risks of identified practices and the presence of organisational mechanisms to mitigate those. Applying the measurement process defined in the previous section (7.5.1) for information handling practices[27], the process in Figure 17 emerges.

[27] This process should be applied to all the other measurement areas outlined in the remainder of this section. For space reasons I only include this one example on information handling

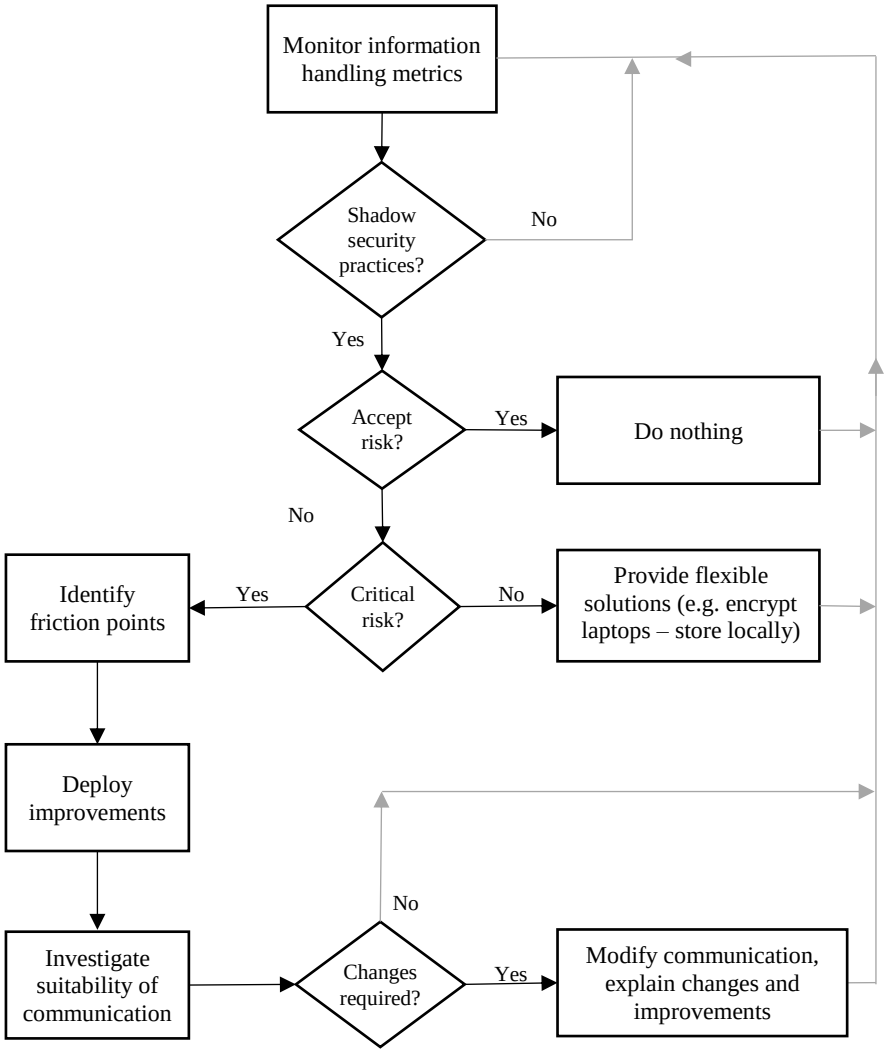

Figure 17: Risk-driven intervention process for information handling systems

7.5.2.2 Access Control - Provisioning of Accounts

Quick deactivation of a leaver's account was reported as being very important by the information security managers of both participating organisations (in one of the two companies there was a target of a maximum of 48-hours for deactivation). But examination of organisational account control systems and discussions with account managers, revealed that in many cases leaver's accounts are left active for much longer, either in case future need for system access emerges, or because accounts administrators were not informed about an employee having left the organisation. An interesting example came from contractor accounts: many people whose contract expires, often re-join the organisation after short periods of time, so their accounts were left untouched "just in case they come back". Another example was the use by new starters of their supervisor's accounts until their own account could be set up, while the supervisor remained close-by during use as a security precaution. In order to identify these, and other account misuse cases, an organisation can measure the following:

1. *Mean time for leaver account deactivation*: Measure mean time it takes for an employee that has left the company to have their access revoked and compare this to targets defined in the organisation's security policy. If this time is higher than what organisational security risk management considers acceptable, improvements are required in access revoking process; either

better connection between accounts management teams and HR, or delegation of access revoking to line managers.

2. *Mean time for new account creations*: Measurement of account creation time is also important; if new accounts take long to create, teams will use what they already have: managers and teams use generic accounts, or accounts that are left active after people leave the company, or even share their passwords to provide access to new joiners. The time between an account creation request and successful account creation, can indicate the perceived lead-in time required so that the creation process is completed by the day a new employee has joined the organisation. In cases where emergency access is required, organisations should consider creating centrally-managed short term access provisions.
3. *Prolonged account inactivity*: If an account is showing no or limited activity, it could either be unused (and should be a candidate for deletion), or the owner has simply chosen to act outside of the access control system, accessing files in some other way. In such cases, what barriers do organisational access-granting processes create? Is there a way to mitigate this effect? This metric can also indicate to security managers that a provisioned system is seeing inconsistent use and may also provide inconsistent coverage and security.

These three metrics can allow security management evaluating the effectiveness of current account management provisions, taking actions to mitigate risks from account sharing. Reduced account sharing will also allow for accountability in conditions where further investigation of employee actions and subsequent enforcement are required.

7.5.2.3 IT support - Response to helpdesk requests

Security management should also aim to assess the effectiveness of organisational provisions, aiming to support employees in their primary tasks. As the results have shown, ineffective organisational support provisions can lead to employees distancing themselves from organisational security. Support should be assessed using a number of indicators:

1. *Resolved/Not resolved problems* and *Time to fulfil request*. Security managers should be able to identify whether support provisions can meet employee needs and assess the impact of potentially problematic support functions on employee ability to comply with security. Support processes may be appropriate, and employees instructed as to when to contact a helpdesk in specific circumstances, but then the response time becomes critical. If call response times are slow, employees with momentary pressures (e.g., deadlines, one-off meetings with associated deliverables) will have to adapt there and then using their own understanding of IT and security expectations.
2. *Number of incidents responded to and time taken to respond.* In some cases employee requests may not be fulfillable. Despite that, it is still important for support functions to communicate back to employees the reason for refusal. The time taken for this response is equally important. Slow responses that lead to undesired outcomes can distance employees from security, reducing their willingness to request formal support in the future, which acts as a key driver for shadow security development. In addition, details of "unusual" requests need to be recorded, to allow identification of potential lack of organisational provisions for some primary task needs.

Unusual requests can also aid identification of employee misconceptions and unrealistic expectation from security support that can then be targeted through communication and training.

The above metrics can be useful for an organisation to assess the effectiveness of central security support provisions. Target performance values (e.g. time to respond, number of issues resolved etc.) may differ across organisations, even across organisational divisions, due to varying security risk appetite, so the above metrics need to be adapted to the specifics of the target environments. In addition, when support performs outside desired limits, helpdesk staffing and staff training may also need to be revisited.

7.5.2.4 Employee feedback and reports

The results from the interview and the survey analyses also showed that employees are willing to report security mechanisms that cause problems in primary task completion. Despite that, in a number of cases they believed the organisation did not respond appropriately to their reports. Security management needs to treat employee willingness to report as an opportunity to identify elements of security implementation that currently fail to serve the primary task purpose. In order to achieve this, employee reports should be:

1. Grouped based on related security implementation elements, combined with numerical metrics for each different element (e.g. remote access problems, password reset requests). Interventions should then be prioritised to address high primary task impact problems first.
2. Logged, in order to create an "end-to-end" story. Employees should be informed about the number of new issues security management identified and resolved using their help, stressing the importance of their participation to deliver effective security. The effectiveness of such an approach can be measured by logging employee reports and calculating the percentage of those where improvements were delivered and feedback was provided, with security management aiming to address as many of the reported problems as possible.

Successful implementation of the above can increase employee participation in security management. The emerging participatory security environment can allow security management to create (or modify) solutions seamlessly integrated with employee primary tasks, thus reducing non-compliance and shadow security development. In addition, communication of the influence on security management of employee feedback and reports, can increase employees' perceived contribution in protecting the organisation, improving their motivation for secure behaviour and reporting of security problems, reducing their reliance on shadow security practices.

7.5.2.5 Password behaviour

Employees having to deal with friction-inducing password policies and mechanisms, often resort to self-devised password management strategies, using their own risk awareness and the presence of inter-employee trust to reduce emerging primary task impact. In the interview analysis a number of practices were identified relating to password use: despite awareness of policy clauses on password selection, with writing down and sharing of those also not permitted, employees choose simple passwords to cope with frequent changes, write those down in password protected documents or notebooks they carry with them all the time, or share those with colleagues to ensure responsibility delegation or urgent access to systems is provided when access management is perceived as problematic. Employees often also recognise the risks associated with their practices as well. As discussed in section 7.2, security hygiene should be

security management's priority in order to reduce emerging insecure practices; in this case realised through easy to use password managers compatible with all organisational systems and quick and effective access management procedures. In order to measure the effect of attempted improvements, a number of sources of information can be used (in addition to the adoption of password manager discussed in section 7.5.2.2):

1. *Feedback and reports on password manager adoption*. Measure employee report of problems with password management software. Line managers should also be probed to discuss the experience of their staff with the software at group meetings and communicate it back to security management. Problems with password manager should be addressed to avoid creating the need for employees to resort to other practices.
2. *Abnormal access patterns.* Employee sharing of passwords can be detected through the presence of abnormal access patterns from employee accounts. Those can be both geographic and machine-based mismatches, between subsequent log-in sessions or physical access control and attempts to access organisational systems. High frequency of abnormal access patterns indicates a need to examine the effectiveness and response times of organisational access granting processes (also discussed in section 7.5.2.3).
3. *Password reset statistics*. The number of password resets should also be measured (both through logs of calls to the security helpdesk and automatic reset mechanisms). High number of password resets can indicate excessive employee reliance on those, due to either forgetting their passwords, or resetting those after sharing with their colleagues to eliminate potential risks. Frequent password resets can signal the need to increase timeframes for password expiry, again depending on organisational risk appetite, even considering providing one-time access tokens for infrequently used systems.

When security management implements changes in security mechanisms or processes driven by the above metrics, security communication should aim to draw employee attention on those, with line managers also communicating the potential benefits to employees.

7.5.2.6 Screen lock monitoring

Employees often do not lock their computer screens when they leave their computers unattended, despite their awareness of the need to do so. The main driver for this behaviour is the existence of inter-employee trust, with the belief that their colleagues can be trusted to behave securely acting as a risk mitigating factor by itself; consequently it reduces their perceived need for screen locking practices. For some organisations this may be acceptable, for example if the number of external people present in a specific environment is minimal, or when certain functions deal with non-critical data. In other cases security management may decide unlocked screens are risky and should be eliminated. In order to measure and influence such behaviour, organisations need to record the number of unlocked screens identified during regular checks, communicate the importance of screen lock policy clauses in mitigating security risks (through channels appropriate for each target organisational division), and eventually sanction violations. Follow-up measurements of unlocked screens can assess the effectiveness of the above approach. Contrary to other metrics presented in this section, the measurements required for screen lock behaviour monitoring cannot be easily collected from organisational systems or existing physical

processes, so investing some organisational resource for manual data gathering is required. But if security management believes that related risks justify the required time and effort for data collection, either for the whole organisation or for specific functions, cost-effective ways should be found (e.g. security staff conducting random checks around organisational premises).

7.5.2.7 Actual adoption and use of organisational systems

The organisations examined implemented centrally managed systems to enable employee secure behaviour. Password managing tools were present in Company B for employees to store their passwords, while network storage was available in both companies to provide secure and backed up storage for organisational information. Shadow security practices emerged when those systems failed to meet employee productivity needs: (1) the password manager was incompatible with some systems, so employees had to find other ways to store their passwords, (2) network storage was limited, leading to local storage and ad-hoc backups, and (3) connectivity provisions were unreliable, leading to employees using self-procured approaches to transfer files. The above practices increase organisational security risks, but there is currently no mechanism in either of the two organisations to identify such practices and take appropriate risk-mitigating actions. Security management can identify potential disruption caused by such mechanisms by measuring:

1. *Password manager adoption and usage statistics*. Low adoption and usage of password manager can indicate that employees resort to other practices to manage the large number of organisational passwords they have (e.g. writing those down in documents).
2. *Utilisation of network storage.* Lack of usage of organisational storage provisions also indicates that employees resort to other practices (e.g. storing information locally and backing up to own drives).

In both the above cases, lack of use of organisational provisions should be seen as a need to examine the fitness-for-purpose of related mechanisms, also requesting feedback from employees or their line managers on problems they encounter when using those.

7.5.2.8 Assessing behaviours and SAET effectiveness

As discussed in section 7.2.3, it is important to ensure that security training is tailored to employee tasks in order to address organisational security challenges. But current metrics on user behaviour required for ISO standard compliance are related to completion rates of organisational training programmes, which only proves successful completion, without allowing for assessment of the effectiveness of the training. In addition, general employee security awareness and behaviours are hard to measure, without consuming significant employee time and effort through employee surveys and questionnaires. Both the above approaches provide minimal ability to dynamically monitor employee responses to changes in the security environment and are also impractical for frequent use, thus unsuitable for a dynamic, metrics-driven security management approach. The metrics defined in the previous sections can address the above drawbacks: they can be collated to create an overall indicator of employee security behaviour, which can be expressed as a function of (1) training completion rates, (2) employee actions to mitigate organisational risks (e.g. reporting potential security risks, screen lock, password manager adoption), (3) their information storage and sharing habits, (4) their willingness to report potential problems back to the

organisation and participate in security protection, also adding in (5) manager training completion rates (Figure 18).

$$Security\ behaviour = a(training\ completion) + b(actions) + c(information\ habits) + d(reporting\ rates) + e(manager\ training)$$

Figure 18: Overall security behaviour formula

The fifth element of the above formula, manager training, is hard to measure through readily-available organisational information. It requires access to manually collected information for manager education, like measuring manager CBT success, also assessing management training effectiveness through possible questionnaires and surveys (that may still be expensive and time consuming, but are easier to conduct and cheaper if they are only targeting managers instead of the organisation in its entirety). In addition, behavioural variations between different organisational divisions can also be attributed to differences in management, as one of the major factors for shadow security, and subsequent micro-culture development, was line manager communication. It is also important for security management to understand that the coefficients presented in the security behaviour formula need to be organisation-specific. Security managers in organisations need to decide on which of the metrics defined above matter the most, based on their own security challenges, risk appetite, resources available and mitigation priorities; this should then be incorporated in their models. Security managers may also decide to remove or add elements to the equation, depending on organisation-specific requirements for risk mitigation or availability of information. Coefficients may also need to be differentiated to reflect behaviours across different organisational divisions, allowing for differentiated risk management strategies for low and high risk areas. As a result, the above formula should be seen as a basis for building a general security behaviour metric, adapted to better reflect specific organisational settings, related security challenges and risk appetite.

7.5.3 Consider impact of interventions

Security management should also use measurable information to aid system design and assess the effect of changes in security on employee primary tasks, together with subsequent behavioural responses. Modern system design methodologies call for assessment of the effort users need to expend on a system in early design stages, also recommending iterative development and deployment of technology solutions (Checkland and Poulter, 2006). Despite that, updates to security provisions are currently deployed without testing, mostly in a reactionary way or to comply with regulation and international standards (Herath and Rao, 2009a). In essence, there exists no pre- or post-deployment assessment of the impact of security mechanisms on employee productivity, with attempts for improvement only coming when security significantly disrupts productive activity. To improve on this, security managers should aim to use measurable information to predict the potential resource overheads of proposed security changes, also creating processes for continuous assessment of the post-deployment impact of those.

7.5.3.1 Pre-deployment suitability assessment

Security management needs to adopt early user testing and piloting to improve the effectiveness of security changes, turning security management into an iterative process. For example, the introduction of

a new business system that requires password authentication may seem a straightforward task, demanding minimal additional effort for employees. But the cumulative effect of adding another username-password pair to the list employees need to remember can create problems: increasing the cognitive load placed upon them further strains their capacity to both recall individual passwords (encouraging the use of recall aids like writing passwords down) and generate truly unique credentials for individual systems (making re-use of existing passwords an increasingly attractive solution). Such problems can be identified, and potentially avoided, if employee effort demands by existing security implementations are quantified using methods like the NASA TLX (Hart and Staveland, 1988). Incorporating these methods in security management and design allows for accurate estimation of the resources employees need to invest to comply with existing security, also assessing the additional workload created by a proposed new mechanism. This, or other similar approaches, can assess the potential impact of proposed interventions, ensuring that they are well-aligned with employee primary tasks, but also quantifiable and compatible with the organisation's security risk management strategies.

7.5.3.2 Post-deployment monitoring

Pre-deployment assessments can often fail to capture the full impact of a change in security: organisations are complex environments, with many people connecting from various locations, using different devices, and performing a wide variety of production tasks. This complexity can prevent accurate assessment of post-deployment impact and prediction of emerging employee behaviours. In addition, as employee resources invested for secure behaviour add up cumulatively (Section 2.6.2 - Beautement et al., 2008), a new security mechanism lead to exhaustion of employees' compliance budget. Employees can then just quietly resort to their self- or team-procured solutions, to achieve what they perceive as effective security-productivity balance, strengthening the presence of shadow security in the organisation. To alleviate this, pre-deployment impact assessments need to be combined with continuous measurement and monitoring of the impact of security on employee productive activity. As Schein (2010) notes, if the environment is undergoing increased change, it is not appropriate to base decisions in the past or in the present, and that it is necessary to think *"in terms of the near future to assess whether or not our solutions are working".* As a result, user reaction to security changes can only be accurately assessed after their deployment. This post-deployment assessment process should be done in three distinct steps:

1. Deploy a desired change, also defining a set period of time over which no other security interventions will take place, to allow isolating the effect of the intervention in question.
2. Identify the expected impact on behaviour metrics. Define what is considered as a positive and negative outcome and relate those to expected reductions or increases in metrics.
3. If indicators of shadow security change negatively, the new system may have increased the burden of the new system on productive activity, so the source of negative impact needs to be identified and addressed.

Regular assessment of the suitability of systems allows security management to become an iterative process, moving away from the current static, "fire and forget"[28] approach, enabling more dynamic and data-driven security behaviour management.

7.5.4 Benefits of measurement

The shadow security metrics presented in this chapter can improve current ability of security managers to make decisions in order to effectively mitigate organisational security risks. This is a need identified by Bartsch and Sasse (2013), who called for approaches to increase security decision-makers' expertise and awareness to support policy decisions. Using human behaviour metrics as drivers for continuous assessment and improvement can provide a number of advantages, compared to current security management approaches:

1. *Data-driven security behaviour management.* The introduction of metrics allows for easier and cheaper employee behaviour assessment and integration of the findings in security management. Collating metrics to create one or more security behaviour *super-metrics* allows for continuous organisation-wide awareness and behaviour assessment, without the need for continuous, potentially disruptive, direct engagement. This enables prioritisation of security deployments to address high risks and implementation of targeted security interventions to eliminate identified shortcomings.
2. *Reduces security management costs and makes security enforcement cheaper*. Instrumenting the infrastructure to measure shadow security could be relatively cheap compared to maintaining or rebuilding fractured security mechanisms, or managing a demoralised, fractious workforce that has developed too many non-sanctioned security habits. It also allows accurate pre- and post-deployment assessment of the impact of security mechanisms and processes on employee activities. Using measurement to deploy more user-centred security mechanisms and processes also enables cheaper and more effective enforcement, as it reduces productivity-related shadow security behaviours that can complicate attempts to identify potential violations.
3. *Behaviour metrics included in risk management*. By collating shadow-security driven metrics, organisations can identify the proportion of time employees have to spend interacting with security mechanisms. Based on organisational risk appetite, security management can then set targets of desired employee resources invested on delivering security. This allows modifying elements of the security implementation to adjust those resources, bringing security behaviour management in line with the organisation's risk management approach.
4. *Enable team-level security management*. Confining and fine-graining the proposed metrics can be used to capture team-specific behaviours and identify micro-culture development within organisational sub-groups. This allows for targeted interventions, to improve specific mechanisms or deliver targeted communication, in areas where employee behaviour is not in-line with organisational risk appetite.

[28] Military term for missiles that require no further guidance after launch

5. *Improves adaptability over time*. The existence of readily available information makes security management adaptable to external factors that influence security behaviour. Internal security breaches communicated to employees, or security breaches affecting other organisations exposed in global media, can change employee risk perceptions and behaviours in an unpredictable way. Having the aforementioned shadow security metrics in place, allows assessing the impact of such events and focusing subsequent mitigation attempts to areas where allocated resources can have maximal impact.

The above advantages suggest that shadow security-driven metrics are a powerful tool, which can improve security management attempts to better assess both current security approach performance and employee behaviour, in relation to the organisation's desired security state.

7.6 Chapter conclusion

Shadow security creates a unique opportunity to consolidate security management goals with actual employee behaviours. Instead of attempting to enforce compliance, security managers can leverage the existence of shadow security in an organisation, using it as a resource to call upon in order to adapt to turbulent times. Measuring, learning and managing it provides organisations with the ability to improve their control-oriented security approaches, using current employee security behaviours as an input to their security strategy. On the surface, control-oriented security may provide a sense of stability that negates the need to place faith in members of the organisation to do the right thing of their own volition. But where it appears to be failing is to change and adapt to what individuals experience as time goes on (as already demonstrated in public transport systems, for instance Molotch, 2013). To implement an adaptable and flexible security management strategy, security managers must be able to recognise when and where shadow security is created, its causes, and how to adapt security provisions to better align those with employee productivity needs. Learning from, and not ignoring, employees can enhance security, aligning it with organisational goals and increasing its effectiveness. If users are not heard, they can become disenfranchised and, should they have a legitimate concern about security, they will not remain passive in the face of ill-fitting solutions. Instead, they will engineer their own shadow security practices, not to evade provisioned security, but as an attempt to balance security and productivity due to the perceived lack of organisational support. The emerging user reaction to an organisation's security implementation needs to be heard, otherwise it weakens the organisation's security posture. Once identified, shadow security existence should not be treated as a problem, but as an opportunity to identify shortfalls in current security implementations that can be leveraged to provide more effective security solutions for organisations. As discussed earlier in this chapter, security managers can learn from shadow security in a number of ways: they can identify areas of security that require improvements, measure the effectiveness of security mechanisms after deployment, engage with users in the design of security solutions, and leverage the position of team managers as both mediators for security and conduits for feedback as to the appropriateness of security solutions in supporting productive tasks.

Security management should also understand that shifting more responsibility for security towards employees is ineffective. No matter how good employee intentions are, modern security challenges are getting more and more complicated, thus maintaining sufficient and accurate understanding of the variety of threats an employee may face is an unrealistic expectation. Asking employees to take action to

mitigate a large number of risks significantly increases the emerging security-related cognitive load on them. Combined with security management's failure to deliver security hygiene, the emerging incompatibility of security with employee primary tasks leads to significant friction between security and productivity. To effectively encourage employee participation in risk mitigation, security management should aim to listen to employees, understand the challenges they face and adapt security management to those, choosing solutions that are also compatible with role-related risks. This allows emerging policies and mechanisms to be context-specific, eliminating the problems with blanket security rules discussed in section 7.3, improving alignment between security and primary tasks. Attempts for improved alignment through learning may require increased resources at their early stages, but they should be seen as an investment: the more resources security management invests on aligning security implementations with employee priorities, the less the impact of the former on employees' primary task, thus the less the employee resources that will be expended on security. In addition, the emerging practices should deliver improved risk mitigation.

Effective security also needs to aim for a productive balance between trust and assurance. The findings of this work suggest that employees possess both the ability and motivation to behave securely, honouring the trust shown towards them by the organisation (*organisation-employee trust*), also aided by contextual motives to do so. But when security creates conflict with other parts of their work and their relationships with their colleagues, non-compliance becomes their only option to preserve the existing trust relationships in the social environment of the organisation (*inter-employee trust*). To reduce this conflict, security management needs to take advantage of trust and aid in its development, refraining from over-assurance once trust is developed. Employees that have been screened, trained and understand the risks of insecure behaviour, should not need to choose between organisation-employee trust and inter-employee trust when interacting with security mechanisms: both trust relationships contribute to the organisation achieving its productivity targets while remaining secure. Security design that accommodates for this can lead to the creation of a high-trust/low-assurance environment which can introduce significant economic benefits for organisations: compliance coming from employees motivated to behave securely, not forced to do so, reduces the need for expensive assurance mechanisms. As a result, as long as everyone sticks to the rules, individuals or organisations can benefit from the cost savings of a trusted environment. But when the rewards from not playing by the rules are significantly higher than the consequences of not doing so, assurance mechanisms need to exist to change the risk-reward structure, dis-incentivising untrustworthy behaviour.

The shadow-security driven metrics presented in this chapter make it possible to design and deploy more effective and efficient information security management. All the suggested measurements can be generated without imposing significant resource overheads: much of the information needed to identify the existence of shadow security behaviours is already available in various forms around various organisational systems (or relatively easy to generate and collect). A combination of the above metrics (together with additional ones organisations can implement based on their own security challenges) can provide a suite of indicators for not just the performance of technical systems, but also the performance of processes that support employee behaviours. Security managers should use the metrics and security management processes presented in this chapter to build context-specific security mechanisms that effectively address security risks, according to their organisation's risk appetite. The aforementioned

metrics and processes should be used as the basis for creating an organisation-wide, continuous learning and improvement process for security management, allowing effective and efficient deployment of new security mechanisms and improvement of existing ones. Despite that, they should not be seen as an off-the-shelf solution to manage employee security behaviour, but as useful starting points, based on the improved understanding of security behaviours that emerged from the case studies presented in this thesis. Each organisation should consider which of the metrics and processes are compatible with their security priorities, and then tailor their security management approach to match those. The emerging improvements in security-productivity alignment can reduce the overhead of security on employee primary tasks, increase the levels of employee security compliance, and lead to more effective and efficient security implementations.

Chapter 8: Case study in industry and lessons learned

As discussed in chapter 5, security non-compliance and shadow security behaviours were widely prevalent in Company B. After presenting the research findings to the organisation, the researcher was asked to join them on a full-time placement for 6 months. The purpose of the placement was to identify, propose and coordinate the delivery of improvements in Company B's security implementation, driven by the knowledge that emerged from examining the non-compliant behaviours and shadow security development in the organisation. This chapter discusses how the improved understanding of employee security behaviours that emerged from chapters 4, 5 and 6, together with the lessons learned and the emerging guidelines to improve security management presented in chapter 7, were used during the researcher's placement in Company B to: (1) drive improvements in organisational security communication, (2) identify sources of data and devise metrics to assess the effect of deployed interventions on employee behaviours, and (3) identify potential improvements the organisation should incorporate in its long-term security strategy. In the second half of this chapter the focus is shifted away from the practical application of shadow security, presenting the lessons emerging from the application of the work presented in this thesis in a corporate environment. Those lessons are then used to provide advice and principles that can be useful to both researchers and practitioners aiming to apply user-centred security research findings in organisational environments.

8.1 Placement purpose

Company B is a global telecommunications organisation with strong UK presence. The research findings from chapters 5 and 6 were presented by the research team to the organisation's Head of Security and Chief Operations Officer. They both understood the security challenges their employees faced, how those challenges lead to insecure behaviours and shadow security development, and also recognised the need to address those. They also recognised shadow security as a phenomenon from which their security management could learn and benefit. As a result, they asked the researcher to join Company B for 6 months, to help them design and deliver security improvements. The researcher would also remain in close touch with the UCL Information Security Research Group, in order to take advantage of the knowledge and potential support from the rest of the group while helping the organisation deliver the required improvements.

The researcher was positioned as an information security consultant in the Company B's information risk and security management team. The role was based in their head office, but the researcher had to interact and collaborate with various teams across the country. The researcher was responsible to review areas where non-compliance and shadow security behaviours were identified, devise a plan for the organisation to fix those, and deliver as much of those improvements as possible during the placement.

After consultation with the organisation's security leaders, it was agreed that the researcher would aim to: (1) improve understanding of shadow security development within Company B, (2) identify additional organisation-specific drivers of it, (3) identify sources of information that could be used to measure it, (4) suggest improvements of existing security mechanisms and processes, (5) align those improvements with organisational security audit requirements, (6) deliver a sample of those improvements while being employed by the organisation, and, based on the above, (7) provide guidance for delivery and

effectiveness assessment of future ones. The length of the placement prevented delivering measurable improvements for all the elements of Company B's security where problems were identified (described later in this section). As a result, the researcher together with Company B's security management decided to focus on improving employee awareness and the organisation's security culture. For the remaining areas requiring improvements, the researcher would create a report after the end of the placement, documenting suggested improvements, together with metrics to assess the effectiveness of those.

8.1.1 Understanding shadow security drivers in the organisation

As discussed in chapters 5 and 6, Company B employees possessed sufficient awareness of the sensitivity of organisational information, together with ability and motivation to behave securely in order to minimise organisational security risks. Thus, where security mechanisms supported productive activity, they responded positively by following recommended practices. In contrast, when friction-inducing security created problems in primary task completion, employee risk awareness and understanding of the need for security led to shadow security development. Shadow security and insecure behaviours also emerged from employees' inaccurate understanding of potential security risks and their lack of knowledge on the availability of appropriate organisational mechanisms or processes to mitigate security risks. This section discusses each of the above security behaviour drivers based on example behaviours in Company B, as identified in the grounded theory analysis.

8.1.1.1 Good architectural means leading to secure behaviours

As discussed in Chapter 5, architectural means that supported employee activities towards primary task completion acted as drivers for secure behaviour. Examples of these in Company B were identified and presented to security managers as examples of how "good security" can encourage secure behaviour and positive culture development within the organisation. For example:

1. Lockable drawers, hot-desking and clear desk checks acted as drivers for clear desk compliance. Employees who had no lockable drawers or had permanently assigned desks, reported lower levels of compliance.
2. The presence of a reliable organisational VPN connection, allowing uninterrupted access to all organisational systems, minimised employee need to store information locally on laptops in case organisational access was not possible when working from home.
3. Responsive helpdesk and easy access control setup reduced the need to share credentials where system access is required.

8.1.1.2 Compliance expensive or impossible

When architectural elements of the security implementation created high compliance overheads or made compliance impossible, employees resorted to insecure behaviours or shadow security practices.

1. Lack of availability or problems in connectivity to the organisational network (e.g. due to lack of internet connection on a train or at a client site) led to employees requiring access to specific files storing those locally on their machines.
2. The allocated network storage space each individual had was severely limited. As a result, employees relied on local laptop storage for their past and currently-working documents. The

lack of official backup mechanisms for locally stored information, also led to teams and individuals devising their own ad-hoc backup strategies using self-procured drives. Those were either encrypted and unencrypted and, in some cases, even kept at employees' homes when they worked from there.

3. Slowdown caused by lack of easy to use organisational file-sharing systems led to employees sharing files through multiple other organisational or third-party channels. Decisions on file-sharing practices were ad-hoc, both at individual and team level, with employees mostly sharing information through emails instead of SharePoint or shared drives. In addition, where collaborative sharing was required, the use of third-party cloud storage services was also identified (e.g. Dropbox).
4. Problems with company-provided encrypted USB drives led to employees using unencrypted ones. Storage capacity of encrypted drives was insufficient for employee needs, due to the large size of diagrams and other information employees often had to store. In addition, employees also reported problems in the procurement of those (not everyone had one), creating a need to find alternative solutions.
5. The lack of lockable space for storing paper documents, combined with the need to comply with clear desk policy, lead to employees often having to carry sensitive documents at home in their laptop bags.
6. Inconsistent email filtering and website blocking often prevented access to websites and blogs useful for work-related information. This led to employees sometimes having to use personal accounts, or access the required information using their own personal machines, transferring it to their corporate ones later, thus bypassing organisational information filtering systems.
7. Corporate password management software did not work for all systems employees had to use. The problem created by employees having to manage multiple passwords for various systems, was accentuated by different password change rules across different systems (e.g. different expiration periods and different password length and structure requirements). In addition, an organisational password storage software, where employees could store their passwords securely instead of writing those down, was not installed by default on employee laptops and many were unaware of its existence. As a result, writing down passwords was a common practice around the organisation, both in paper form (e.g. employee notebooks) and within digital documents.
8. Employees reported that access revoking for leavers appeared to take long or never happened. Despite the security policy requiring quick account de-activation, accounts of people that had left the organisation appeared to remain active for some time after their departure. This led to a perceived inability of account managers to effectively manage access to information, further encouraging employees to devise their own solutions to resolve access problems.
9. Security and compliance across the company appeared to be measured using CBT completion rates. But employees reported that they have to go through too many CBTs on various organisational topics, with communicated information often perceived as common sense. Having to take the majority of those CBTs at the same time increased the cognitive load placed upon them, with employees treating those as compulsory "tickboxing" exercises, not as something they could benefit from. In the end, the information communicated through CBTs

was often ignored, with employee security behaviour being based on practices they themselves considered fit-for-purpose.

In all the above cases, the security mechanisms or processes in place created either disruption in primary task completion ability, significant time burden, or increased the cognitive load required for secure behaviour. When employees considered the disruption or the effort required as unmanageable, they resorted to self-devised security practices.

8.1.1.3 Lack of knowledge and awareness

The second major category of shadow security drivers related to the inaccurate security risk awareness amongst employees and the inadequate understanding of organisational risk mitigation mechanisms and processes. Employees were aware of the importance of the information they deal with, potential security breaches and their impact to the organisation, thus recognising the benefit of security. But the lack of accurate risk understanding and knowledge on behaviours required to keep the organisation secure (or related available mechanisms) also lead to insecure behaviours and shadow security development. A few examples:

1. The presence of encryption on employee computers left them feeling assured that storing information locally on their laptops is a secure practice. No one appeared to acknowledge that hard drive encryption is vulnerable to a wide range of attacks if someone gets physical access to their laptop (e.g. cold boot attacks – Halderman et al., 2009).
2. Storing files locally was also a result of lack of awareness among some employees of the existence of personal network drives.
3. Perception of some organisational information as non-sensitive led to information being taken home on paper or other devices, or left around the office, later picked up by clear desk inspections (which "don't happen often" in some locations, as employees said). When asked to discuss potential risks from this behaviour, some employees downplayed the sensitivity of the information they deal with, also referring to data without classification markings as generically non-sensitive

Examining the drivers behind the awareness problems, employees referred to central security communication and training mechanisms as irrelevant, generic, inconsistent and overloaded, also reporting to not always reading it. Security communication is mostly done at team meetings by line managers and their colleagues, but both managers and employees reported that they do not know the complete in's and out's of policies. As a result, they often have to apply their own role-specific content filtering, with managers communicating what they consider as the most critical knowledge for their teams. In addition, the training content was referred to as common sense. Marking documents using organisational classification guidelines for example, appeared to confuse employees, with the majority reporting not using those. The risks from the development of such behaviours and their impact on organisational culture are extensively discussed in section 5.3.2: security management loses control and understanding of employee security behaviours, employee resources available to security are significantly reduced, and alienation between security and the organisation's productive divisions also emerges.

8.1.2 Identifying potential improvements

The next part of the process involved devising a plan for delivery of security improvements, driven by the security-productivity alignment guidelines presented in sections 7.2 and 7.3. Using those, a number of suggestions emerged for the organisation:

1. *Simplify communication.* The organisation had to reduce the need for employees to filter though policy content. Managers should be properly informed about security risks, assess those and decide which communication clauses apply to their teams. They should then communicate appropriate risk mitigation practices at team meetings.
2. *Make CBTs role-specific and spread those throughout the year.* CBTs needed to better reflect context-specific challenges employees in different organisational divisions face. For example not all employees need to use all data classification levels, but CBT content on data classification is generic for everyone. In addition CBTs on different topics should be evenly spread throughout a calendar year, to ensure employees do not have to do all their CBTs at the same time, thus reducing the potential for those to become a tickboxing exercise.
3. *Provide secure physical document storage.* Employees need to have access to secure physical storage for any paper-based information they need to use. This will reduce both the number of documents left around by non-hot-desking employees and the need for those who hot desk to take sensitive information with them when they have nowhere to store it.
4. *Provide password manager support.* Centrally procured official password managers should be fully compatible with all corporate systems in order to reduce the need for employees to write their passwords down, physically or electronically.
5. *Deploy centralised corporate file sharing with automatic backups*. Easy to setup and use information sharing mechanisms need to be put in place to avoid employee use of other information storage and sharing mechanisms like emails, or the use external cloud storage providers. After deploying such mechanisms, security management also needs to communicate the presence of the new functionality back to employees, its improved usability, and the importance of using it to participate in organisational protection.
6. *Mandatory USB encryption.* Removable USB storage should automatically be encrypted by appropriate software on company computers. If this is not possible, the organisation should provide encrypted USB drives of sufficient capacity to all its employees, also communicating the need to use company-approved approaches to store, backup and share company information.
7. *Improve leaver process.* Line Managers should ensure leaving procedures are completed in a timely manner, in collaboration with HR. In addition, an automatic alert system should be in place to detect instances of people leaving the organisation that have not had their access removed automatically.
8. *Encourage reporting.* Employee willingness to report security concerns and seek support when in doubt should be encouraged by the organisation through security communication. Reporting and support should be done through line managers, who should then communicate that information to security management directly, or through easy to use reporting mechanisms. In both cases sufficient follow-up mechanisms need to be in place, for employees to be informed on security management actions driven by their reports.

The above improvements are presented in more detail in Appendix L, together with relevant metrics to assess the effectiveness of their implementation. Unfortunately delivering all those in the 4 months the researcher had left in the organisation was not practically feasible. As a result, the head of security asked the researcher to focus on improving organisational security communication practices, and then use the lessons learned to provide guidance on the delivery of the required improvements in other areas of the security implementation. The remainder of this chapter presents the steps taken to achieve so, the problems encountered, and the lessons learned for both industry and research.

8.2 Delivering security communication improvements

In order to deliver the required communication improvements, the researcher started by (1) examining existing security communication and identifying its drawbacks, and then (2) devise a set of requirements for improved communication by liaising with various stakeholders around the organisation. Based on those, the (3) desired communication content was identified and agreed with the information security team, together with (4) indicators that should be used to measure improvements. After completing the above, the researcher was asked to liaise with the information security team member responsible for security awareness, and deliver required improvement in collaboration with corporate communications. This section describes the researcher's actions in order to deliver those improvements, together with problems in the organisational environment that prevented successful deployment of those during the researcher's placement within Company B.

8.2.1 Identify problems with existing communication

The first step towards delivering effective communication was to identify problems with the existing organisational security communications approach. Examining the communications plan that has been delivered during the previous year (Appendix K), three areas requiring improvements were identified:

1. *Communication redundancy due to various audit requirements*: Company B had to comply with a number of different security standards (e.g. ISO27001, PCI-DSS and various sector-specific others). In many cases, responsibility for passing related audits relied on different stakeholders (e.g. different members of Information security team, IT security, Physical security, or corporate communications). In order to fulfil the requirements for those audits, the person or team responsible for each one sent out security communication material, with minimal central coordination of the content and the timing of those communications. This confirmed employee reports (presented in chapter 5) that security communication creates unmanageable information overload for them, consequently failing to improve their understanding of organisational risks and appropriate behaviours to mitigate those.
2. *Generic, not role-specific communication*: All employees in Company B received the same security communication through the same media (emails). This observation also relates back to the findings of chapter 5 where employees referred to security communication as generic and unrelated to their role-specific security challenges.
3. *No effectiveness assessment*: The involvement of security management in delivering the content included in the communications plan ended when the content went out. No mechanisms existed to assess the impact of the communicated risks, principles and desired behaviours on employee

actions. The only way security management attempted to assess employee security compliance was by recording the rate of completion of CBT-based training modules, which, as discussed earlier in this thesis, had minimal influence on employee behaviour.

In general, communication was not centrally planned, with different stakeholders sending out different information to employees. In addition, the content sent to employees was generic, and the organisation had no mechanisms to identify the influence of communications on employee security behaviours.

8.2.2 Requirements for improving communication

Based on the identified problems (generic and redundant communication without adequate effectiveness assessment), two main areas for improvements were identified in order to deliver more effective and efficient security communication: (1) unify awareness requirements of the various security-related audits and emerging communication, in order to reduce employee overload, and (2) target communication to address current employee behaviours, identify where differentiation of communication for different employee roles was required, and use post-deployment measurements to assess the effect of it. This section presents the steps taken in the organisation to deliver the above improvements.

8.2.2.1 Unify different awareness requirements

In order to reduce the amount of security communication sent to employees, it was important to unify the security awareness requirements for the various information security-related standards the organisation was audited for, and create a communications plan that would satisfy them all. The researcher examined the standards in question (e.g. ISO 27001, SOX, PCI-DSS), discussed compliance requirements with the owners of various security audits, also taking into account awareness requirements emerging from the organisation's plan to deliver the CESG 10 steps to Cyber Security (CESG, 2015) at the same time the researcher was there. This led to the emergence of a communications plan that addressed the goals and priorities of all the stakeholders involved in security communication, satisfied awareness requirements from all the relevant standards, and reduced redundancy in security communication.

To ensure centrally-coordinated delivery of the new communications plan and consistency with other corporate communication, the member of the security team responsible for communication would liaise with the organisation's central communications team. The communications team would then be responsible to deliver the finalised content to employees. It was then agreed that no security-related information would be sent to the communications office for distribution to employees, unless it came from the aforementioned security team member.

8.2.2.2 Identified target behaviours, desired metrics and hygiene requirements

Based on the research findings, six areas where organisational communication had to be improved or deployed emerged. For each area, sources of measurable information were identified, that would allow the organisation to quantitatively assess the effectiveness of the delivered changes. In addition, security hygiene requirements were identified and recorded as prerequisites for employees to follow the communicated practices (Table 9). To ensure compatibility of the above principles with Company B's corporate security strategy, the researcher presented those to the Security Council. They were positively

received and commended as a significant improvement over existing practices (the final communication plan can be found in Appendix K).

Target behaviours	Current state	Ideal state	Hygiene requirements	Metrics	Information exists - Yes/No?
Privacy markings	Employees aware what they are – not know how to use those Leads to over-classification	Information held or processed has value assessed by author or business owner - corresponding privacy marking assigned	Easy availability of marking instructions Clear explanation of how to assess sensitivity of corporate documents Not all people use all levels – target communication content based on this	Markings on documents left around - site security to provide this information Number of correctly/incorrectly marked documents	Yes, through clear desk inspections logs – need to update logs kept to include classification
Information handling and protection	Employees downplay information importance	Employees understand importance of information they handle	Requires effective communication and training	Volume of traffic to cloud providers Volume of email traffic Usage of internal file storage and sharing systems DLP data: number of sensitive information sharing attempts	Yes, but need to create/deploy mechanisms to capture those
	Data sharing ad-hoc – using external cloud services, emails	Centralised corporate file sharing, no cloud services used	Shared drives managed at group level – allow easy sharing of information		
	No centralised backup / data transfer strategy	Centralised backup – no ad-hoc backups	Network drives are sufficiently large and backed up		
	Unencrypted own USB drives used	Encrypted USB drives are used	Centrally provided USB sticks or mandatory encryption of USB devices	Encrypted vs unencrypted USB use statistics	
	Clear Desk: documents left around	No documents left around	Lockable drawers for all employees	Number of documents left around	Yes, through clear desk logs
Password behaviour	Writing down passwords prevalent practice	Employees download and use password storage tool Passwords never need to be written down	Working password manager – no compatibility problems Password manager and password storage tool integrated	Password tool usage statistics	Yes, adoption and usage statistics of password management software
Access control	Slow leaver process Accounts remain active after departure	Line Managers report departures promptly Access revoking for leavers done automatically through HR	HR leaver process linked with account deactivation	List of unused accounts HR leavers – time to deactivation list	No, but possible to do by connecting HR with accounts
Virus and malware	Use of personal USB drives	No personal USB drives used	Provide corporate USB sticks to everyone Finely-tuned virus scanning at organisational email servers	Reduction in own USB use Infected machines detected on the network?	Yes, but need to create/deploy mechanisms to capture those
	Downloading information from own email accounts	Malicious emails blocked			
Reporting security incidents	Employees do not see response to reports Little or no employee willingness to report	All problems are reported, directly or through line managers Followed up, feedback back to employees	Easy to use reporting mechanisms Reported false positives for email and website blocking addressed Rapid response to response Effect of reporting communicated	Helpdesk requests and aggregate reports Manager reports and of employee concerns Number of false positives reported Percentage of "feedback given" incidents	Yes, but need to create/deploy mechanisms to capture those

Table 9: Target behaviours with metrics, hygiene requirements and related metrics

Despite their usefulness in capturing various different elements of employee behaviours, even full deployment of the above security hygiene principles, communication and metrics in an organisation cannot accurately capture the full picture of employee security behaviours. For example, the volume of traffic to cloud storage websites may be an indicator of their use for corporate file sharing, but can also be a result of personal employee use of the corporate network. Despite this, the purpose of the proposed metrics is to identify indicators that can be combined to demonstrate potential effectiveness of improved security communication on employee behaviour. In addition, hygiene requirements are used to demonstrate the need to remove friction-inducing security, underlining the importance of security hygiene as a pre-requisite to any attempt to influence employee behaviours. The metrics and hygiene requirements constitute a significant improvement over the current organisational inability to quantify and measure security behaviours and evaluate the effectiveness of organisational security communication.

8.2.3 Problems in delivery

Despite initial adoption of the communication improvements plan by organisational security management, attempts to deliver the improvements presented in section 8.2.2 faced a number of challenges, caused by insufficient and slow access to organisational resources and information, problems in achieving security hygiene requirements, and unexpected changes in organisational strategy. This section discusses how various elements of the organisational environment created obstacles in delivering the updated security communication plan in the available timeframe, and how they negatively affected the researcher's ability to deploy changes in a controlled environment and assess their impact.

8.2.3.1 Resourcing problems and unavailability of information

Despite having board-level approval, access to key people and information required to deliver improvements and deploy corresponding metrics proved to be difficult for the researcher, even while situated inside the organisation. Engagement with key people in the organisation was necessary to provide information required for metrics to assess the effectiveness of security communication. People responsible for network monitoring for example, were asked to provide data on traffic towards third-party cloud storage servers. Helpdesk managers were asked to share the number of calls they received per month. Physical security was asked to keep logs of the number of documents found around every day, also noting their classification. In addition, account security was asked to provide information on the time it takes to revoke leaver accounts, and the number of unused accounts that are still active in the organisation. Unfortunately many of the employees acting as contact points in those divisions often reported to be busy with their day-to-day tasks. Without any formal responsibility to provide the required information or instructions to cooperate by their managers, engagement with this project became a low priority task for them. For example, information on network and account usage was held by different organisational divisions, outside of central security management, making access to it challenging to achieve. Even physically visiting information owners in various locations around the country did not provide access to the required information. In most cases there was a visible reluctance of individuals to share that information. This could be attributed to attempts to avoid the effort required to collect and provide the information, but also avoidance of the potential for the information provided to reveal problems in the security implementation, for which some of the information holders could be held

accountable. In the end, the only division that provided the requested data was the IT support helpdesk on the number of calls received and reporting on information security issues.

8.2.3.2 Lack of security hygiene

A number of security hygiene elements identified as prerequisites for secure employee behaviour were not present in the organisation. For example, asking employees not to store information on personal drives made no sense, due to the absence of a centrally backed-up solution that also satisfied employee primary task requirements. Increasing employee personal network storage space (a hygiene requirement for this behaviour), could not be delivered due to the lack of available storage on company servers; any attempts to increase server capacity had to go through a formal approval process, subject to available funds in the coming financial year. This meant that delivering communication asking employees not to use personal drives to backup information would be ineffective, due to the lack of a viable alternative solution. In general, attempts to remove friction-inducing security elements always stumbled on the lack of budget or available planning. The subsequent failure to deliver many of the hygiene requirements of section 8.2.2 by the organisation, reduced the potential effectiveness of the improved security communications plan.

8.2.3.3 Personnel changes disrupting delivery

Delivering security communication was made harder when the person responsible for creating the content and coordinating communication delivery was sent on an international placement. This happened two months into the researcher's 6-month placement, after identifying and agreeing on target improvements, courses of action and delivery dates. Having to recruit another person for the role took an additional two months, which meant the communication plan could not be delivered in its entirety in the remaining 2-month period. Despite that, an opportunity to deliver some tangible improvements appeared when the organisation decided to deploy an encrypted USB and DLP system. It was agreed for the researcher to focus on the communication required to be delivered with it, also measuring potential changes in employee behaviour after communication delivery (through the metrics on encrypted USB and DLP use presented in Table 7).

8.2.3.4 Changes and delays in agreed deployment of systems

The initial plan for encrypted USB and DLP deployment, required piloting and initial measurements to be completed before the end of the researcher's placement, but once again, significant delays prevented this. Despite full deployment of the system being set to start after the end of the placement, it initially appeared to be possible to get access to software generated logs on user behaviour, through an early pilot scheduled to start earlier. Unfortunately, the implementation was also pushed back a number of times, due to contractual problems between the software provider and the company's 3rd party internal IT provider. In addition, after helping the organisation design the pilot, the researcher was informed that the organisation had inadequate storage space to store required logs generated by the encrypted USB and DLP systems, which made assessing the impact of any communication related to user information storage and sharing habits impossible. The above problems created significant challenges in delivering an end-to-end project within the short time the researcher was present in the organisation, with controlled end-to-end interventions and measurement becoming impossible.

8.2.3.5 Outsourcing complicating data access

A large part of IT was externally managed (outsourced) with service providers having no obligation to provide the information required for this project. In addition, half-way through the placement, a large part of Company B's operations was outsourced, with most employees only finding out on the day it was officially announced. The short timescale of the researcher's placement made it impossible for information security to re-negotiate the outsourcing contract terms to include the sharing of information required for measuring effectiveness of the security improvements (e.g. access to virus logs on company computers managed by a service provider).

8.2.3.6 Post-placement collaboration

After the end of the placement, the researcher produced a list of improvements required for the organisation to improve its security posture and use shadow security to improve security-productivity alignment. The suggested improvements were discussed with the head of security who acknowledged those as useful for the organisation. They then assigned a member of the information security team as the main contact between the university and Company B, to ensure collaboration would continue and deliver those improvements. Despite continuous communication between the researcher and Company B, improvements could not be implemented due to the same problems identified while the researcher was on site (lack of budget for security hygiene and lack of access to measureable information). In addition, the person responsible for delivery of the changes was not very responsive to queries from the researcher, as delivering the improvements was not their primary job.

8.2.4 Placement review

Despite the failures in delivering desired improvements, attempting to apply the findings of this thesis internally within an organisation provided a number of valuable outcomes:

1. Shadow security metrics were directly related to information readily available, or easily obtainable in the organisation examined. This suggests that security managers interested in applying the findings have significant amounts of the information required to measure it if effective collaboration with information owners can be achieved.
2. The metrics-based approach outlined in chapter 7 was used to create an organisational security communications plan, which was presented to the organisation's Security Council. It was positively received as a novel approach to measure and manage employee security behaviours, which is currently a significant challenge in modern organisational security management.
3. Based on the improved understanding of organisational systems and processes gained through the placement, at the end of the six-month period, a report was created that included the identified drivers behind shadow security evolution, security hygiene problems with suggestions for improvements, and metrics that could be used to assess the effectiveness of attempted changes (Appendix L). The organisation agreed to use this approach in the future and communicate the results back to the researchers, but unfortunately they have not done so to date.

Despite the organisation agreeing to deploy the new security communication plan and allow the researcher to access related information to assess its effectiveness, after the end of the 6-month placement security communication reverted back to their old "fire and forget" approach. Upcoming audits require

security communication to be delivered within short periods of time and, without planning for metrics deployment, various audit owners reverted back to their old approach of just sending the information to employees directly. In addition, despite the researcher providing support and advice to the organisation for a significant period of time after the end of the placement, the slow improvements delivery meant that the researcher had to stop after some time, as this research had to be completed within the timeframes of a PhD project. There was also a lack of response from the new employee responsible for organisational content delivery after the end of the placement, which made access to information required for research purposes even harder. In the end, despite some preliminary momentum built by security management and their support for delivering shadow security inspired improvements, the organisation never managed to deliver the hygiene requirements and metrics required to put those improvements to practice.

8.3 Lessons learned for research

This case study presented a unique opportunity to apply security research findings in a corporate environment. Despite the problems in delivering and measuring the required improvements within the available timeframe, the experience and the lessons learned are useful for any security researcher attempting to deliver improvements in a commercial environment. The emerging lessons can be grouped in four main areas: (1) interventions and changes in organisations can take significantly longer than academic experiments, (2) inclusion of desired changes in corporate governance and strategy is key to their successful deployment, (3) security hygiene is expensive and slow to achieve, and (4) lack of complete control of the organisational environment makes many interventions difficult. This section discusses the lessons learned from the researcher's placement in Company B, providing advice and guidance to researchers who want to apply their findings to deliver security improvements in organisations.

8.3.1 Interventions take time and require good planning

Research-driven interventions in organisational environments can take a significant amount of time and need to be part of corporate security strategy to be effectively deployed. Changes need to be outlined as medium-to-long term projects, included in corporate security strategy, and accompanied by detailed planning by the organisation to enable successful delivery. In addition, related stakeholders should be identified before commencing intervention attempts and provided with a clear description of the role they play in recommended changes, together with their emerging responsibilities. In addition, resources required for intervention delivery need to be allocated as part of annual budgets, with people who need to engage and aid delivery having this included in their job descriptions and annual performance targets. If this does not happen, delivering changes can become a secondary priority for them; in a modern organisation, where employees have to meet tight deadlines, interventions will inevitably run the risk of not being delivered. In general, any attempt to apply research in practice and deliver changes in corporate security needs to be part of an organisation's security strategy, to ensure availability of required time and resources.

8.3.2 Need for corporate governance adoption

Research in organisations cannot deliver effective changes, unless organisational leadership understands the importance of required interventions and is willing to provide adequate support and resources for their

deployment. In a corporate environment with low profit margins, high competitiveness and tight deadlines, delivering security improvements often runs the risk of becoming a second-rate requirement. Security is considered important in principle, but in practice productivity prevails. While this is acceptable for a profit-driven organisation, ignoring security can often lead to damages in ability to proceed with productive activities: security incidents are on the rise year on year and their impact can bring an organisation's productive activities to a halt (CEBR, 2015). As a result, security improvement attempts should be a concern for everyone in corporate governance: security is a collective achievement and effective improvements require engagement of a number of different stakeholders across organisational divisions to work. Before commencing attempts for research-driven improvements, a researcher needs to ensure corporate governance is content with required changes, understands the benefits for the organisation, and is willing to allocate the resources required for successful delivery.

8.3.3 Align delivery targets with regulatory requirements

It is important for researchers to align the end-result of research-driven improvements with the various regulations and industry standards that organisations have to comply with. Frequent audits against a wide range of information security standards and regulation (see section 8.2.2.1) create pressure for the stakeholders responsible for those to perform required risk mitigation actions (e.g. communicate at least some security principles to employees to "tick the box" and meet the audit requirements for actions taken to improve user awareness). This requires careful planning of research-driven interventions, considering the requirements of organisational audits, thus ensuring emerging actions and related metrics provide sufficient evidence for the organisation to satisfy audit requirements. This can introduce long term benefits for audit owners: a centrally-coordinated security improvements program, combined with good security metrics can provide readily-available information on the effectiveness of various security controls, reducing the need for manual evidence collection to pass their annual or bi-annual audits.

8.3.4 Lack of total control and the need for adaptability

An organisational environment undergoes changes constantly (e.g. during the researcher's engagement in Company B, outsourcing of an important organisational division took place, with people even high above in the organisation not knowing about it until the day it was publically announced). Constant changes prevent researchers from conducting controlled experiments (to statistically test hypotheses), as control over other external factors that can affect employee security behaviours is often impossible (for example a high-profile breach at a competitor that received media attention may act as a motivator for secure behaviour for employees). In order to reduce the effects of this unpredictability, researchers need to:

1. *Be adaptable and willing to change*. Sometimes experiments may need to be postponed until after significant organisational changes have been completed. If projects are planned over periods longer than the one described in this chapter (i.e. 6 months), it may be possible to plan proposed interventions and measurements to adapt to future changes in the organisational environment.
2. *Aim for learning when control is impossible*. Where controlled experiments are not possible security research should aim to learn from access to organisations, using it as opportunity to apply and refine emerging theories and devise hypotheses to be tested in the future.

3. *Divide work to be done to smaller independent sub-tasks.* Breaking down research in smaller sub-tasks that can be independently investigated reduces the complexity of having to manage a potentially volatile organisation-wide project. Instead, it allows focusing on a sample of improvements that can be delivered in shorter timeframes. Presenting security hygiene requirements to an organisation for example, should be done by understanding that some of those may never be fully achieved due to budget constraints. As a result, it would be unrealistic for a research project to assume all proposed hygiene requirements will be adopted by an organisation. Instead the project should focus on the simpler ones and attempt to deliver those to demonstrate the benefits of using a science-based approach in information security management.

In general, researchers need to understand that modern organisations are constantly evolving in order to remain competitive and maintain their ability to innovate. As a result, researchers should be willing to adapt to changing conditions and be flexible and willing to learn through exploration if controlled experiments cannot be conducted.

8.4 Lessons learned for industry

The lessons learned from this case study also provide valuable insights for organisations who seek to improve the effectiveness of their information security approaches. Attempts to deliver such improvements require a number of different steps: (1) understanding the importance of security hygiene in delivering security behaviour changes, (2) formalisation of individual employee contributions in security, (3) promotion of a learning-oriented security management approach, (4) understanding of the benefits of measurement in effective security management, (5) improvement of existing information security standards and regulation, (6) reframing security improvements as investments that improve organisational long-term viability, and also (7) encouragement of further collaboration between government, academia and industry to provide more scientifically driven security management. This section discusses each of the above steps, outlining what organisations need to do to effectively achieve those.

8.4.1 Hygiene is an (expensive) necessity

As discussed extensively in chapters 7 and 8, the presence of security hygiene is a vital requirement for any attempt to deliver security behaviour improvements. Unfortunately hygiene sometimes comes at a high cost, requiring significant changes in an organisation's security mechanisms and processes to make compliance easy for employees (e.g. providing additional network storage for employees to store information). In addition, again for cost-saving reasons, third-party security solutions are often deployed that lack adequate customisation to fit organisation-specific needs (for example the password manager that failed to work with a number of organisational systems). In those cases security hygiene needs to be looking for the "least-bad" solution: security management should test pilot deployments of as many alternatives as possible, and deploy the solution that creates minimal disruption to employee productive activities.

8.4.2 Formalise everyone's security contribution

Security responsibilities need to be included in employees' job descriptions. Blanket security policies, threatening sanctions for non-compliance have minimal impact on employee behaviours, especially when non-compliance is widespread and has become part of corporate security culture (or local micro-cultures within organisational subdivisions). The findings of this thesis have shown that employees understand the need for security and are willing to take actions to protect an organisation, as long as they understand related risks and what actions they are expected to take. Those actions should be context-specific, based on employee roles and tasks, and also better communicated, through their line managers that are best placed to communicate context-specific security advice.

8.4.3 Promote a learning-driven security culture

Organisations should aim to listen to their employees and incorporate their feedback in managing security. As discussed in section 7.3.3, line managers have considerable influence on employee behaviours, thus part of their responsibilities should be to encourage employees to communicate problems they encounter in security implementations. That information should then be communicated back to security managers, in order improve their understanding of the impact of the security implementation on employee primary tasks, and re-design security to reduce security-productivity friction. Employee reporting should be complemented with continuous feedback back to employees, presenting the impact of their reports on organisational security management. This can lead to the development of a more collaborative security culture, improving alignment of security with organisational goals, thus also improving its effectiveness.

8.4.4 Metrics are vital for security management

Deploying security metrics can improve the effectiveness of information security management compared to current "fire and forget" approaches. Despite the potential benefits of metrics deployment, their use in Company B was limited. The existing audit-driven security culture encouraged deploying the minimum security controls required to satisfy audit requirements, with minimal assessment of their effectiveness. This turned the company's security management process to a tickboxing exercise, without a systematic way to assess its effectiveness, other than the lack of severe security incidents. This can be changed by capturing snapshots of various security-related information sources (see sections 7.5.2, 8.2.2), through which an organisation can measurably assess the effect of attempted improvements in its security implementation. In order to do so, appropriate channels need to be created for security management to have direct and uninterrupted access to that information, which can be then automatically included into deployed security metrics (e.g. access to network storage usage by employees). Automation is a key requirement for such an approach, as the volume of information generated by various organisational systems can be unmanageable on a day-to-day basis. Minimal disruption to both information owners (e.g. network administrators) and security managers should also be a key requirement for such a measurement approach. The end result should be a list of readily available metrics, which can enable more informed decision making, both for high-level security strategy, and day-to-day security management.

8.4.5 Need for more effective standardisation

Today a number of security standards exist with which organisations need to demonstrate compliance. The ISO27000 series of standards for example, is used to cover many aspects of information security management (deployment of information security management systems and related controls, security risk management, security metrics deployment etc.). Industry-specific standards also exist (e.g. PCI-DSS required for organisations accepting card payments on their retail operations), with various governments often also providing additional security good practice guidelines (e.g. UK CESG 10 steps to Cyber Security). Unfortunately in the organisation studied, effective deployment of those standards was prevented by two main factors: (1) lack of security hygiene consideration in the standards the organisation had (or had chosen to) apply, and (2) extensive cross-standards content redundancy. This section discusses what actions organisations that create the above standards need to take to eliminate the aforementioned problems.

8.4.5.1 Include security hygiene in standards and good practice

Despite all modern information security standards including user education and awareness as a key element of an effective security implementation, the need for security hygiene as a prerequisite of secure behaviours is not part of the standards' content and recommended controls. This often leads to the deployment of systems that fail to effectively support employee primary task activities (e.g. slow or problematic corporate file sharing provisions), with employees inevitably deploying their own, more appropriate shadow security solutions. To avoid this, it is important to assess the usability of security controls included in standards in addition to their effectiveness. Security managers need to understand that secure behaviour principles, presented to employees through communication and training, cannot be followed if related mechanisms or processes they need to interact with are either friction-inducing or even completely absent.

8.4.5.2 Eliminate redundancy

Redundancy elimination from various standards organisations need to comply with is also key to a more effective security implementation. If an organisation has already been through an audit of a standard that includes a number of clauses on user awareness, why would they need to go through the same process again for another standards with similar clauses? The overheads created from this redundancy consume valuable resources, with the owners of various audits often having to collect similar information more than once during each audit period. Information security standardisation bodies need to collaborate to remove this redundancy, by allowing cross-referencing between clauses in standards and providing exemptions from required evidence, if audits of other standards with similar clauses have already taken place. This requires various standardisation bodies agreeing on acceptable timeframes between different audits, potentially including other parameters like depth of coverage and authority that conducted the audit.

8.4.6 Security improvements are long-term investments

Effective security does not come cheap: significant time, effort and organisational resources need to be invested into achieving effective risk reduction and deployment of appropriate measurements. As recent industry data demonstrate, current organisational approaches to security do not manage to keep

organisations secure: the number of security breaches continues to increase year on year with their impact becoming more and more expensive (PwC, 2015). Organisations need to accept that investments in improving security are the only way to fortify themselves from potentially catastrophic future attacks. Investing towards metric development, mechanism improvements to improve security hygiene, and improvements in employee security behaviours, may demand significant initial costs, but long term benefits can outweigh those costs: reduced exposure to breaches reduces organisational costs of breach recovery, also saving employee resources (both time and effort) consumed by the presence of friction-inducing security mechanisms. As a result, the high fixed cost of implementing a metrics-driven security management approach, which also has security hygiene at the centre of it, should be seen as a long-term investment to deliver effective security protection.

8.4.7 Government – Academia – Industry relationships

As mentioned earlier in this thesis, the research conducted was part of a larger project, *Productive Security*, funded by UK Government research grants. The continuous engagement of an academic research group (ISRG) with both industry partners and government departments allowed better understanding of the existing relationships between the three (academia, government and industry), also identifying potential areas for improvement. This section outlines the lessons learned from this interaction, using those to suggest improvements in future collaboration between academia, government and industry, in order to create more effective security solutions.

8.4.7.1 Improving existing Academia-Government-Industry relationships

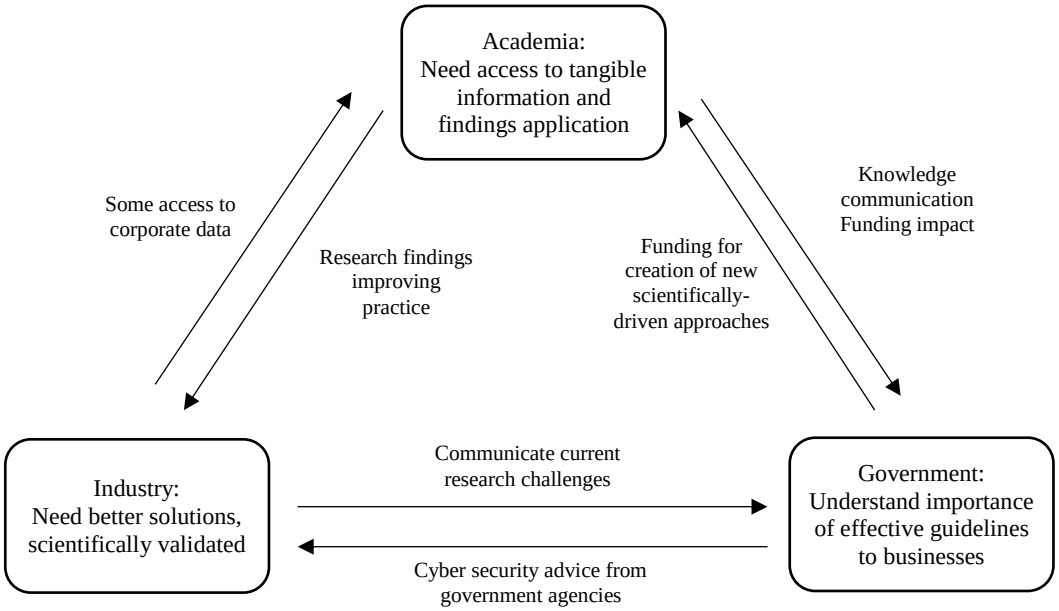

Figure 19: Existing Academia, Government and Industry security challenges and relationships

Currently academia, industry and the government interact through three two-way relationships that face a number of challenges (Figure 19):

1. *Government-Industry*: UK enterprises value advice coming from government sections on cyber security (e.g. CESG 10 steps to cyber security). Panels also exist for government to listen to the

challenges industry faces and provide advice to them. But, unfortunately current threat of potential sanctions driven by existing legislation makes it hard for organisations to report security breaches or near misses, as those sanctions often come with prohibitively high costs (e.g. fines - European Commission, 2015).

2. *Academia-Government*: The government is still the main source of funding for academic research, with emerging knowledge being communicated back to the funding providers in the form of academic publications. Government funding usually comes with some impact requirements, but facilitation to deploy the findings outside academia is currently minimal. Academic institutions are currently required to build their own relationships with potential industry partners interested in deploying their findings and then report potential impact back to the funding providers.
3. *Industry-Academia*: Academic researchers often build relationships with collaborators in industry, but access to and use of corporate data in academic research is currently minimal. In addition, academia rarely gets to influence corporate security strategy and decision making, for reasons similar to those outlined in section 8.2.3. There is some use of academic research findings by industry, but this does not happen often. Research-driven security improvements rarely get to be included in long-term corporate security planning. This prevents the authors from investigating the effectiveness of their research findings in practice, also reducing the potential for improving those. In addition, instead of engaging with academia, organisations nowadays mostly rely on external consultants to provide security advice. This advice is often based on best-practice industry principles rather than scientific ones, often failing to effectively manage organisational security challenges.

As the above suggest, currently there is a disconnection between government, industry and academic research. The existing two-way relationships need to be replaced by a centrally-coordinated three-way collaboration. The government can act as a facilitator in the industry-academia relationships, encouraging and leading collaborative projects that can benefit all three sides: (1) universities will secure access to high quality industry data, allowing (2) formulation of better security advice for organisations based on scientific principles, thus resulting to (3) higher impact emerging from government-funded information security research.

8.4.7.2 The importance of collaboration to deliver better security

The complex and ever changing nature of modern information security breaches makes it almost impossible for organisations to achieve effective security protection in isolation. Collaboration between organisations and communication of lessons learned from breaches and near misses should be encouraged by the government, in order to improve available knowledge on latest attack methods, thus improving ability to defend against those. Unfortunately organisations are currently reluctant to openly discuss security problems, mostly due to the severity of potential consequences, like increased customer churn (Ponemon Institute, 2014) or the danger of having to pay severe fines (European Commission, 2015). Recent data released by the UK's Information Commissioner's Office suggests that less than 1 in 10 organisational data breaches are reported (Frearson, 2015). Organisations should be encouraged by the government to come forward about those breaches, in order to improve collective defence abilities. Academia can play a key role in such an approach, acting as an independent mediator, which collects,

anonymises and analyses breaches and near misses that are reported confidentially by organisations. The lessons learned can then be communicated back to organisations as research reports, together with suggestions on how they can improve their existing security approaches to avoid their reoccurrence in the future. Adoption of such a collective learning approach can provide a number of advantages, as it (1) provides organisations with real-world data on latest attack trends so that they can prepare for future ones, (2) creates a collaborative defence culture, where organisational security professionals can share information, moving away from today's deniability-based culture, and (3) allows academic research to access rich, real-world data to produce high-impact research that can solve significant problems of modern information security management.

8.5 Case study conclusion

The case study presented in this chapter aimed to investigate the potential of incorporating the research findings presented in chapters 4, 5, 6 and 7, in order to deliver improvements to an organisation's current security management strategies. Despite frequent changes in the organisational environment and lack of available resources for end-to-end intervention delivery, the lessons learned from working closely with an organisation revealed insights valuable for both academia and industry:

1. Measurable information on employee behaviour exists in abundance across various organisational systems. By implementing mechanisms to continuously assess employee behaviour-related risks, organisations can align their security communication and training with organisational risk appetite, taking appropriate corrective measures when behavioural risks increase above accepted levels.
2. Problems in improvement delivery due to lack of resources or the presence of friction-inducing security systems, exemplify the importance of security hygiene as a prerequisite for delivering effective behavioural change interventions.
3. The experience the researcher gained by attempting to deliver improvements in an organisation, allowed better understanding of the constraints concerning the deployment of research findings in organisational environments and the importance of top management support in attempts to deliver security implementation or behaviour improvements.
4. The improved understanding of the challenges modern organisations face when attempting to deliver effective security (e.g. lack of resources, lack of knowledge exchange), allowed identifying areas for improvement in the relationship between academia, government and industry. Improving the current state of the relationship could lead to improved future collaboration, enhancing organisations' ability to defend themselves from modern security attacks. Using academia as a proxy to encourage information sharing on security incidents and leveraging the emerging knowledge to provide effective defence, can improve ability of modern organisations to stay secure in today's challenging security landscape.

To conclude, despite the case study presented in this chapter not managing to deliver the desired measurable improvements in Company B's security implementation, the lessons learned led to the emergence of valuable insights for both academics and practitioners aiming to collaborate to deliver security improvements in organisational environments.

Chapter 9: Conclusion and contributions

9.1 Overview

Motivation for this research stemmed from the researcher identifying the inability of current security management attempts to create security solutions well-aligned with employee productivity priorities. Despite security managers acknowledging the contribution of employees in delivering effective risk mitigation, current security mechanisms and processes are often incompatible with employee primary tasks, creating friction between security and productivity (section 2.6.1). Employees then refuse to accept the emerging productivity overhead, resorting to insecure behaviours (section 2.6.2). Subsequent security management attempts to eliminate such behaviours through implementation of additional security controls have proven to ineffective (section 2.6.3), sometimes even increasing organisational risk exposure (section 2.6.4). The emerging need for a less taxing, more flexible security approach, which also provides adequate risk mitigation, calls for user-centred security research that improves existing understanding of employee responses to security-productivity friction, also using the emerging paradigms to provide security management principles that accommodate employee priorities.

As a first step towards achieving the employee behaviour understanding discussed above and provide security management with improved understanding and guidelines to design more productivity-driven security, the research presented in this thesis engaged directly with employees in two large organisations, discussing and analysing their responses to friction-inducing security. The research commenced by looking at past research investigating security behaviours, identifying a number of drawbacks (Section 2.8):

1. The majority of research on user beliefs and perceptions driving security behaviours focused on individual home users, while organisational security research focused on higher level risk management and policy formulation approaches.
2. There were only minimal attempts to directly engage with organisational security users using an exploratory research approach to identify and understand the challenges they face in their everyday interactions with security.
3. Research did not attempt to investigate employee responses to friction-inducing security, only characterising employee behaviours as either compliant or non-compliant with organisational security policies.
4. Attempts to identify and consider employee priorities in security design only focused on designing new systems, without attempting to provide knowledge and tools to enable improvements in existing ones.
5. Research has not managed to devise effective security behaviour metrics. Thus it failed to enable security management driven by organisational ability to identify and measure current behaviours, deliver attempted improvements in line with the organisation's security risk appetite, and prioritise allocation of available resources.

In an attempt to improve on the above drawbacks, this thesis presented two case studies conducted in two large organisations, directly engaging with employees, examining their interaction with organisational security provisions, the problems security creates in their primary tasks, together with subsequent

employee responses and coping mechanisms. The case study design was driven by 6 research questions, driven by 5 case study propositions, devised from the problems identified in past organisational security research (section 3.3.1). This chapter (1) uses the findings presented in this thesis to answer the research questions, (2) discusses the validity of the case study propositions, (3) presents the emerging research contributions for both industry and academia, (4) presents a critical review and limitations of the research presented in this thesis, and (5) outlines potential future research directions based on the emerging paradigms.

9.2 Revisiting research questions

The depth of the investigation the grounded theory analysis allowed, provided significant insights on employee behaviours that enabled the researcher to answer all 6 research questions presented at the beginning of Chapter 5.

1. *Do employees understand the need for security mechanisms in the organisation? If yes or no, why?* The results of the analysis demonstrated that employees who understood the need for security were following the official organisational security practices, when the related effort did not create prohibitive primary task overheads (sections 4.6.1 and 5.2.1.3). Contrary to past research presenting them as opportunistic and willing to bypass security when control is not present (section 2.6.5), employees in both organisations examined were willing to invest some of their time and effort to contribute to security risk mitigation, even when no controls and enforcement existed. In other cases though, employees appeared to lack awareness of security risks or mitigation mechanisms, which led to the development of insecure behaviours. The main driver of those was the dysfunctional and generic organisational security communication and training, which failed to provide adequate risk awareness and motivation for employees to participate in security protection (sections 4.6.2.1 and 5.3.1.3).
2. *What security-related challenges do employees find when attempting to proceed with their primary tasks? How do they respond to friction between their primary task and security mechanisms and processes?* Despite their awareness and understanding of the need for security policies and mechanisms, employees chose to procure their own security solutions when security blocked or slowed down their primary tasks (section 5.3.1). They used readily available resources (their own knowledge and inter-employee trust), to devise their own *shadow security* approaches that eliminated or reduced emerging security-productivity friction, while also attempting to deliver some risk mitigation. In other cases they chose to just ignore security. Employee decision between shadow security practices and ignoring security depended on their perceived availability of the less taxing option. For example they password-protected sensitive files shared through emails (shadow security), but used unencrypted drives for larger file sharing in the office when encrypted drives were either unavailable or created problems (insecure behaviour). Decisions were made at an individual or team level (or sometimes both), depending on the team culture and their line manager's advice. In essence, shadow security behaviours, presented employees' own understanding of how workable security, well-fit to their primary tasks, should look like. Their development was accentuated by a lack of accurate risk awareness, ignorance about policies, and employees' need to preserve their relationships with their colleagues. In a number of cases employees also recognised that their

behaviours went against the organisation's security policies, but felt they were the only way to preserve productivity. The wide deployment and variation of emerging shadow security behaviours leads to loss of security management's ability to monitor current state of security in the organisation, also increasing organisational risk exposure, as employees often do not possess accurate risk awareness to make ad-hoc security decisions (section 5.2.3.1).

3. *When organisational security provisions appear to provide inadequate risk mitigation, what do employees do?* A number of cases were identified where existing organisational security systems did not manage to effectively mitigate security risks, or no risk mitigation provisions existed at all (e.g. Company B security policy not providing guidance on how to protect laptops). Employees then took actions to mitigate perceived risks themselves (e.g. not leave it in the car, take it home overnight), often supported by their line managers or colleagues (section 5.3.1.5). In other cases, they downplayed the need for security due to a perception that security management was not interested in delivering effective risk mitigation (e.g. not taking action to remove leavers from access control systems - section 5.3.1.4). This increased their disregard for centrally administered security, providing justification for shadow security development.
4. *How do employees respond to perceived lack of organisational security support? What are the risks from their behaviours and what can organisations learn from those?* When security support is slow to respond to employee requests, or fails to provide solutions to their reported problems, they turn to their colleagues and managers for support. This increases shadow security development at team level, also leading to the emergence of varying security micro-cultures across different organisational divisions. These micro-cultures reduce security management's ability to monitor and control employee security culture development, or to assess the compatibility of the emerging culture with the organisation's security risk appetite. As a result, security managers are left unable to assess the effectiveness of deployed risk mitigation approaches. In addition, the lack of accurate risk understanding amongst employees and line managers, due to the complexity of information security risks, results in the behaviour and habits emerging from the above micro-cultures failing to provide sufficient risk mitigation. Despite the risks the above practices create, organisations can take advantage of employee reports to identity areas where improvements in security implementation are required, also tracking the number of reported problems successfully resolved to assess whether improvements are required in organisational security support provisions.
5. *How can the improved understanding from the previous questions be used to transform the systems in place to eliminate the problems discovered, avoiding the need to redesign the systems completely?* Shadow security is an indicator that existing security management approaches are failing to provide employees with workable security. It presents conditions where security better-fitted to productive activity is required, so its presence should be seen as an opportunity to identify potential improvements to better align security with productivity requirements. Attempts to deliver that alignment, should aim to use readily available (or easy to collect) information from around the organisation to develop metrics that enable identification of shadow security behaviours. Those metrics should then be used to drive security management decisions, driven by the organisational security risk appetite. A set of example metrics was presented in section 7.5, based on the available information identified in the two organisations examined. While those may not be applicable to all organisations, they can provide a basis for developing similar approaches, where security

management can use other organisation-specific information to develop their own relevant security behaviour metrics.

6. *What trust relationships develop in an organisation and how do they influence security behaviours?* The shadow security analysis of chapter 6 also led to the identification of two security-related trust relationships in organisations: *organisation-employee trust* (shown by the organisation towards its employees) and *inter-employee trust* (developed between employees during their interactions both inside and outside of the security environment). The two relationships come into conflict when the security policy asks employees to show distrust towards their colleagues, for example by prohibiting password sharing. Inter-employee trust then prevails due to *contextual* and *intrinsic* incentives that encourage employees to preserve their relationships with their colleagues, in order to maintain a collaborative environment and benefit from it in the future (section 6.6.2). The immediate availability of inter-employee trust also makes it a readily-available resource to cope with friction-inducing security, accentuating shadow security development (section 6.5.4). As a result, any attempt to use shadow security to deliver improvements in organisational security implementations (discussed above in relation to question 5 and extensively in chapter 7), needs to also understand the effects of trust relationships on employee security behaviours and formalise their presence in emerging security mechanisms and processes (section 7.4).

9.3 Revisiting research propositions

The research propositions (originally defined in section 3.3.1), aimed to assess the effectiveness of the chosen research methodology (case study directly engaging with employees, also using grounded theory as a data analysis tool) as a security behaviour research tool, also providing the ability to answer the research questions discussed in the previous section. Early indications on the validity of those propositions emerged from the analysis in chapter 4 and were discussed in section 4.7, explaining that further research was required to be able to provide solid evidence on their validity. The findings that emerged from chapters 5 and 6 both strengthened evidence on proposition validity emerging from chapter 4, and are discussed in detail in the remainder of this section

P1. "Directly discussing problems of security implementations and compliance with employees can lead to improved understanding of the reasons driving employee insecure behaviours"

Using semi-structured interviews to discuss employee experiences with organisational security mechanisms, policies and processes lead to a number of previously unidentified insights on employee behaviours: (1) identification of employee willingness to participate in security, contrary to past research that presented them as opportunistic, (2) identification of employee drivers for secure behaviour, (3) identification, characterisation and categorisation of insecure behaviours, based on specific elements of the security implementation or the organisational environment that led to their development. The wide number of example behaviours identified and their prevalence in the organisations examined (presented in detail in chapters 4, 5 and 6), together with steps taken to improve outcome validity and generalisability (section 3.4) provide sufficient evidence that P1 is a valid proposition.

P2. "*Engagement with employees can allow falsifying current beliefs that employees can be forced to comply with security*"

Security implementations that fail to provide uninterrupted protection to organisational productive activities create significant overheads for employees. Security management attempts to enforce such friction-inducing security on employees through security controls (technical and policies with sanctions) lead to: (1) employees always finding ways to bypass friction-inducing security, even when restrictions are implemented to prevent this. Any subsequent attempts to tighten controls (2) increase policy enforcement costs, due to the need to anticipate for all potential non-compliance behaviours and exhaustively eliminate those. Excessive enforcement attempts also create a (3) negative attitude towards security, reducing security management's ability to leverage security-awareness of its workforce and encourage increased participation in security protection, thus (4) decreasing security management ability to defend itself against constantly changing threats. It also (5) prevents organisations from formalising the trust shown towards their security-conscious employees and providing flexibility to address security-related friction to be able to proceed with their productive tasks. In addition, (6) given the high-number of identified violations emerging from employees bypassing friction-inducing security, security management attempts to sanction violations would result to an unmanageably large number of employees being disciplined. The above six points emerged from the findings of the analyses presented in chapters 4, 5 and 6, and demonstrate the importance of security hygiene (section 7.2.1) as a prerequisite to any attempts to enforce security policies through controls. As a result they provide sufficient evidence on the validity of P2.

P3. "*Engagement with employees can allow identification of employee responses to friction-inducing security*"

The identification, characterisation and understanding of shadow security presents a new paradigm for security management, providing significantly improved insights compared to past research on employee behaviours. Initial indications of employees adapting security were made by Inglesant and Sasse (2010), who identified that employees re-organise their primary tasks to reduce exposure to friction-inducing security, and Bartsch and Sasse (2012), where employees responded to problematic access control provisions by sharing information through informal channels. Building on those reports, shadow security identification manages to capture employee responses to a variety of different friction-inducing elements of the security implementation (section 5.2). Employees who come across friction-inducing security, ignore, bypass or modify official security, attempting to mitigate risks using less taxing, self-devised practices. In addition, when official security comes into conflict with their relationships with their colleagues, asking them to treat those as untrustworthy, shadow security develops at team-level. This leads to collaborative violations, as employees often consider their colleague relationships as more important than behaving securely. The above findings constitute a significant improvement in the understanding of employee responses and coping mechanisms with friction-inducing security, providing significant evidence on the validity of P3.

P4. "*Engagement with employees can allow the identification of problems in security implementations (both policies and mechanisms) that organisations have not currently identified through other means*"

As discussed in section **Error! Reference source not found.**, past research in organisational information security primarily focused on using research tools like questionnaires to test pre-defined hypotheses, with limited attempts to examine employee interaction with security implementations in their entirety. The exploratory nature of this work attempted to build on early insights of exploratory security behaviour research (section 2.8.2), to identify and describe previously unidentified problems in security implementations, improve security managers' ability to capture those, and provide guidance on addressing the risks emerging from their existence. Some of the behaviours emerging from this research (e.g. clear desk, screen lock, employees using own USBs) were often easy for organisations to capture using their current security processes, but the improved understanding of the drivers behind those (friction-inducing security and inter-employee trust) also improves security management's ability to deploy appropriate improvements. In other cases though, the open and exploratory approach of interviews and analysis process managed to capture a number of otherwise hard to identify friction-inducing mechanisms and processes, together with corresponding employee behaviours (e.g. ineffectiveness of organisational security communication, employees sharing passwords or storing documents locally on laptops). This led to improved understanding of situations where existing security implementations fail to accommodate employee priorities, providing sufficient evidence that P4 is also a valid proposition.

P5. "*Engagement with employees can improve existing organisational ability to manage current information security challenges*"

The identification of shadow security, together with its characterisation and understanding of factors that drive its development, led to the creation of a number of different tools that security managers can use to identify, understand and improve security implementations. The emerging model of employee security behaviours (7.1.2), the risk-driven security intervention processes (7.5.1), the metrics allowing identification and prevalence assessment of friction inducing security (7.5.2), together with the pre-deployment intervention impact assessment and post-deployment monitoring process (7.5.3), manage to: (1) improve security management's ability to understand how friction-inducing security affects employee behaviours, (2) identify and prioritise improvements based on risk assessment and available resources to deliver the best possible security risk mitigation, also (3) aligning security mechanisms and processes with organisational productivity. Improved alignment (4) enables employees to behave securely, (5) also allowing security management to implement a continuous, metrics-driven monitoring process, to capture a holistic understanding of the state of information security behaviours in the organisation. All the above points suggest that research directly engaging with employees can improve security managers' ability to deliver less taxing and more effective security, providing sufficient evidence that P5 is also a valid proposition.

9.4 Contributions

This thesis presented a number of new paradigms, models and processes that allow security managers to effectively understand and manage employee security behaviours. The emerged knowledge on shadow security development (section 5.3), security-related trust relationships (section 6.5) and their impact on the effectiveness of current security management attempts (sections 5.3.4 and 6.6), improves current understanding of the security challenges faced by employees in modern organisations (security and productivity coming to friction), the effect of the above paradigms on their security decisions (security violations or shadow security), and the consequences to the organisation (reduced security implementation effectiveness). In addition, the emerging tools and processes (shadow security metrics – section 7.5.1, risk-driven behaviour measurement and decision making process – section 7.5.2), and the lessons learned from attempts to apply those in an organisation (section 8.4), provide practical guidance for both researchers and security managers to aid the delivery of a metrics-driven security management approach, using readily available or easy to collect information. This section presents the thesis contributions to research and industry in detail.

9.4.1 Research

9.4.1.1 Substantive

This thesis revealed a number of employee security behaviour insights, improving on the findings of past security research. It (1) identified employee willingness to invest time and effort in order to behave securely, but only when security was compatible with their primary tasks. It (2) enriched current understanding of employee responses to friction-inducing security (the *shadow security*), also (3) demonstrating the importance of the need to stop considering employee security behaviours as a binary, compliant or non-compliant decision. It also (4) revealed a number of different elements of security implementations that drive shadow security development. Another contribution is (5) the emerging model of employee security behaviour that improves current understanding of the influence of various elements of the organisational environment on employee security decisions, culture and habit development. The model also (6) provides focus for future research attempts to disrupt the security culture and habits cycle presented in section 7.1.2, in order to deliver long lasting security behaviour change. In addition, (7) the trust relationships identified provided a new paradigm for employee security behaviour, which further improved understanding of the drivers behind policy violations and shadow security practices. Finally, (8) the metrics-driven shadow security improvements process also demonstrates the feasibility of delivering improvements to existing security, based on information collected within the organisation.

9.4.1.2 Methodological

The thesis also (1) provided sufficient insights to confirm the validity of research propositions, (2) demonstrating the usefulness of case study as an information security research tool and (3) grounded theory as an analysis approach to enable in-depth exploratory investigation of employee behaviours. In addition, (4) closely working with organisations and directly interacting with employees can also improve outcome validity and subsequent research impact. The case study findings also revealed that, (5) in order to be able to deliver effective security interventions, researchers need to understand that organisational

security changes take time, require good planning and need to be part of a formalised information security strategy approved by top management.

9.4.2 Industry

9.4.2.1 Substantive

The main industry-related contribution emerging from this thesis is the identification and understanding of shadow security and its usefulness as a security management tool. The research presented in this thesis, improved understanding of how shadow security develops and how it can help security management. It provides a unique opportunity to re-think current security management approaches and deliver more effective protection for organisations, while still serving the business strategy. In order to deliver that protection, organisations need to:

1. *Take advantage of intrinsic propensity of employees to behave securely*. The first and foremost benefit of the findings of this work provides is the clear evidence that employees want security. They feel connected to the organisation, they are motivated to participate in protection and willing to do so if the current security implementation does not create prohibitive time and effort overheads. But, when security-productivity friction emerges, employee productivity focus leads to shadow security development. To reduce emerging friction, employees should be involved in security design, in order to deliver security mechanisms better fit around their productivity priorities (section 7.3.1).
2. *Measure behaviour, but deliver hygiene first*. Before attempting to measure and improve security behaviours, security management needs to understand that the most important prerequisite for learning and data-driven behavioural change is security hygiene. Security mechanisms and processes not designed with employee priorities in mind will inevitably lead to security-productivity friction. Employees will then bypass those and deployed security will never manage to deliver adequate risk mitigation (7.2.1). Security hygiene may require some additional resource investment at its early stages, but in the long run it can drive cost-effective risk mitigation, by reducing shadow security development, thus improving security management's ability to detect and further investigate potentially malicious security violations.
3. *Implement metrics driven, learning-based security management*. The identified metrics provide a unique ability for security management to quantify its decisions and align those with organisational risk appetite (section 7.4). Shadow security metrics can reveal areas where security management interventions are required, with subsequent resource allocation being based on organisational risk priorities, thus providing the best possible risk mitigation given the available resources. Over time this approach can evolve to an automated and low-resource approach to manage security, allowing for continuous assessment of mechanism and process effectiveness in both a pre- and post-deployment way. It is important to also note that, in accordance with the ethical principles presented in section 3.6, the deployed metrics should not be used to enable mass identification and sanctioning of employees, but should be treated as an opportunity for organisations to deploy a learning-based security management approach.
4. *Formalise trust presence, avoid excessive enforcement but sanction misbehaviours*. The findings of this thesis also present a good starting point to understand how trust plays a crucial

role in delivering security protection for an organisation (sections 6.6 and 7.4). Trust shown towards employees should be formalised in security implementations and its presence should be a central part of security communication (section 7.4.2), with appropriate processes implemented to sanction violations; once again security hygiene is key to delivering this (section 7.4.2.1). When this is achieved, trust also becomes an effective risk management tool: where security risks are low, trusting employees enables resources to be invested in mitigating more important ones (section 7.4.2.2). The emerging employee responsibility should be visible to employees, with consequences for misbehaviours being both communicated and enforced (section 7.4.2.5)

The above four points should be treated as the pillars on which modern organisations should aim to build effective security management approaches. They provide a unique opportunity to manage security behaviour using a centralised, learning-oriented approach, decrease security-productivity friction and provide more effective security risk mitigation. Initial resources required to put the above to practice should be seen as investments to deliver a sustainable, predictive, adaptable and effective security implementation.

9.4.2.2 Methodological

The findings and emerging paradigms allowed reframing modern security management as a continuous, learning-based approach that can be adaptable to the continuously changing modern security challenges (section 7.5.1). They also present the importance of metrics to the success of such an approach, allowing easier identification of employee responses to friction inducing security (section 7.5.2). It is also important for both security managers and top-level organisational managers, to understand the impossibility of delivering effective security improvements without corporate governance adoption. Security decisions should be driven from the top of an organisation, ensuring formal allocation of resources and access to information required to implement such a security management approach.

Another paradigm that emerged from the case study in chapter 8, is the need to create comprehensive and well-integrated standardisation programs for information security management. Organisational attempts to comply with a wide range of information security standards lead to redundancy, with valuable resources being expended on passing various audit processes (section 8.4.5). Standardisation bodies should aim to eliminate this redundancy, by creating standards compatible between them that include interchangeable clauses, allowing the emergence of more effective and easy to apply standards that aid effective security management, rather than creating overheads.

Both the substantive and methodological contributions for industry will be easier to put to practice if organisations understand the benefits of seeking help from academia. Organisations should take advantage of existing academic knowledge on human behaviour and methodological principles required for effective metrics deployment, to improve their existing security management approaches (section 8.4.7.1). Governments should also be involved in this approach, further encouraging industry collaboration with academia: government bodies are often the main source of funding for academic research, so enabling collaboration between industry and academia can maximise the real-world impact of allocated funds and resources (section 8.4.7.2).

9.5 Research limitations

Despite the importance and applicability of the contributions of this thesis, looking back to the analysis process, a number of potential drawbacks can be identified:

1. The 30 interviews used for the thematic analysis (chapter 4) were randomly chosen. Given the purpose of that analysis (provide preliminary understanding of employee behaviours to guide further analyses), it would have been beneficial to select interviews covering a wide range of employee backgrounds and organisational positions. The negative effects of this were later alleviated by the subsequent grounded theory analysis of the entire company A dataset and iterative analysis to ensure no behaviours of interest were missed. Despite that, achieving a wider representation would have possibly improved the emerging preliminary employee behaviour understanding. This would have made the analyses presented in chapters 5 and 6 easier to conduct.
2. The time limitations, created by the need to complete this research within the timeframe of a PhD degree, limited the number of organisations that could be examined to two. The time required to analyse the available dataset from Company A (also liaising with the company for clarification on identified security problems, access to resources/policies required etc.), collect and analyse data from Company B, together with subsequent analyses to confirm and better characterise the paradigms presented in this thesis, made it impossible to conduct a third analysis[29]. Despite the drawbacks, the identification of similar behavioural patterns in both organisations, both in terms of shadow security and trust relationships, provided sufficient evidence on the validity of case study propositions.
3. Despite some attempts to deploy shadow security-driven security management approaches in Company B (discussed extensively in chapter 8), time constraints and structural problems in the organisation (section 8.2.3) prevented successful application of the findings of this research in an organisation. The emergence of the presented models and security management processes from direct engagement with organisations provides some evidence on their suitability to organisational security management, but putting those to practice would have strengthened that evidence.

9.6 Future work

The exploratory nature of this work, together with the above critical review, present a number of potential opportunities to build on the findings and the suggestions of this thesis, which could not be explored during the course of a three year PhD project. This section provides potential directions for future research, in order to expand the scope of the emerged paradigms, but also deploy and assess the effectiveness of the presented security management processes.

[29] Despite attempting to work with a third organisation, limitations in their security management resources, together with other logistical and time constraints did not allow for this to happen

9.6.1 Improve shadow security understanding

This work allowed identification of shadow security as a phenomenon, together with its development drivers and its effect on employee behaviours. Based on the findings, two major areas where further research can improve shadow security understanding were identified:

1. Security "micro-culture" development within organisational sub-divisions needs to be further examined. Micro-cultures develop within teams and are reinforced by both team managers and team members providing support to each other. Future research needs to examine those to identify how variations within different organisational subdivisions, like differing primary task and security requirements, physical arrangements (e.g. working from home, between-office differences) and line management practices can affect micro-culture development and subsequent security behaviours. In order to achieve this, shadow security measurements need to be deployed in an organisation and then comparisons being drawn between subdivisions, attempting to correlate between division variations and emerging security behaviours. This can improve security management ability to target shadow security-driven interventions towards specific organisational subdivisions, delivering targeted risk mitigation (section 7.5.4).
2. Employee risk perceptions regarding their chosen shadow security practices also need to be assessed. In many of the shadow security and trust-driven policy violation examples presented in chapters 5 and 6, employees acknowledged that some of their practices were compromising security. Further interviews and in-depth analyses are required, to investigate employee perception of risks associated with those practices (e.g. when cloud storage is used to store corporate data, are employees aware that cloud storage providers may be compromised? If yes do they take any mitigating actions?). Better characterisation of employee risk perceptions can allow security managers to better assess the risks emerging from current employee security practices, but also target future behavioural change attempts towards changing those risk perceptions.

9.6.2 Expand scope

Future research also needs to investigate and characterise shadow security development in environments that vary from those examined in this work. Organisations of varying sizes, with diverging operational procedures, operating in different countries and different corporate cultures need to be examined. As discussed in section 7.5, one of the main advantages of shadow-security measurement approaches is the ability of security managers in different organisations to flexibly adjust the proposed metrics, based on organisation-specific risks, security risk appetite, risk prioritisation and resources available. Shadow security may emerge with different characteristics in organisations of varying size and industries. Examining shadow security development in varying contexts can allow researchers to create improved guidelines for managing shadow security development in different organisational settings.

It is also important to further examine the compatibility of shadow security-driven information security management with current regulatory frameworks and international standards (some preliminary discussion on this was is presented in section 8.4.5). The security management process that emerged from the findings needs to be examined for compatibility with modern information security legislation

and standardisation requirements. Providing sufficient compatibility evidence, combined with the shadow security benefits presented in section 7.5.4, can encourage adoption of shadow security in organisational attempts to deliver effective and efficient security.

9.6.3 Testing emerging paradigms and models

The metrics-driven security management approach presented in section 7.5 should be put to practice in a few organisations. Potential resource and security effectiveness gains should be recorded and subsequent communication should encourage organisational adoption of shadow security measurement as a "tried and tested" security management approach. The effect of trust relationship formalisation on security behaviours should also be assessed (section 7.4.2), by putting it to practice and measuring its impact on employee behaviours through the deployed shadow security metrics.

Another area that requires further research is the potential to quantitatively test the model of security behaviour presented in section 7.1.2. This may be difficult though, due to the complexity and inter-relations between various elements of the model and emerging behaviours. It may prove to be hard to conduct controlled experiments to test individual cause and effect relationships in isolation, or isolate the effect of individual factors on emerging security behaviours. Despite this, attempting to formally assess the validity of the model may also reveal other elements of the organisational environment affecting employee security behaviours that the analyses presented in this thesis may have failed to capture.

9.6.4 Potential extensions to the devised models

Despite the security behaviour model presented in section 7.1.2 providing valuable employee behaviour insights to organisational security management, a number of potential areas for further research were identified:

1. Research needs to investigate the impact of the changing organisational environment on security management approaches. Outsourcing, for example, is increasingly popular amongst large organisations, in an attempt to save money and receive better service from specialist providers. Its impact on employee security trust development and its effects on security behaviour have not been examined to date. Employee responses to outsourcing and other changes in the organisational environment should be examined (e.g. increased amount of employees working from home and deployment of schemes like Bring Your Own Device), identifying their influence on security-related trust relationships and shadow security development.
2. Security self-reporting by employees also deserves to be further researched. As part of a participatory security management approach (section 7.3.1), it is important to evaluate whether employees would be willing to report security problems, but also security violations, if sufficient assurance is provided that such reporting will have no negative impact on them. Past research already suggested that users are willing to participate in security and that the presence of organisation-employee trust can improve motivation to cooperate even further, acting as a substitute for control (section 7.4.2). As a result, it is important to encourage organisations to deploy the employee reporting mechanisms and corresponding feedback mechanisms presented in section 7.3.1, and assess the effects of this deployment on employee behaviours.

3. The need for mutual authentication mechanisms also needs to be examined. Fléchais et al. (2005) suggested that the creation of simple, reliable means of mutual authentication for employees to authenticate to each other can significantly reduce the risks from social engineering. Unfortunately no evidence was found in the work presented in this thesis to support that statement, but this is a promising suggestion that deserves to be part of further future research on the subject.

In general, all the steps of the shadow security management process (section 7.3) can be investigated in depth. For many of those though, it can be impractical or even impossible to be tested using traditional hypothesis testing approaches; as explained in section 8.3.4, controlled experiments are hard when the researcher requires control over many elements of the organisational environment. Despite that, deploying the above process and collecting targeted measurements to assess the impact of specific elements of the security implementation, can provide sufficient indication of their effectiveness. This can provide security managers with a new and powerful tool for effective security risk management decision making and resource allocation.

References

Adams, Anne, and Martina Angela Sasse. 1999. “Users Are Not the Enemy.” *Communications of the ACM* 42 (12). ACM: 40–46. doi:10.1145/322796.322806.

Adams, John. 1995. *Risk*. Psychology Press. http://books.google.co.uk/books/about/Risk.html?id=xqdY_4N0_rsC&pgis=1.

Albrechtsen, Eirik. 2007. “A Qualitative Study of Users’ View on Information Security.” *Computers & Security* 26 (4): 276–89. doi:10.1016/j.cose.2006.11.004.

Albrechtsen, Eirik, and Jan Hovden. 2009. “The Information Security Digital Divide between Information Security Managers and Users.” *Computers & Security* 28 (6): 476–90. doi:10.1016/j.cose.2009.01.003.

Alfawaz, Salahuddin, Karen Nelson, and Kavoos Mohannak. 2010. “Information Security Culture: A Behaviour Compliance Conceptual Framework.” *Conferences in Research and Practice in Information Technology Series* 105: 47–55. http://www.mendeley.com/catalog/information-security-culture-behaviour-compliance-conceptual-framework/.

Amaratunga, Dilanthi, Baldry, David, Sarshar, Marjan, Newton, Rita. 2002. “Quantitative and Qualitative Research in the Built Environment: Application Of ‘mixed’ research Approach.” *International Postgraduate Conference*. http://www.adolphus.me.uk/emx/research_design/meth_be_files/p17.htm.

Anderson, Evan E., and Joobin Choobineh. 2008. “Enterprise Information Security Strategies.” *Computers & Security* 27 (1-2): 22–29. doi:10.1016/j.cose.2008.03.002.

Anderson, Ross J. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Vol. 5. John Wiley & Sons. http://books.google.co.uk/books/about/Security_Engineering.html?id=eo4Otm_TcW8C&pgis=1.

Anderson, Ross J., and Tyler Moore. 2006. “The Economics of Information Security.” *Science (New York, N.Y.)* 314 (5799): 610–13. doi:10.1126/science.1130992.

Ashenden, Debi. 2008. “Information Security Management: A Human Challenge?” *Information Security Technical Report* 13 (4). Elsevier Advanced Technology Publications: 195–201. doi:10.1016/j.istr.2008.10.006.

Ashenden, Debi. 2015. “Information Security Awareness: Improving Current Research & Practice.”

Ashenden, Debi, and Martina Angela Sasse. 2013. “CISOs and Organisational Culture: Their Own Worst Enemy?” *Computers & Security*. http://discovery.ucl.ac.uk/1417350/1/Ashenden_and_Sasse_-_2013_-_CISOs_and_organisational_culture_Their_own_worst_-postprint.pdf.

Auerbach. 1974. *Auerbach Guide to Time Sharing Services*. Auerbach Publ.

http://books.google.co.uk/books/about/Auerbach_Guide_to_Time_Sharing_Services.html?id=iROjHwAACAAJ&pgis=1.

Axelrod, R. 1980. “More Effective Choice in the Prisoner’s Dilemma.” *Journal of Conflict Resolution*. http://www.jstor.org/stable/173638.

Bacharach, M, and D Gambetta. 2001. “Trust in Signs.” *Trust in Society*. https://books.google.co.uk/books?hl=en&lr=&id=xuSFAwAAQBAJ&oi=fnd&pg=PA148&dq=Trust+in+signs&ots=DsFfl4XBdg&sig=fScu6s5Of68_Mx3b9zvh6aF_1Hs.

Bartsch, Steffen. 2012. “Broadening the Scope of Security Usability from the Individual to the Organizational : Participation and Interaction for Effective, Efficient, and Agile Authorization.” http://elib.suub.uni-bremen.de/peid=D00102681&Exemplar=1&LAN=DE.

Bartsch, Steffen. 2014. “Policy Override in Practice: Model, Evaluation, and Decision Support.” *Security and Communication Networks* 7 (1): 139–56. doi:10.1002/sec.547.

Bartsch, Steffen, and Martina Angela Sasse. 2012. “Guiding Decisions on Authorization Policies.” In *Proceedings of the 27th Annual ACM Symposium on Applied Computing - SAC ’12*, 1502. New York, New York, USA: ACM Press. doi:10.1145/2245276.2232015.

Bartsch, Steffen, and Martina Angela Sasse. 2013. “How Users Bypass Access Control - And Why: The Impact Of Authorization Problems On Individuals And The Organization.” *ECIS 2013 Completed Research*. http://aisel.aisnet.org/ecis2013_cr/53.

Baskerville, Richard, and Mikko Siponen. 2013. “An Information Security Meta-policy for Emergent Organizations,” April. MCB UP Ltd. http://www.emeraldinsight.com/doi/full/10.1108/09576050210447019.

BCS. 2011. “BCS Code of Conduct.” www.bcs.org/category/6030.

Beautement, Adam, Martina Angela Sasse, and Mike Wonham. 2008. “The Compliance Budget.” In *Proceedings of the 2008 Workshop on New Security Paradigms - NSPW ’08*, 47. New York, New York, USA: ACM Press. doi:10.1145/1595676.1595684.

Björck, F. 2001. “Security Scandinavian Style.” *Doctoral Dissertation, Stockholm University.* http://people.dsv.su.se/~bjorck/files/bjorck-thesis.pdf.

Blakley, Bob, Ellen McDermott, and Dan Geer. 2001. “Information Security Is Information Risk Management.” In *Proceedings of the 2001 Workshop on New Security Paradigms - NSPW ’01,* 97. New York, New York, USA: ACM Press. doi:10.1145/508171.508187.

Blythe, Jim, Ross Koppel, and Sean W. Smith. 2014. “Circumvention of Security: Good Users Do Bad Things.” *IEEE Security & Privacy* 11 (5). IEEE Computer Society: 80–83. http://cat.inist.fr/?aModele=afficheN&cpsidt=27789556.

Böhme, Rainer, and Jens Grossklags. 2011. “The Security Cost of Cheap User Interaction.” In *Proceedings of the 2011 Workshop on New Security Paradigms Workshop - NSPW ’11*, 67. New York, New York, USA: ACM Press. doi:10.1145/2073276.2073284.

Boyatzis, Richard E. 1998. *Transforming Qualitative Information: Thematic Analysis and Code Development*. SAGE Publications. http://books.google.co.uk/books/about/Transforming_Qualitative_Information.html?id=_rfClWRhIKAC&pgis=1.

BPS. 2009. “Code of Ethics and Conduct.” http://www.bps.org.uk/system/files/documents/code_of_ethics_and_conduct.pdf.

Braun, Virginia, and Victoria Clarke. 2006. “Using Thematic Analysis in Psychology.” *Qualitative Research in Psychology* 3: 77–101.

Brostoff, S, and MA Sasse. 2000. “Are Passfaces More Usable than Passwords? A Field Trial Investigation,” November. SPRINGER-VERLAG LONDON LTD. http://discovery.ucl.ac.uk/19830/4/RPS deposit licence.pdf.

Brostoff, Sacha, and Martina Angela Sasse. 2001. “Safe and Sound.” In *Proceedings of the 2001 Workshop on New Security Paradigms - NSPW ’01*, 41. New York, New York, USA: ACM Press. doi:10.1145/508171.508178.

Brotby, W. Krag, Hinson, Gary. 2013. “PRAGMATIC Security Metrics: Applying Metametrics to Information Security.” *Auerbach Publications*. http://www.amazon.co.uk/PRAGMATIC-Security-Metrics-Metametrics-Information/dp/1439881529.

Bryman, Alan E. 2003. “Triangulation.” In *The SAGE Encyclopedia of Social Science Research Methods*. SAGE Publications. http://books.google.com/books?id=iu1yAwAAQBAJ&pgis=1.

Bryman, Alan E. 2012. *Social Research Methods*. Oxford University Press. http://books.google.com/books?hl=en&lr=&id=vCq5m2hPkOMC&pgis=1.

BSI Group. 2014. “Benefits of Using Standards.” http://www.bsigroup.com/en-GB/standards/benefits-of-using-standards/.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.” *MIS Quarterly* 34 (3). Society for Information Management and The Management Information Systems Research Center: 523–48. http://dl.acm.org/citation.cfm?id=2017470.2017477.

Bussing, A. 2002. “Trust and Its Relations to Commitment and Involvement in Work and Organisations.” *SA Journal of Industrial Psychology*. http://reference.sabinet.co.za/sa_epublication_article/psyc_v28_n4_a7.

Cai, Jian, Xiangdong Liu, Zhihui Xiao, and Jin Liu. 2009. “Improving Supply Chain Performance

Management: A Systematic Approach to Analyzing Iterative KPI Accomplishment." *Decision Support Systems* 46 (2): 512–21. doi:10.1016/j.dss.2008.09.004.

Camp, L. 2009. "Mental Models of Privacy and Security." *IEEE Technology and Society Magazine* 28 (3). IEEE: 37–46. doi:10.1109/MTS.2009.934142.

Camp, L. Jean. 2011. "Reconceptualizing the Role of Security User." *Daedalus* 140 (4). MIT Press 55 Hayward Street, Cambridge, MA 02142-1315 USA journals-info@mit.edu: 93–107. doi:10.1162/DAED_a_00117.

Caputo, D., M. Maloof, and G. Stephens. 2009. "Detecting Insider Theft of Trade Secrets." *IEEE Security & Privacy Magazine* 7 (6). IEEE Computer Society: 14–21. doi:10.1109/MSP.2009.110.

CEBR. 2015. "60% of British CTOs Say UK Government Is Performing Poorly in Protecting Firms from Cyberattacks." *Centre for Economics and Business Research*. http://www.cebr.com/reports/60-of-british-ctos-say-uk-government-is-performing-poorly-in-protecting-firms-from-cyberattacks/.

Checkland, P, and J Poulter. 2006. *Learning for Action: A Short Definitive Account of Soft Systems Methodology and Its Use for Practitioner, Teachers, and Students*. http://library.wur.nl/WebQuery/clc/1928849.

Chen, Kuanchin, and David C. Yen. 2004. "Improving the Quality of Online Presence through Interactivity." *Information & Management* 42 (1): 217–26. doi:10.1016/j.im.2004.01.005.

Cherdantseva, Y., and J Hilton. 2012. *Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals*.

Churchhouse, R. F. 2002. *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet*. Cambridge University Press. http://books.google.co.uk/books/about/Codes_and_Ciphers.html?id=FM5auDN2DXIC&pgis=1.

Clark, D. 2014. "The Role of Trust in Cyberspace." *Trust, Computing, and Society*. https://books.google.com/books?hl=en&lr=&id=ZtbSAgAAQBAJ&oi=fnd&pg=PA17&dq=the+role+of+trust+in+cyberspace&ots=mew2rBjy8G&sig=W3X1UO17zhf5fgYb8oarsNB7FTY.

CNSS. 2010. *Committee on National Security Systems: National Information Assurance (IA) Glossary*.

Corritore, Cynthia L., Beverly Kracher, and Susan Wiedenbeck. 2003. "On-Line Trust: Concepts, Evolving Themes, a Model." *International Journal of Human-Computer Studies* 58 (6). Academic Press, Inc.: 737–58. doi:10.1016/S1071-5819(03)00041-7.

Costa, AC, RA Roe, and T Taillieu. 2001. "Trust within Teams: The Relation with Performance Effectiveness." *European Journal of Work and …*. http://www.tandfonline.com/doi/abs/10.1080/13594320143000654.

Cranor, Lorrie, and Simson Garfinkel. 2005. "Security and Usability," August. O'Reilly Media, Inc.

http://dl.acm.org/citation.cfm?id=1098730.

Da Veiga, A., and J.H.P Eloff. 2010. “A Framework and Assessment Instrument for Information Security Culture.” *Computers & Security* 29 (2): 196–207. doi:10.1016/j.cose.2009.09.002.

Deutsch, M. 1958. “Trust and Suspicion.” *Journal of Conflict Resolution*. http://www.jstor.org/stable/172886.

Dhamija, Rachna, J. D. Tygar, and Marti Hearst. 2006. “Why Phishing Works.” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI ’06*, 581. New York, New York, USA: ACM Press. doi:10.1145/1124772.1124861.

Dhillon, Gurpreet, and James Backhouse. 2001. “Current Directions in IS Security Research: Towards Socio-Organizational Perspectives.” *Information Systems Journal* 11 (2): 127–53. doi:10.1046/j.1365-2575.2001.00099.x.

Dix, Alan, Janet Finlay, Gregory Abowd, and Russell Beale. 2003. *Human-Computer Interaction (3rd Edition)*. Prentice Hall.

Dourish, Paul, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. “Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem.” *Personal and Ubiquitous Computing* 8 (6). Springer-Verlag: 391–401. doi:10.1007/s00779-004-0308-5.

Dourish, Paul, and David Redmiles. 2002. “An Approach to Usable Security Based on Event Monitoring and Visualization.” In *Proceedings of the 2002 Workshop on New Security Paradigms - NSPW ’02*, 75. New York, New York, USA: ACM Press. doi:10.1145/844102.844116.

DPA. 1998. “Data Protection Act.” *Information Commissioner’s Office*.

Egelman, S, and S Schechter. 2013. “The Importance of Being Earnest.” *Financial Cryptography and Data Security*. http://link.springer.com/chapter/10.1007/978-3-642-39884-1_5.

Eisenhardt, K. M. 1989. “Building Theories from Case Study Research.” *Academy of Management Review*. http://amr.aom.org/content/14/4/532.short.

European Commission. 2015. “Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market.” http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

Evans, Rob. 2013. “Serious Fraud Office Admits Losing Thousands of Documents Linked to BAE.” *Guardian News, 8 August 2013*. http://www.theguardian.com/law/2013/aug/08/serious-fraud-office-bae-documents.

Eysenck. 2013. *Case Studies in Behaviour Therapy*. Vol. 26. Routledge. http://books.google.com/books?id=2IIuAgAAQBAJ&pgis=1.

Faily, Shamal, and Ivan Fléchais. 2010. “A Meta-Model for Usable Secure Requirements Engineering.” In *Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems - SESS ’10*, 29–35. New York, New York, USA: ACM Press. doi:10.1145/1809100.1809105.

Flechais, Ivan, Cecilia Mascolo, and Martina Angela Sasse. 2007. “Integrating Security and Usability into the Requirements and Design Process.” *International Journal of Electronic Security and Digital Forensics* 1 (1). Inderscience Publishers: 12. doi:10.1504/IJESDF.2007.013589.

Flechais, Ivan, Jens Riegelsberger, and Martina Angela Sasse. 2005. “Divide and Conquer.” In *Proceedings of the 2005 Workshop on New Security Paradigms - NSPW ’05*, 33. New York, New York, USA: ACM Press. doi:10.1145/1146269.1146280.

Florêncio, Dinei, and Cormac Herley. 2010. “Where Do Security Policies Come From?” In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS ’10*, 1. New York, New York, USA: ACM Press. doi:10.1145/1837110.1837124.

Flyvbjerg, Bent. 2006. “Five Misunderstandings About Case-Study Research.” *Qualitative Inquiry* 12 (2): 219–45. doi:10.1177/1077800405284363.

Flyvbjerg, Bent. 2011. “‘Case Study.’” In *The Sage Handbook of Qualitative Research, 4ed.*, 301–16. Thousand Oaks, CA: Sage Publications.

Frearson, Joanne. 2015. “Thousands of Potential Data Breaches Going Unreported, Says ViaSat UK - » Business Reporter.” *Business Reporter*. http://business-reporter.co.uk/2015/06/02/thousands-of-potential-data-breaches-going-unreported-says-viasat-uk/.

Fukuyama, F. 2001. “Social Capital, Civil Society and Development.” *Third World Quarterly*. http://www.tandfonline.com/doi/abs/10.1080/713701144.

Fulford, Heather, and Neil F. Doherty. 2003. “The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation.” *Information Management & Computer Security* 11 (2-3). Emerald: 106–14. http://cat.inist.fr/?aModele=afficheN&cpsidt=14970664.

Furnell, S.M., A. Jusoh, and D. Katsabas. 2006. “The Challenges of Understanding and Using Security: A Survey of End-Users.” *Computers & Security* 25 (1): 27–35. doi:10.1016/j.cose.2005.12.004.

Gabel, Detlev, Bertrand Liard, and Daren Orzechowski. 2015. “Cyber Risk: Why Cyber Security Is Important.” *White & Case LLP International Law Firm, Global Law Practice*. http://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz. 2003. *Practical UNIX and Internet Security*. “O’Reilly Media, Inc.” http://books.google.co.uk/books/about/Practical_UNIX_and_Internet_Security.html?id=t0IExLP-MPMC&pgis=1.

Gerring, John. 2004. “What Is a Case Study and What Is It Good For?” *American Political Science*

Review 98 (02). Cambridge University Press: 341–54. http://journals.cambridge.org/abstract_S0003055404001182.

Gersick, C. J. G. 1988. "TIME AN TRANSITION IN WORK TEAMS: TOWARD A NEW MODEL OF GROUP DEVELOPMENT." *Academy of Management Journal* 31 (1). Academy of Management: 9–41. doi:10.2307/256496.

Giddens, A. 2013. *The Consequences of Modernity*. https://books.google.com/books?hl=en&lr=&id=SVmkJEwWGwAC&oi=fnd&pg=PT45&dq=the+consequences+of+modernity+giddens&ots=5jmWlCQUKJ&sig=xM6ZuXZSCNpjRrYE3xJZajuxEOY.

Glaser, Barney G., Anselm L. Strauss, and Elizabeth Strutzel. 1968. "The Discovery of Grounded Theory; Strategies for Qualitative Research." *Nursing Research* 17 (4). http://journals.lww.com/nursingresearchonline/Citation/1968/07000/The_Discovery_of_Grounded_Theory__Strategies_for.14.aspx.

Graves. 2007. *The Twelve Caesars*. Penguin; Rev. Ed. / edition. http://www.amazon.co.uk/gp/product/B002RI9T64?btkr=1.

GRT. 2012. "British Intelligence Speaks Out On Cyber Threats." *GRT Corporation*. http://www.grtcorp.com/content/british-intelligence-speaks-out-cyber-threats.

Guba, Egon G., Lincoln, Y. S. 1994. "Competing Paradigms in Qualitative Research." In *Handbook of Qualitative Research*, 163–94.

Gurbaxani, VC, and CF Kemerer. 1999. *An Agency Theory View of the Management of End-User Computing*. *Pitt.edu*. An agency theory view of the management of end-user computing. Sloan School of Management, Massachusetts Institute of Technology, 1989. http://www.pitt.edu/AFShome/c/k/ckemerer/public/html/CK research papers/AgencyTheoryViewMgtEndUserComputing_GurbaxaniKemerer90.pdf.

Gurbaxani, Vijay Chandur. 2010. "An Agency Theory View of the Management of End-User Computing," July. General Books LLC. http://dl.acm.org/citation.cfm?id=1893144.

Hadnagy, C. 2010. *Social Engineering: The Art of Human Hacking*. https://books.google.co.uk/books?hl=en&lr=&id=9LpawpklYogC&oi=fnd&pg=PR13&dq=social+engineering+the+art+of+human+hacking&ots=vakyDPg5VT&sig=Mkqr-UkZ_qaeFHK-s-xW-saM64w.

Hagen, Janne Merete, Eirik Albrechtsen, and Jan Hovden. 2013. "Implementation and Effectiveness of Organizational Information Security Measures." *Information Management & Computer Security* 16 (4). Emerald: 377–97. http://cat.inist.fr/?aModele=afficheN&cpsidt=21201160.

Halderman, J. Alex, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A.

Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. 2009. “Lest We Remember.” *Communications of the ACM* 52 (5). ACM: 91. doi:10.1145/1506409.1506429.

Handy, Charles. 1999. “Trust and the Virtual Organization,” May. Harvard Business School Press, 107–20. http://dl.acm.org/citation.cfm?id=303444.303451.

Hart, SG, and LE Staveland. 1988. “Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research.” *Advances in Psychology*. http://www.sciencedirect.com/science/article/pii/S0166411508623869.

Hedström, Karin, Ella Kolkowska, Fredrik Karlsson, and J.P. Allen. 2011. “Value Conflicts for Information Security Management.” *The Journal of Strategic Information Systems* 20 (4): 373–84. doi:10.1016/j.jsis.2011.06.001.

Herath, Tejaswini, and H Raghav Rao. 2009a. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations.” *European Journal of Information Systems* 18 (2). Nature Publishing Group: 106–25. doi:10.1057/ejis.2009.6.

Herath, Tejaswini, and H.R. Rao. 2009b. “Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness.” *Decision Support Systems* 47 (2). Elsevier Science Publishers B. V.: 154–65. doi:10.1016/j.dss.2009.02.005.

Herley, Cormac. 2009. “So Long, and No Thanks for the Externalities.” In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop - NSPW ’09*, 133. New York, New York, USA: ACM Press. doi:10.1145/1719030.1719050.

Herley, Cormac. 2014. “More Is Not the Answer.” *IEEE Security & Privacy* 12 (1): 14–19. doi:10.1109/MSP.2013.134.

Higgins, Huong Go. 1999. “Corporate System Security : Towards an Integrated Management Approach.” *Information Management & Computer Security* 7 (5). Emerald: 217–22. http://cat.inist.fr/?aModele=afficheN&cpsidt=1972331.

Hine, Mike. 2014. “Remote Working Policies Causing Data Breach Risk.” *Infosecurity Magazine*. http://www.infosecurity-magazine.com/news/remote-working-policies-data-breach/#.VFo8VMgXKrA.facebook.

Holmstrom, Bengt. 1989. “Agency Costs and Innovation.” *Journal of Economic Behavior & Organization* 12 (3): 305–27. doi:10.1016/0167-2681(89)90025-5.

Höne, Karin, and J.H.P Eloff. 2002. “What Makes an Effective Information Security Policy?” *Network Security* 2002 (6): 14–16. doi:10.1016/S1353-4858(02)06011-7.

Hubbard, DW. 2010. *How to Measure Anything: Finding the Value of Intangibles in Business*. https://books.google.co.uk/books?hl=en&lr=&id=CBAh4eM-g3AC&oi=fnd&pg=PT11&dq=How+to+measure+anything:+Finding+the+value+of+intangibles+in

+business&ots=WLCdrhP0oH&sig=ggGhypR2FaM9Cmi2tBGIRx7zc_w.

IBM. 2014. “IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of Cyber Attack and Incident Data from IBM’s Worldwide Security Operations.”

IISP. 2007. “The IISP Code of Ethics.” https://www.iisp.org/imis15/iisp/Member/IISP_Code_of_Ethics.aspx.

Information Security Forum. *IRAM2: Information Risk Assessment Methodology 2*.

Inglesant, Philip G., and Martina Angela Sasse. 2010. “The True Cost of Unusable Password Policies.” In *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI ’10*, 383. New York, New York, USA: ACM Press. doi:10.1145/1753326.1753384.

Inglesant, Philip G., and Martina Angela Sasse. 2011. “Information Security as Organizational Power: A Framework for Re-Thinking Security Policies,” September. IEEE. http://discovery.ucl.ac.uk/1328206/1/STASTsanitised.pdf.

ISACA. 2009. “Risk IT Framework.”

ISACA. 2014. “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.” http://www.isaca.org/cobit/pages/default.aspx?cid=1003566&appeal=pr.

ISO 27000. 2014. “ISO 27000 - ISO 27001 and ISO 27002 Standards.” http://www.27000.org/.

ISO 27004. 2015. “Introduction to ISO 27004 / ISO27004.” *ISO 27004*. Accessed May 12. http://www.27000.org/iso-27004.htm.

ISO 31000. 2015. “ISO 31000 - Risk Management - ISO.” Accessed May 18. http://www.iso.org/iso/home/standards/iso31000.htm.

ISO 9241. 2015. “ISO 9241-210:2010 - Ergonomics of Human-System Interaction -- Part 210: Human-Centred Design for Interactive Systems.” *2010*. Accessed June 24. http://www.iso.org/iso/catalogue_detail.htm?csnumber=52075.

ISO/IEC 27005:2011: Information Technology -- Security Techniques -- Information Security Risk Management.

ITIL. 2014. “Information Technology Infrastructure Library.” http://www.itil-officialsite.com/.

James, H. L. 1996. “Managing Information Systems Security: A Soft Approach,” October. IEEE Computer Society, 10. http://dl.acm.org/citation.cfm?id=524432.857867.

Jannson, K., and R. von Solms. 2013. “Phishing for Phishing Awareness.” *Behaviour & Information Technology* 32 (4-6). Taylor & Francis: 584–93. http://cat.inist.fr/?aModele=afficheN&cpsidt=27465778.

Johnson, M. Eric, and Eric Goetz. 2007. “Embedding Information Security into the Organization.” *IEEE Security & Privacy Magazine* 5 (3). IEEE Educational Activities Department: 16–24. doi:10.1109/MSP.2007.59.

Joint Task Force Transformation Initiative. 2011. “SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View.” National Institute of Standards & Technology.

Karyda, Maria, Evangelos Kiountouzis, and Spyros Kokolakis. 2005. “Information Systems Security Policies: A Contextual Perspective.” *Computers & Security* 24 (3): 246–60. doi:10.1016/j.cose.2004.08.011.

Kelly, Thomas. 1998. “THE MYTH OF THE SKYTALE.” *Cryptologia* 22 (3). Taylor & Francis: 244–60. doi:10.1080/0161-119891886902.

Ken Blanchard. 2010. “Building Trust.” *Ken Blanchard Companies*. http://www.kenblanchard.com/img/pub/Blanchard-Building-Trust.pdf.

Kerckhoffs, Auguste. 1883. “La Cryptographie Militaire.” *Journal Des Sciences Militaires* 9: 5–38.

King, William R. 1978. “Strategic Planning for Management Information Systems.” *MIS Quarterly* 2 (1). Society for Information Management and The Management Information Systems Research Center: 27. doi:10.2307/249104.

Kirlappos, Iacovos, and Martina Angela Sasse. 2012. “Security Education against Phishing: A Modest Proposal for a Major Rethink.” *IEEE Security and Privacy Magazine*. http://discovery.ucl.ac.uk/1353958/.

Kirlappos, Iacovos, and Martina Angela Sasse. 2014. “What Usable Security Really Means: Trusting and Engaging Users.” *Human Aspects of Information Security, Privacy, …*. http://link.springer.com/chapter/10.1007/978-3-319-07620-1_7.

Kirlappos, Iacovos, Martina Angela Sasse, and Nigel Harvey. 2012. “Why Trust Seals Don’t Work: A Study of User Perceptions and Behavior.” In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7344 LNCS:308–24.

Klein, Heinz K., and Michael D. Myers. 1999. “A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems.” *MIS Quarterly* 23 (1). Society for Information Management and The Management Information Systems Research Center: 67. doi:10.2307/249410.

Knapp, Kenneth J., R. Franklin Morris, Thomas E. Marshall, and Terry Anthony Byrd. 2009. “Information Security Policy: An Organizational-Level Process Model.” *Computers & Security* 28 (7): 493–508. doi:10.1016/j.cose.2009.07.001.

Kraemer, Sara, Pascale Carayon, and John Clem. 2009. “Human and Organizational Factors in Computer

and Information Security: Pathways to Vulnerabilities." *Computers & Security* 28 (7): 509–20. doi:10.1016/j.cose.2009.04.006.

Kritzinger, Elmarie, and S. H. von Solms. 2005. "Five Non-Technical Pillars of Network Information Security Management." *Communications and Multimedia Security*, 277–87. http://link.springer.com/chapter/10.1007/0-387-24486-7_21.

Krol, Kat, Matthew Moroz, and Martina Angela Sasse. 2012. "Don't Work. Can't Work? Why It's Time to Rethink Security Warnings." In *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 1–8. IEEE. doi:10.1109/CRISIS.2012.6378951.

Kumaraguru, Ponnurangam, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. "School of Phish." In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 1. New York, New York, USA: ACM Press. doi:10.1145/1572532.1572536.

Lacey, David. 2011. "Things That Need to Change in Information Security Standards." *Computer Weekly*. http://www.computerweekly.com/blogs/david_lacey/2011/07/things_that_need_to_change_in.html.

Lapke, M, and G Dhillon. 2008. "Power Relationships in Information Systems Security Policy Formulation and Implementation." *ECIS*, 1358–69. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1182&context=ecis2008.

Lapke, M. 2008. "Power Relationships in Information Systems Security Policy Formulation and Implementation." *PhD Thesis, Virginia Commonwealth University*. http://www.researchgate.net/publication/221409146_Power_Relationships_in_Information_Systems_Security_Policy_Formulation_and_Implementation/file/9c960523912ad89ed2.pdf.

Laszka, Aron, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme. 2014. "Secure Team Composition to Thwart Insider Threats and Cyber-Espionage." *ACM Transactions on Internet Technology* 14 (2-3). ACM: 1–22. doi:10.1145/2663499.

Lee, Allen S., and Richard Baskerville. 2003. "Generalizing Generalizability in Information Systems Research." *Information Systems Research* 14 (3). INFORMS: 221–43. doi:10.1287/isre.14.3.221.16560.

Love, Linda F., and Parbudyal Singh. 2011. "Workplace Branding: Leveraging Human Resources Management Practices for Competitive Advantage Through 'Best Employer' Surveys." *Journal of Business and Psychology* 26 (2): 175–81. doi:10.1007/s10869-011-9226-5.

Martins, A, and J.H.P Eloff. 2002. "Information Security Culture." *Security in the Information Society IFIP Advances in Information and Communication Technology Volume 86, 2002, Pp 203-214*. http://dl.acm.org/citation.cfm?id=719826.

Mayer, RC, JH Davis, and FD Schoorman. 1995. “An Integrative Model of Organizational Trust.” *Academy of Management …*. http://amr.aom.org/content/20/3/709.short.

McDowell, Mindi. 2009. “Understanding Denial-of-Service Attacks.” *US-CERT*. https://www.us-cert.gov/ncas/tips/ST04-015.

Melik, James. 2011. “Fake Goods Save Money but at What Cost? - BBC News.” http://www.bbc.co.uk/news/business-16087793.

Mintzberg, Henry. 1985. “THE ORGANIZATION AS POLITICAL ARENA.” *Journal of Management Studies* 22 (2): 133–54. doi:10.1111/j.1467-6486.1985.tb00069.x.

Mitnick, Kevin D., and William L. Simon. 2002. *The Art of Deception: Controlling the Human Element of Security*. Wiley. http://books.google.co.uk/books/about/The_Art_of_Deception.html?id=VR_aVP0KKh8C&pgis=1.

Molotch, H. 2013. “Everyday Security: Default to Decency.” *Security & Privacy, IEEE*. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6682949.

Moore, AP, DM Cappelli, TC Caron, and E Shaw. 2011. “A Preliminary Model of Insider Theft of Intellectual Property.” *Technical Report, Carnegie Mellon University*. http://isyou.info/jowua/papers/jowua-v2n1-2.pdf.

Moore, G.E. 1998. “Cramming More Components Onto Integrated Circuits.” *Proceedings of the IEEE* 86 (1): 82–85. doi:10.1109/JPROC.1998.658762.

Morgan, MG. 2002. *Risk Communication: A Mental Models Approach*. http://books.google.co.uk/books?hl=en&lr=&id=ieXbkmYf3mAC&oi=fnd&pg=PR1&dq=risk+communication+a+mental+models+approach&ots=xMt6k35GSd&sig=-RxXKuDPidoKZoY4SZEgOVEMC94.

Morrison, EW, and SL Robinson. 1997. “When Employees Feel Betrayed: A Model of How Psychological Contract Violation Develops.” *Academy of Management Review*. http://amr.aom.org/content/22/1/226.short.

Mukherjee, Arjun, Bing Liu, and Natalie Glance. 2012. “Spotting Fake Reviewer Groups in Consumer Reviews.” In *Proceedings of the 21st International Conference on World Wide Web - WWW ’12*, 191. New York, New York, USA: ACM Press. doi:10.1145/2187836.2187863.

Muncaster, Phil. 2015. “Generation Z Predicts End to Passwords and PINs by 2020.” *Infosecurity Magazine*. http://www.infosecurity-magazine.com/news/generation-z-predicts-end/.

Nielsen, Jakob. 2010. “Mental Models and User Experience Design.” http://www.nngroup.com/articles/mental-models/.

Oxford Dictionary of English. 2010. Oxford University Press.

http://books.google.co.uk/books/about/Oxford_Dictionary_of_English.html?id=anecAQAAQBAJ&pgis=1.

Pahnila, Seppo, Mikko Siponen, and Adam Mahmood. 2007. “Employees’ Behavior towards IS Security Policy Compliance.” In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, 156b – 156b. IEEE. doi:10.1109/HICSS.2007.206.

Pallas, Frank. 2009. “Information Security Inside Organizations-A Positive Model and Some Normative Arguments Based on New Institutional Economics.” *Available at SSRN 1471801*.

Palmer, Malcolm E., Craig Robinson, Jody C. Patilla, and Edward P. Moser. 2001. “Information Security Policy Framework: Best Practices for Security Policy in the E-Commerce Age.” *Information Systems Security* 10 (2). Auerbach: 13–27. http://cat.inist.fr/?aModele=afficheN&cpsidt=980821.

Paulk, M.C., B. Curtis, M.B. Chrissis, and C.V. Weber. 1993. “Capability Maturity Model, Version 1.1.” *IEEE Software* 10 (4): 18–27. doi:10.1109/52.219617.

Pawson, Ray, and Nick Tilley. 1997. *Realistic Evaluation*. SAGE Publications Ltd.

Payne, Shirley C. 2009. “A Guide to Security Metrics.” *SANS Institute InfoSec Reading Room*. http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55.

PCI-DSS. 2014. “PCI Security Standard.” *PCI Standards Council*. https://www.pcisecuritystandards.org/.

Pelaez, Manuel Humberto Santander. 2010. *Measuring Effectiveness in Information Security Controls*.

Pfleeger, Shari Lawrence, and Deanna D. Caputo. 2012. “Leveraging Behavioral Science to Mitigate Cyber Security Risk.” *Computers & Security* 31 (4): 597–611. doi:10.1016/j.cose.2011.12.010.

Pfleeger, Shari Lawrence, and Martina Angela Sasse. 2015. *Studying Usable Security: How to Design and Conduct Case Studies*.

Pfleeger, Shari Lawrence, Martina Angela Sasse, and A Furnham. 2014. “From Weakest Link to Security Hero: Transforming Staff Security Behavior.” *Journal of Homeland Security …*. http://www.degruyter.com/view/j/jhsem.2014.11.issue-4/jhsem-2014-0035/jhsem-2014-0035.xml.

Pipkin, DL. 2000. *Information Security*. http://cds.cern.ch/record/1544490.

Ponemon Institute. 2014. “IBM 2014 Cost of Data Breach Study - United States.” IBM Corporation. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/.

Poulsen, K. 2000. “Kevin Mitnick Testifies before Congress. Mitnick to Lawmakers: People, Phones and Weakest Links.” http://www.politechbot.com/p-00969.html.

PSN. 2014. “PSN - Public Services Network - Groups - GOV.UK.” *Public Services Network Standard*. https://www.gov.uk/government/groups/public-services-network.

PwC. 2015. *Global State of Information Security Survey 2015*. http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml.

Resnick, P. 2001. "Beyond Bowling Together: Sociotechnical Capital." *HCI in the New Millennium*. http://drzaius.ics.uci.edu/meta/classes/informatics161_fall06/papers/15-ResnickSTK.pdf.

Riegelsberger, Jens, Martina Angela Sasse, and John D. McCarthy. 2005. "The Mechanics of Trust: A Framework for Research and Design." *International Journal of Human-Computer Studies* 62 (3). Academic Press, Inc.: 381–422. doi:10.1016/j.ijhcs.2005.01.001.

Rogers, Yvonne, Helen Sharp, and Jenny Preece. 2011. *Interaction Design: Beyond Human - Computer Interaction*. Vol. 6. John Wiley & Sons. http://books.google.co.uk/books/about/Interaction_Design.html?id=b-v_6BeCwwQC&pgis=1.

Rousseau, Denise M. 1989. "Psychological and Implied Contracts in Organizations." *Employee Responsibilities and Rights Journal* 2 (2): 121–39. doi:10.1007/BF01384942.

Rudolph, K. 2006. "Security Awareness and Privacy Training Courses and Programs." *Native Intelligence, Inc.* http://www.nativeintelligence.com/ni-programs/metrics-04.asp.

Runeson, Per, and Martin Höst. 2008. "Guidelines for Conducting and Reporting Case Study Research in Software Engineering." *Empirical Software Engineering* 14 (2): 131–64. doi:10.1007/s10664-008-9102-8.

Saltzer, J.H., and M.D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63 (9): 1278–1308. doi:10.1109/PROC.1975.9939.

Sarbanes-Oxley Act. 2002. "Public Law No. 107-204." *Washington, DC: Government Printing Office*. https://scholar.google.co.uk/scholar?q=sarbanes+oxley&btnG=&hl=en&as_sdt=0%2C5#0.

Sasse, Martina Angela, Debi Ashenden, and D Lawrence. 2007. "Human Vulnerabilities in Security Systems." *Human Factors Working Group, Cyber Security KTN Human Factors White Paper*. http://scholar.google.co.uk/scholar?hl=en&q=Human+Vulnerabilities+in+Security+Systems&btnG=&as_sdt=1,5&as_sdtp=#0#0.

Sasse, Martina Angela, Sacha Brostoff, and Dirk Weirich. 2001. "Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal* 19 (3). Kluwer Academic Publishers: 122–31. doi:10.1023/A:1011902718709.

Sasse, Martina Angela, and Ivan Flechais. 2005. "Usable Security: Why Do We Need It? How Do We Get It?" *In Cranor, L. F., Garfinkel, S. (Eds.). Security and Usability: Designing Secure Systems That People Can Use*, 13–30. http://discovery.ucl.ac.uk/20345/.

Sasse, Martina Angela, and Iacovos Kirlappos. 2014. "Design for Trusted and Trustworthy Services: Why We Must Do Better." *Trust, Computing, and Society*. https://books.google.co.uk/books?hl=en&lr=&id=ZtbSAgAAQBAJ&oi=fnd&pg=PA229&dq=kirla

ppos+sasse&ots=mev9tGgDaF&sig=KHTLV5t6pz5ATMXEMnRu-9M_-wc.

Sasse, Martina Angela, M Steves, Kat Krol, and D Chisnell. 2014. “The Great Authentication Fatigue – and How to Overcome It,” July. Springer International Publishing. http://discovery.ucl.ac.uk/1434817/1/The_Great_Authentication_Fatigue_Sasse_Krol.pdf.

Saunders, Dominic. 2012. “4 Reasons Security Policies Fail, And 7 Steps to Make Sure They Don’t.” *Insurance & Technology*. http://www.insurancetech.com/security/4-reasons-security-policies-fail-and-7-steps-to-make-sure-they-dont/d/d-id/1313985?

Schaub, Florian, Ruben Deyhle, and Michael Weber. 2012. “Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms.” In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia - MUM ’12*, 1. New York, New York, USA: ACM Press. doi:10.1145/2406367.2406384.

Schechter, S.E., R. Dhamija, A. Ozment, and I. Fischer. 2007. “The Emperor’s New Security Indicators.” In *2007 IEEE Symposium on Security and Privacy (SP ’07)*, 51–65. IEEE. doi:10.1109/SP.2007.35.

Schein, EH. 2010. *Organizational Culture and Leadership*. https://books.google.co.uk/books?hl=en&lr=&id=kZH6AwTwZV8C&oi=fnd&pg=PR9&dq=Organizational+Culture+and+Leadership&ots=9nd_jBAqPi&sig=PD9jGOjf511DHzEguSYpUbKEHLs.

Schlienger, Thomas, and Stephanie Teufel. 2003. “Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture,” September. IEEE Computer Society, 405. http://dl.acm.org/citation.cfm?id=942790.942977.

Schneier, Bruce. 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley. http://books.google.co.uk/books/about/Applied_cryptography.html?id=6NdQAAAAMAAJ&pgis=1.

Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*. John Wiley. http://books.google.co.uk/books/about/Secrets_and_lies.html?id=eNhQAAAAMAAJ&pgis=1.

Schneier, Bruce. 2012. *Liars and Outliers: Enabling the Trust That Society Needs to Thrive*. https://books.google.co.uk/books?hl=en&lr=&id=lPsbhIUexo0C&oi=fnd&pg=PA122&ots=8_LTx8mdjR&sig=dR1Ne61hPAcZja0iHK_noa9BB28.

Schwarz, Michiel, and Michael Thompson. 1990. *Divided We Stand: Re-Defining Politics, Technology and Social Choice*. University of Pennsylvania Press. http://books.google.com/books?hl=en&lr=&id=KPuUYqbU91MC&pgis=1.

Sheng, Steve, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. “Anti-Phishing Phil.” In *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS ’07*, 88. New York, New York, USA: ACM Press. doi:10.1145/1280680.1280692.

Silowash, GJ, DM Cappelli, and AP Moore. 2012. “Common Sense Guide to Mitigating Insider Threats.” http://repository.cmu.edu/sei/677/.

Siponen, Mikko. 2006. “Information Security Standards Focus on the Existence of Process, Not Its Content.” *Communications of the ACM* 49 (8). ACM: 97. doi:10.1145/1145287.1145316.

Siponen, Mikko, and Robert Willison. 2009. “Information Security Management Standards: Problems and Solutions.” *Information & Management* 46 (5): 267–70. doi:10.1016/j.im.2008.12.007.

Smetters, D. K., and Nathan Good. 2009. “How Users Use Access Control.” In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS ’09*, 1. New York, New York, USA: ACM Press. doi:10.1145/1572532.1572552.

Smith, Andrew. 2009. “Nigerian Scam E-Mails and the Charms of Capital.” *Cultural Studies* 23 (1). Taylor & Francis: 27–47. http://cat.inist.fr/?aModele=afficheN&cpsidt=20987116.

Smith, Michael. 2004. *Station X: The Codebreakers of Bletchley Park*. Pan. http://books.google.co.uk/books/about/Station_X.html?id=Wv4mSVDtA-wC&pgis=1.

Stajano, Frank, and Paul Wilson. 2011. “Understanding Scam Victims.” *Communications of the ACM* 54 (3). ACM: 70. doi:10.1145/1897852.1897872.

Stewart, Geordie, and David Lacey. 2013. “Death by a Thousand Facts,” April. Emerald Group Publishing Limited. http://www.emeraldinsight.com/doi/full/10.1108/09685221211219182.

Stoneburner, G, A Goguen, and A Feringa. 2002. “Risk Management Guide for Information Technology Systems.” *Nist Special Publication 800.30 (2002): 800-30*. http://www.security-science.com/pdf/risk-management-guide-for-information-technology-systems.pdf.

Stone-Gross, B, R Abman, Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Vigna Giovanni. 2013. “The Underground Economy of Fake Antivirus Software.” *Economics of Information Security and Privacy* 3: 55–78. http://link.springer.com/chapter/10.1007/978-1-4614-1981-5_4.

Strauss, Anselm, and Juliet M. Corbin. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications. http://books.google.co.uk/books/about/Basics_of_Qualitative_Research.html?id=wTwYUnHYsmMC&pgis=1.

Symantec. 2014. “Data Loss Prevention (DLP) Software.” http://www.symantec.com/en/uk/data-loss-prevention.

Taleb, Nassim Nicholas. 2010. *The Black Swan:: The Impact of the Highly Improbable: With a New section:“On Robustness and Fragility.” Random House*. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Black+Swan:The+Impact+of+the+Highly+Improbable:+With+a+new+section:+“On+Robustness+and+Fragility”#1.

Tan, Yao-Hua, and Walter Thoen. 2000. “Toward a Generic Model of Trust for Electronic Commerce.” *International Journal of Electronic Commerce* 5 (2). M. E. Sharpe, Inc.: 61–74. http://dl.acm.org/citation.cfm?id=1287018.1287024.

Thomas, G. 2011. “A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure.” *Qualitative Inquiry* 17 (6): 511–21. doi:10.1177/1077800411409884.

Thomson, Kerry-Lynn, and R. von Solms. 2005. “Information Security Obedience: A Definition.” *Computers & Security* 24 (1): 69–75. doi:10.1016/j.cose.2004.10.005.

Thomson, Kerry-Lynn, R. von Solms, and Lynette Louw. 2006. “Cultivating an Organizational Information Security Culture.” *Computer Fraud & Security* 2006 (10): 7–11. doi:10.1016/S1361-3723(06)70430-4.

Thomson, ME, and R Von Solms. 1997. “An Effective Information Security Awareness Program for Industry.” *Proceedings of the WG*. http://scholar.google.co.uk/scholar?hl=en&q=An+effective+information+security+awareness+program+for+industry&btnG=&as_sdt=1%2C5&as_sdtp=#0.

Trochim, William M.K. 1985. “Pattern Matching, Validity, and Conceptualization in Program Evaluation.” *Evaluation Review* 9 (5): 575–604. doi:10.1177/0193841X8500900503.

Trochim, William. 2006. “Pattern Matching for Construct Validity.” *Research Methods Knowledge Base*. http://www.socialresearchmethods.net/kb/pmconval.php.

Trompeter, C.M., and J.H.P Eloff. 2001. “A Framework for the Implementation of Socio-Ethical Controls in Information Security.” *Computers & Security* 20 (5): 384–91. doi:10.1016/S0167-4048(01)00507-7.

Tuyls, Pim, Boris Skoric, and Tom Kevenaar. 2007. “Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting,” October. Springer-Verlag New York, Inc. http://dl.acm.org/citation.cfm?id=1324776.

UCL. 2011. “UCL Information for Current Students: Plagiarism 2011.” http://www.ucl.ac.uk/silva/current-students/guidelines/policies/plagiarism.

UK Cabinet Office. 2014. “Keeping the UK Safe in Cyber Space - Policy.” https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace.

US-CERT. 2015. “Tips.” https://www.us-cert.gov/ncas/tips.

Van Niekerk, Johannes Frederick. 2007. “Establishing an Information Security Culture in Organizations : An Outcomes Based Education Approach.” http://dspace.nmmu.ac.za:8080/jspui/handle/10948/164.

von Solms, Basie. 2006. “Information Security – The Fourth Wave.” *Computers & Security* 25 (3): 165–68. doi:10.1016/j.cose.2006.03.004.

von Solms, Basie, and R. von Solms. 2005. “From Information Security To…business Security?” *Computers & Security* 24 (4): 271–73. doi:10.1016/j.cose.2005.04.004.

Vroom, Cheryl, and R. von Solms. 2004. “Towards Information Security Behavioural Compliance.” *Computers & Security* 23 (3). Elsevier Advanced Technology Publications: 191–98. doi:10.1016/j.cose.2004.01.012.

Walsham, Geoff. 1993. “Interpreting Information Systems in Organizations,” January. John Wiley & Sons, Inc. http://dl.acm.org/citation.cfm?id=583196.

Wash, Rick. 2010. “Folk Models of Home Computer Security.” In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS ’10*, 1. New York, New York, USA: ACM Press. doi:10.1145/1837110.1837125.

Weirich, Dirk. 2005. “Persuasive Password Security.” *Doctoral Dissertation, University College London*.

Weirich, Dirk, and Martina Angela Sasse. 2001. “Pretty Good Persuasion.” In *Proceedings of the 2001 Workshop on New Security Paradigms - NSPW ’01*, 137. New York, New York, USA: ACM Press. doi:10.1145/508171.508195.

Whitman, Michael, and Herbert Mattord. 2011. *Principles of Information Security*. Cengage Learning. http://books.google.co.uk/books/about/Principles_of_Information_Security.html?id=L3LtJAxcsmMC&pgis=1.

Whitten, Alma, and J. D. Tygar. 1999. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0,” August. USENIX Association, 14. http://dl.acm.org/citation.cfm?id=1251421.1251435.

Williams, Patricia A H. 2008. “When Trust Defies Common Security Sense.” *Health Informatics Journal* 14 (3): 211–21. doi:10.1177/1081180X08092831.

Winch, Jessica. 2014. “One in 10 Consumer Problems on eBay Are Scams, Says Citizens Advice.” http://www.telegraph.co.uk/finance/personalfinance/money-saving-tips/10942767/Scammers-steal-thousands-from-Gumtree-and-eBay-shoppers.html.

Winkler, Ira. 1997. *Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do about It*. Prima Pub. http://books.google.co.uk/books/about/Corporate_Espionage.html?id=ge7a68kDIXEC&pgis=1.

Wong, Caroline. 2011. *Security Metrics, A Beginner’s Guide*. http://www.amazon.co.uk/Security-Metrics-A-Beginners-Guide/dp/0071744002.

Wood, Charles Cresson. 2000. “An Unappreciated Reason Why Information Security Policies Fail.” *Computer Fraud & Security* 2000 (10): 13–14. doi:10.1016/S1361-3723(00)10029-6.

Yin, Robert K. 2009. *Case Study Research: Design and Methods*. SAGE Publications. http://books.google.co.uk/books/about/Case_Study_Research.html?id=FzawIAdilHkC&pgis=1.

Zurko, Mary Ellen, and Richard T. Simon. 1996. “User-Centered Security.” In *Proceedings of the 1996 Workshop on New Security Paradigms - NSPW ’96*, 27–33. New York, New York, USA: ACM Press. doi:10.1145/304851.304859.

Appendix A: Related Publications

Chapter 4:

Kirlappos, I., Beautement, A., Sasse, M.A. (2013). Comply or Die Is Dead: Long Live Security-Aware Principal Agents. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).7862 LNCS. doi:10.1007/978-3-642-41320-9_5.

Chapters 5 and 7:

Kirlappos, I., Parkin, S., Sasse, M.A. (2014). Learning from 'Shadow Security': Why understanding noncompliant behaviors provides the basis for effective security. Workshop on Usable Security San Diego, California. doi:10.14722/usec.2014.23.

Kirlappos, I., Parkin, S., Sasse, M.A. (2015). "Shadow security" as a tool for the learning organization. ACM SIGCAS Computers and Society, 45 (1), 29-37. doi:10.1145/2738210.2738216

Chapters 6 and 7:

Kirlappos, I., Sasse, M.A. (2014). What Usable Security Really Means: Trusting and Engaging Users. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).8533 LNCS. doi:10.1007/978-3-319-07620-1_7.

Sasse, M.A., Kirlappos, I. (2014). Design for Trusted and Trustworthy Services: Why We Must Do Better. In Trust, Computing, and Society. (pp. 229-249). Cambridge University Press.

Kirlappos, I., Sasse, M.A. (2015). Fixing Security Together: Leveraging trust relationships to improve security in organizations. USEC 2015 San Diego, California

Appendix B: Sample interview questions

Interview topics

Introductory Questions

1. What do you do at the organisation?
2. How long have you been working at the organisation?
3. What does your usual day involve?

Security Awareness

1. How does security fit in to your day?
2. Do you think your work has any security implications?
3. Do you encounter information that is in any sense confidential or sensitive?

Clear Desk Policy

1. Is there a policy that says what you should do with your desk when leaving in the evening?
2. Do you have a secure draw or storage area you can use?
3. Do you ever work on paper at all?

Laptops, Remote working and Removable Media

1. Do you ever use a laptop in the course of your work?
2. How do you share information with colleagues?
3. Do you ever use removable storage devices such as USB sticks?
4. When working from home what systems or technologies do you use?

Leadership and Management Roles

1. Do you supervise any other people?
2. Does your supervisor ever mention security issues to you?

Policies, Reporting and Training

1. How much would you say you know about the security policies at the organisation?
2. Have you ever received any security training?
3. Do you think people generally follow the policy rules?
4. Who would you report a security concern to?
5. What do you think of the use of Yammer at the organisation
6. Is anything security related every posted on Yammer?
7. Have you ever posted anything security related on Yammer?

Optional Topics

1. Compliance and security culture
2. Personal/mobile devices
3. Locking screens
4. Password behaviour

5. Password resets
6. Physical security
7. Customer data
8. Data classification
9. Trust

Sample of detailed interview questions (to aid interviewers)

Job/role description

1. What is your Job Description?
    a. What does your job involve?
2. How long have you been doing this job?
    a. How long you've been at the organisation?
3. How does security fit in to your day?
4. What is your background?

Security awareness

1. In the course of your work do you encounter information which is in any sense confidential?
2. Do you think your work has any implications for the security of the organisation?
3. What would be your main security concern?
    a. Are there any other concerns you can think of?
4. Could your work be misused by malicious individuals?
    a. Are you mainly concerned by competitors or by others?
    b. Do you think it is possible that a member of the organisation might pose a threat?

Clear Desk policy

1. Is there a policy that says what you should do with your desk when leaving in the evening?
2. Do you have a secure drawer which is just for your use?
3. Do you work on paper at all?
    a. Do you have papers on your desk?
    b. Do any of them contain information that might be useful to a competitor or that might be considered confidential?
4. Do you use a laptop or desktop in the office?
    a. Do you leave your laptop on your desk when going for lunch?
    b. Is it locked physically?
    c. What do others do with their laptops?
5. Is it password protected?
    a. Just on start-up or is there an automatic password-protected screensaver?

File Sharing and Removable computer media

1. Do you ever share information that is confidential?
2. How do you do this?
    a. To someone inside the company?
    b. To someone outside the company?
3. Do you ever use removable storage devices, such as USB sticks?
4. Is that your own one or was it given to you by the organisation?
    a. Is it just for your use or is it shared by the office?
5. What sort of uses do you have for that?
    a. How important is it to you to be able to use [storage devices] at work?

6. Do you take data home on it?
7. So when you're at home working do you have to use the company laptop or can you take data home on the [storage device] and use it on your personal computers?
8. Was any of this data in any sense confidential?
9. What precautions do you take to protect that data?
10. Is that common in the organisation?

Laptop use

1. Do you ever take a laptop home with you?
2. Is this for working from home or for something else?
    a. How often do you do this?
3. When you take the laptop home what is your usual form of transport?
4. Do you go straight home or do you take your laptop to other locations, for example the gym?
5. Do you think that is the general practice for other colleagues as well?
6. Do you ever have any concerns that it might be lost or stolen?
7. Is there any confidential data stored locally on the laptop itself?
8. Do you store any other information locally or do you mostly use a shared file store?
9. Do you take regular backups?
10. Do you use your own file store somewhere?
11. On your laptop, can you install your own software on it or is it managed by the organisation?
    a. Have you ever installed any software other than that provided by the organisation?
    b. Did you take any precautions when doing so?
12. What's the general view amongst employees on installing software on laptops by yourself?
13. When you take it home can you access your work from home?
14. Would you be accessing a company service from home to do this?
15. What's the process for doing that?
16. Is that any extra procedure compared to what you have to do in the office?
    a. So, when you are in the office what do you have to do? Do you have to log on to the laptop itself or connect to another system?
17. Is it the same password that you use when you're in the office?
18. Are you on the company network once you've done that or is there another password?
19. How do you manage when there is a service outage?

Supervising others

1. Are you responsible for anybody else? Do you supervise anybody else?
2. Are you responsible of making sure that they are aware of the general security procedures and policies?
3. When someone you supervise leaves their organisation I presume they have their access rights revoked?
    a. Are old accounts ever used in the organisation?
4. Do you need to take some action for this to happen?
5. Who supervises you?
6. Do you think your supervisor is concerned with whether you comply with security processes or not?

7. Do they ever mention security issues to you?

Security policies and Training

1. How much would you say you know in general about the security policies?
    a. Do you think in general the policies are well known?
2. Have you had any training about it recently?
    a. Was it new information or just a refresher?
3. How long was that? Was that a day or less than a day?
4. Was it computer based?
5. Was it more actually training or just information delivery?
6. Did everybody in your team do that?
7. Can you remember anything specific that was in it? Any particular points?
8. Were you given any other sort of security training?
9. Are you aware of anything being done to keep people aware of security?
10. How long do security training sessions last for?
11. And do people tend to go to them?
12. Do you receive emails bulletins about security, perhaps reminding you to do a certain thing?
13. Who would you report a security concern to?
14. What do you think of the use of Yammer at the organisation?
    a. Do you use it yourself?
15. Is anything related to security ever posted on Yammer?
16. Have you ever posted anything security related on Yammer?
17. Do they put notices around the company, on notice boards and such like?
18. And does it ever get mentioned in team talks or meetings?
19. Were you aware of any kind of vetting going on, such as people checking your criminal records?

Compliance

1. Would you say the people follow all of the rules all the time in terms of security? Or most people follow them most of the time? Or somewhere in between?
2. Can you think of a reason why somebody might not follow one of them?
3. Are there any policies or procedures that you routinely don't comply with?
    a. Why do you do this?
4. Would people get reprimanded for anything like that, for example if somebody was in the habit of not putting the lock on the screen when they left their desk?
5. Does the organisation check whether employees comply with security policies?
6. So how would someone get caught if they did not follow those?
7. What sanctions or punishments are used against people that get caught?
    a. Do you think these are appropriate?
8. What risks do you think failing to comply with security policy poses to the organisation?
9. What do you do when someone doesn't follow the security policy?
10. Would you report them?
11. Have you ever come across something that you consider to be a vulnerability that the organisation hasn't thought of?

12. What do you think about the security culture in general? Do you think it's quite a security conscious organisation or not very security conscious?
13. In general what do you think of the policies? Do you think they are too strict, too soft, or about right?
14. How would you say that the Information Security compares with other issues, such as health and safety, or carbon reduction, that the organisation also cares about?

Password behaviour

1. Are you the only one that uses your password?
2. Have you ever shared it with anybody else?
3. Do any of your systems use shared passwords or anything like that?
4. How many different systems or services do you use that require a password?
5. Are the passwords you use all the same or are they all different?
6. When a change is required do you change them all at the same time?
    a. Even if they don't all have to be changed at the same time?
7. How often do you need to change your passwords?
8. Do you ever change your password without being prompted to?
9. Did you invent the passwords you use yourself or are they given to you?
    a. Do you have any system for creating new passwords?
    b. Do you create completely new passwords or do you modify your old one, perhaps by incrementally adding to a number in it?
10. Are there any restrictions, such as it has to have capital letters or certain characters?
11. Are you allowed to re-use the same password when you have to reset it?
    a. What about similar passwords but perhaps with a single letter or number changed?
12. So would a typical password be a word with a capital letter at the beginning with a number at the end or something like that?
    a. Is the number on the end something you change when you need to update your password?
13. How do you remember these passwords?
14. Do other people share their passwords to get access to systems?
    a. How often does that happen?

Customer data

1. Do you take any special precautions when dealing with customer data?
    a. What about when it is on a removable storage device?
2. Do you share customer data with your colleagues?
3. Are there guidelines regarding with whom you should share the data?
4. Have you ever refused to pass some information to someone in the organisation?
5. Have others refused to provide you with any information you needed for your work?

Personal devices

1. Do you connect personal devices to the company network?
2. Is the process different than for corporate ones?
3. Are there any particular properties of features your device must have to be used on the network?

4. Is it a common practice to bring in your own devices amongst the employees?

Lock Screen and Confidential Information

1. When you leave your desk do you always lock your workstation?
    a. Even if it's just for a cup of coffee?
2. Is there ever confidential information on your screen that somebody could perhaps see if they're walking through the office?
3. Within the office where you work, are there people you don't know who might be able to perhaps see over your shoulder if they were wandering around?
4. Do you personally do anything to prevent this from happening?
5. Do people around you tend to lock their screens when leaving their desks?
    a. How often do you see unlocked screens?
6. Have you ever seen confidential information on someone else's screen?
    a. Was this information you had access to yourself?
    b. How often does this happen?
7. Is there any information that some people in your team have access to but others don't?
    a. Is that controlled by your password?

Helpdesk

1. Have you ever forgotten your password and had to have it reset?
2. What's the process for doing that?
    a. Is it automated or do you need to speak to a helpdesk or the IT department?
    b. Do you think they might be able to see your password?
3. What sort of procedures do they ask you to go through for checking that you are who you say you are before you reset it?
4. Does that happen often in the organisation? Do others need to get resets often?
5. Apart from changing passwords have you had any other dealings with a helpdesk for any reason?
6. So where are they physically located? Is it somebody in the office are they outside the organisation?
    a. So there isn't somebody locally that you can go and see if you want something done quickly?

Data Classification

1. Does the organisation have any data classification scheme?
2. How is the classification done? Who assigns those?
3. What is the difference between classification levels?
4. If you need to share some information with a colleague, do you check that they are eligible to view that information?
5. Did you ever need to access some information that you were not allowed to?
    a. How did you get access?
6. Do you pass information to colleagues over the phone?
    a. How do you verify who they are?
7. Is it common to share information through the phone?
8. Do you share classified information via email?

    a. To someone outside the company?
9. Do you use any shared folders for collaboration purposes?
10. Do you check the access rights of members before putting something there?
11. Can you set file permissions yourself?
12. Do you know who can change permissions, or what the procedure is?
    a. How long does this usually take?
13. Are people happy to share information in there or do they worry about security a lot?

Website/email access

1. Do you have access to a shared area and your own personal space?
    a. What else do you have access to?
2. Are certain kinds of email blocked, for example if it is too big?
    a. Are there other rules and restrictions around email use?
3. Have you received emails from colleagues that they shouldn't have sent?
4. Have you ever fallen foul of the rules or had anything blocked or undelivered?
5. Have you ever heard of anybody being reprimanded for inappropriate email use for example?
6. Do you do any casual browsing (e.g. personal email, news) while on company networks?
7. Are there certain web pages that you can't access?
8. Is there ever an occasion where you legitimately have a need for getting onto something and find you can't?
    a. Have you ever used a workaround to get passed the restriction?
    b. Do you know if other people do?
    c. How often does this happen?

Physical security

1. What about the physical security. How do you enter this site here for example?
2. Can you see a way someone could get into the building without authorisation?
3. Do you wear your passcard all the time?
4. How easy is it for somebody to walk in from the street?
    a. Have you seen anyone tailgating in to the building?
    b. How often does this happen?
    c. Would you stop them if you noticed it happening?
5. Is there any other security to prevent them moving between the different blocks, for example?
    a. Have you observed tailgating inside the building?
    b. How often does it happen?
    c. Would you confront someone if you saw them doing it?
6. Have you ever bypassed any of the building's physical security?
7. If you notice somebody that you didn't recognise without a passcard would you challenge them or something? I mean, somebody came and sat down in one of your colleague's desks or anything like that? Would you think they're a hot-desker from another office? Or would you wonder who they are?
8. Did you have, sort of, hot-desking spaces in the office that people who are visiting would use?

General ISec Issues

1. Have you got any other thoughts about the Information Security here that we haven't covered?
2. In general would you say you trust your colleagues and the other people and around the offices?

Appendix C: Individual responses to risk

Schwarz and Thompson (1990) work on politics, technology and social choice present four commonly-encountered responses to risk, labelled as the *individualist*, *fatalist*, *hierarchist* and *egalitarian*, presented here in the form adapted by Adams (1995).

Individualists: Enterprising 'self-made' people, relatively free from control by others, and who strive to exert control over their environment and the people in it. Their success is often measured by their wealth and the number of followers they command. They are enthusiasts for equality of opportunity, oppose regulation and when they need moral justification of their activities, they believe that self-interested behaviour in a free market operates to the benefit of all. Nature, according to this perspective, is to be commanded for human benefit.

Egalitarians: They have strong group loyalties but little respect for externally imposed rules, other than those imposed by nature. They believe human nature is – or should be – cooperative, caring and sharing, and believe in trust and fairness. Group decisions should be made by direct participation of all members, and leaders should rule by the force of their arguments. The solution to the world's environmental problems is to be found in voluntary simplicity. Nature is to be obeyed and respected and interfered with as little as possible.

Hierarchists: They inhabit a world with strong group boundaries and binding prescriptions, with hierarchical social relationships, where with everyone knowing his or her place. The hierarchy certifies and employs the scientists whose intellectual authority is used to justify its actions. They are devotees of cost–benefit analysis and nervous in the presence of uncertainties that preclude the possibility of attaching uncontested numbers to the variables they are supposed to be managing.

Fatalists: have minimal control over their own lives and belong to no groups responsible for the decisions that rule their lives. They are resigned to their fate and see no point in attempting to change it. Nature is to be endured and, when it's your lucky day, enjoyed. Their risk management strategy is to buy lottery tickets and duck if they see something about to hit them.

Appendix D: Security Behaviour Maturity Model

(adapted from Paulk et al., 1993 by Adam Beautement)

When considering a Security Behaviour version of this model we must consider how to convert these organisational indicators to ones of personal behaviour. The cleanest way to do this is to consider how the individual is managing or motivating their own behaviour – what factors are they considering when planning their security actions. At the highest level they will be actively working toward an improved and improving security culture. At the lower levels employees will be following the policy by rote (possible reluctantly, ineffectively or incompletely) or simply taking actions as they see fit, based on their own internal security model with no input from the organisation. The following levels represent this range of behaviours.

Level 1 – Uninfluenced: At this level user behaviour is mediated only by their own knowledge, instincts, goals and tasks. Their actions will reflect only the needs of their primary task and will only deviate from that where their internal security schema conflicts with those actions. While some members of the organisation may be sufficiently knowledgeable to act securely it is expected that employees at this level will introduce a range of vulnerabilities in to the system. In practice this level can only exist where employees are working on non-organisational systems, as even the act of logging in to a managed network means that organisational security is exerting an influence.

Level 2 – Technically Controlled: Employees at this level act as in Level 1 except where technical controls exist that enforce policy on a case-by-case basis. Technically controlled employees will follow their own security rules except where they must use organisational systems in the execution of their primary task, and those systems enforce policy at the software or hardware level. Realistically this is the lowest practical level that employees working in an office environment could function at.

Level 3 – Ad-Hoc Knowledge and Application: Employees at Level 3 follow policy without necessarily a deep knowledge of what it contains. Their security knowledge comes from the 'best practise' or habits associated with their work environment, rather than from being aware of, and understanding, organisational policy.

Level 4 – Policy Compliant: Level 4 behaviour demonstrates knowledge and understanding of the policy, and compliance with it, even in situations where the local work environment may include the use of workarounds and frequently made excuses. At Level 4 employees can be considered to be useful role models and guides for security culture within the organisation.

Level 5 – Active Approach to Security: At Level 5 employees take an active role in the promotion and advancement of security culture within the organisation. The serve not just the letter of the policy but the intent as well and will challenge breaches at their level appropriately. They see security as a valuable part of the function of the organisation and have internalised this motivation. Level 5 employees are not security zealots, but rather understand the need to balance the security and business processes and champion the cause of security intelligently and effectively.

Appendix E: Survey scenario topics

Scenario A – File Sharing

Jessica, a Business Analyst at a utility company, needs to share a large volume of files with colleagues in her department as part of a high priority task she is undertaking. These files contain “Confidential” company information for “internal use only”. Jessica has made the files available through Microsoft SharePoint, restricting access to certain team members. Some team members tell her they cannot access the files due to incorrect permissions, so Jessica has submitted a request for changes to be made to her colleagues’ permissions and escalated this due to the urgency. However, she knows from past experience that it may take up to 1 week for the changes to be approved and applied. If these files are not made available within the next 2 working days, this will severely impact delivery and quality. As not all of her colleagues require access to all the files, to manually distribute them would involve her identifying the subset of files for each person - this will be a very time-consuming task, so Jessica creates an archive of all the relevant documents and considers how best to deliver it to the group.

1. **Option A**: Request that those with access share their (main log-in) account details and passwords with those without to allow them access to the information.
2. **Option B**: Burn a copy of the files onto a CD/DVD and distribute to the work group.
3. **Option C**: Email the document archive directly to the general work group mailing list using your company email address.
4. **Option D**: Move the files to an unrestricted folder on the internal network to allow the work group to have continued access to it.

Scenario B – Managing Permissions

John is a System Administrator at a utility company responsible for deciding who has access to confidential information. John normally reviews each request and then applies the most appropriate permissions, or the request is denied according to established procedures and guidelines. He undertakes this task every 24 hours to ensure there is no risk of maintenance schedules slipping due to a lack of access to records. John is called away from the office on short notice by a family emergency and he is concerned about how this task will be managed during his absence. The system used to set the permissions does not easily allow him to deputise the task to another account, so he must find another way to ensure this activity is completed while he is away. He is also concerned that as the guidelines are not always clear and require some degree of discretion when granting access, deputising the task may mean there is a higher risk of incorrect permissions being granted. This makes the choice of who to trust this task to in his absence an important one.

1. **Option A**: Leave your password with your secretary, who although temporary, is a trusted employee, with instructions to use your account to resolve "emergency situations". 26
2. **Option B**: Leave your password with a trusted member of the department and ask them to handle "all decision making" while you are away.

3. **Option C**: Grant blanket access rights to the whole department (clone of the permissions of an individual with the most access rights) for the duration of your absence to forestall many of the access requests you are usually is asked to deal with.
4. **Option D**: Give out login details of a range of access permissions (used by temporary workers) with instructions that they be used where existing permissions do not allow access.

Scenario C – USB Stick Usage

Jason works for a utility company as a Commercial Analyst and is currently involved in an important project that requires him to present progress updates to clients, often in offsite locations. Jason would normally use his laptop to take presentations to clients but his laptop is currently in for maintenance. Instead he decides to use an encrypted USB memory stick to transfer the required files to the client site. Unfortunately, shortly before he is due to leave for the meeting, Jason realises he lent out his encrypted USB stick and cannot recall who to. He knows he will not get a replacement at such short notice. In the meantime he still needs some way to transfer information. The presentation includes embedded media and is therefore too large to email and he knows that offsite locations cannot access the internal network.

1. **Option A**: Take the required data on an unencrypted USB stick - you have one to hand.
2. **Option B**: Borrow an encrypted stick from a colleague. You would have to also make a note of their password so you can access the data at the client's site. The colleague had asked that you do not share / erase the confidential data already on the stick.
3. **Option C**: An employee of the client has been visiting the utility company and is due to travel back with you. Use the available unencrypted stick to put a copy of the data onto their laptop and ask them to take it to the client's site.
4. **Option D**: Upload the files to a public online data storage service and recover them at the client's site.

Scenario D – Tailgating

Agnes works for a utility company as a Customer Account Manager and often has meetings on site with external visitors. Agnes is aware that visitors need to be supervised at all times and security / reception are made aware of all visitors. She therefore personally receives visitors and allows them entry/exit through the barrier door which requires an ID pass and further supervises them whilst they are on site. Whilst collecting visitors she often sees unsupervised people without a visible visitor's badge waiting near the barrier door and occasionally ‘tailgate’ (follow closely behind another person) to get into the main building. Although Agnes appreciates that this is a security risk, she is also aware that this is a common occurrence which is normally overlooked.

1. **Option A**: Notify security that you have observed visitors tailgating past the barrier.
2. **Option B**: Confront the people you see tailgating directly and ask them to show you some ID (if they are not known to you) and supervise them back to reception.
3. **Option C**: Assume the people have access and have been checked by the reception staff and continue with your work so as not to disrupt their work or yours.
4. **Option D**: Confront the people and then report their names to either your manager or security.

Scenario E – Document Control

Anne works for a utility company as a Compliance Officer and is responsible for managing and handling documents containing sensitive Critical National Infrastructure (CNI) information. Only certain people can access and use this information, provided they have gone through the appropriate vetting.

Anne recently received an angry phone call from Bob (Senior Manager) who is not happy that his staff no longer have access to important information they need. Anne explains the vetting procedure to him, but he is still not happy and asks to speak to her boss Cyril, who supports Anne and tells Bob that his staff require clearance to access the documents. A couple of weeks later Anne reviews the access logs to the documents, and notices that Dave (who works for Bob) has been accessing a large number of CNI documents. Anne looks into this further and finds that Dave is widely sharing this information to others in his team, none of whom have been through the vetting and managing of privileged information training.

1. **Option A**: Report your observations to Cyril, and urge him to tell Bob formally that this is not acceptable.
2. **Option B**: Send Dave an informal email, reminding him that sharing CNI documents with non-cleared employees is not allowed.
3. **Option C**: Initiate an audit of Bob's Department to attempt to track the use and distribution of the CNI documents.
4. **Option D**: Do nothing - If something goes wrong, Bob has to deal with it as he is the Senior Manager in charge of the department that is sharing the information.

Scenario F – Information Disposal

James works for a utility company as a Senior Contracts Manager and regularly reviews confidential contracts, which contain sensitive commercial information and customer data. He prefers to review documentation in paper form, so he often prints out confidential documents to read and make notes on whilst travelling on the train to/from home. When he is finished with these documents, as an environmentally conscious person, he places them in the recycling bin. At home there is no secure disposal available so he uses the standard recycling service. The risk of 'dumpster diving' (people stealing documents from rubbish bins) has been communicated in a recent Internal Awareness Campaign. It specifically recommends disposing of confidential information in the confidential bin but James feels that this is overly cautious and does not always use the Confidential but the normal recycle bin as he thinks the paper will be destroyed when it is recycled anyway, so there is no need to be concerned.

1. **Option A**: James' working practises are acceptable; recycling the paper is good for the environment and destroys any sensitive information at the same time.
2. **Option B**: James should ensure any paper copies he makes are disposed of specifically in a confidential recycle bin to ensure they are securely shredded once he has finished with them – hard copies are a major source of information leaks.
3. **Option C**: James is right to work in the way that suits him best – without access to the company systems even if someone did get hold of a few bits of information they couldn't damage the utility company anyway.

4. **Option D**: James is being totally reckless with customer's information – the major threat caused by hard copies is to the customers via identity theft and he should stop printing out work unless it is absolutely necessary.

Scenario G – Backing Up Information

Emilia works for a utility company as a Finance Analyst and is a very conscientious individual who occasionally works from home in the evening to catch up on things she could not complete during the day. Emilia normally uses the train to get home. She chooses to leave her laptop as she has recently had her laptop stolen when travelling home from work. Emilia keeps a backup of all her work files on her personal computer so she can access files without having to connect to the utility company system as her home network connection is not always reliable. She knows this is against company policy, but she lives in a safe neighbourhood and does not consider this to be a great security risk. In order to transfer files to her home computer she uses a variety of methods.

1. **Option A**: Use one of your USB sticks to carry your current work with you on the train.
2. **Option B**: Email the files to your personal email account from your work account and download them at home.
3. **Option C**: Use an online storage service such as Drop box as an interim transfer location, deleting the files once you have made a local copy.
4. **Option D**: Log in to the company VPN and make local copies via that connection.

Scenario H – External Threats

Andrew works at a utility company site, and he walks there each morning from the local station. One morning he notices a blue van parked outside the entrance gates. He thinks he has seen the van parked in the same spot several times before over the last couple of weeks. Andrew becomes suspicious so he notes down the van details so he can check again if it is the same van. A few days later, Andrew notices the same van parked in the same location. As he passes the van he observes two individuals, one of whom appears to be taking pictures of the building/people around the building. As soon as the individuals see Andrew, the van pulls away in a hurry.

1. **Option A**: Put it out of your mind; you have seen the van several times and nothing has happened at the site so it probably isn't a threat.
2. **Option B**: Report the incident to your line manager; it is better to report such incidents even if nothing has happened.
3. **Option C**: Report your suspicions directly to security so they can take the appropriate action.
4. **Option D**: Do nothing now but keep an eye out for the van in the future to confirm his suspicions. If it shows up again then report the incident.

Scenario I – Information Requests

Mohammed is a Contract Support Assistant at a utility company who manages 3rd-party contracts. One afternoon, he receives a phone call from Alison who used to work with him at the utility company but now works for one of the utility company's trusted 3rd-party companies. She asks Mohammed for some

commercially sensitive information that is not publicly available through the company's web site. While the company she works for is allowed access to the information, Mohammed is aware that there is a procedure 3rd-parties need to go through to obtain that information. Mohammed politely refuses the request and reminds Alison of the procedure she should follow. Alison now becomes very persistent and reminds Mohammed that they used to be colleagues as well as mentioning the names of several senior people in both companies, saying they will be extremely unhappy if she does not get this information that day. She further says she is still in contact with his line manager and will explain everything to him later, so Mohammed should be ok with providing this information today.

1. **Option A**: Accede to the request for information to ensure that the senior personnel are satisfied and Alison's productivity isn't hampered.
2. **Option B**: Send Alison the information she requested but immediately inform your line manager of the call and that information has been provided.
3. **Option C**: Ask Alison specifically which pieces of information she needs and send through a redacted or edited version of the documents.
4. **Option D**: Send the information through but password protect the file and wait until you have spoken to your line manager before releasing the password to Alison.

Scenario J – Working Practises

Sanjeeta has worked with Kevin at a utility company for a number of years. Kevin has always been an effective member of the team, but is known for 'having his own way of getting things done'. A few months ago Kevin left the utility company to work for one of the utility company's Service Partners. They still maintain a close working relationship and are located at the same site. Recently Sanjeeta noticed that several confidential documents/records were missing and there was no audit trail of who had used them last. Sanjeeta then recalls that Kevin had accessed the documents to resolve a query associated with a project he had recently been working on, so she decides to ask Kevin about the missing documents next time she saw him. When asked about the missing documents, Kevin becomes very defensive and objects to being challenged, telling Sanjeeta that she should "stick to her own work and stay out of mine". Sanjeeta was very taken aback by this response.

1. **Option A**: Do nothing, Kevin's working practises have always been eccentric and this seems to be no more than a product of his usual attitude.
2. **Option B**: Discuss Kevin's behaviour with the department manager – it isn't acceptable for an individual in the department to have their own methods that conflict with the company best practice and policy.
3. **Option C**: Accommodate Kevin's work practises by adjusting your own, it will be easier and more productive for you both.
4. **Option D**: Call the Business Conduct helpline and make a report about Kevin's behaviour – it is suspicious that there appears to be no proper audit of his work.

Appendix F: Thematic analysis codes, themes, categories and relationships

Security awareness and understanding

Awareness of the importance of for information security

Aware of the sensitivity of organisational information

Code	Description
External risk	more careful when dealing with outsiders
Responsibility	they know the risks, feel proud to be responsible
Role awareness	sensitive operations so people know they should be careful
Value security	needs it in their job due to a lot of information exchange

Problems from potential misuse or leak to unauthorised sources (both from a security and a commercial perspective)

Need for security	confidentiality of info protects commercial environment,
Sensitivity awareness	hold and see a lot of confidential information, if someone wants to harm the company can pass that to competitors, easy to do so
Impact Awareness	malicious behaviour can have significant impact on organisations service providing capability
Reputation value	embarassment for organisation if some things were left to leak out, Some of the information could affect the stockmarket
Regulation driver	not allowed to share some information between some parts of the organisation (regulation
Risk awareness	aware they should be careful with email/internet usage/passwords etc. data potentially useful to competitors for commercial gain

Potential problems to themselves as individuals (shaming, potential sanctions imposed by the organisation)

Sanctions exist	(some action was taken against them)

Policy communication and training

Personal information sensitivity

InfoSec misunderstanding	Information they deal with will be of interest to other internal parties, NO SECURITY CONCERNS on their job though

Policy content and understanding

Low policy familiarity	No line for line policy knowledge
Own policy understanding	had to figure out most good practice information on their own
Policy ok	Thinks policy is adequate
Policy perception	“about right”
Policy overloaded	Too much information to read
Policy common sense	new people don't follow common sense rules
Policy location awareness	knows where to find information if needed
Low policy knowledge	can’t recall password security policy, people not aware of the policies in general
Not read policy	knows extensive guidelines exist if you have time to read those
Security team communication	Communication usually done at team talks
Rare central communication	Centrally, rarely receive security advice, occasionally emails about it, changes in policy
Communication	could explain to them a bit more why they should behave in specific

unhelpful	ways
Communication not read	rarely reads those
Security communication mixed within other bulletins	security changes only communicated through at a glance bulletin
Knowledge gap	not very confident on knowledge about policy
No training	No security-related training delivered in the organisation
Training common sense	most things are common sense, “just remember this and that”
Training occasionally	some computer-based training
Training not relevant	finds some questions asked irrelevant, Many things were not interesting to them
Training not on ISec	no specific training on Isec
Security team Induction	security induction through team talk
Training needs improvement	thinks that approprate training would solve a lot of problems, Tickboxing currently

Downplay own responsibility

No sensitive information	information they see not commercially sensitive, information on laptop of limited interest
Low awareness	people surprised when told not to share everything with everyone around them
Compromise hard	more than one compromises required to get useful data (like a jig saw), someone would need to know may pieces of jigsaw to extract conf info
Equipment uninteresting	Laptop, phone etc not interesting information-wise
Downplay risk	doesn’t think anyone intercepting emails would benefit from it, information about projects is available for anyone that can drive to the locations
ISec is confidentiality	Isec is different than commercial confidentiality, NOT SECURITY - JUST CONFIDENTIAL DATA, initial training about confidentiality
Confusion on information sensitivity	Not sure if information sensitive or not

Security mechanisms

USB stick use

Compliant with policy

Encrypted USB	Use company provided encrypted drives
Encrypted USB driver: communication	Because they told them to

Unaware of policy

No USB policy awareness	No idea they had to use company ones

Low encrypted USB drive adoption

Encrypted USB: cost	not all people who need to transfer data have those as they cost too much
Use unencrypted USBs	Use unencrypted USBs in the office, for data transfers between home and work, for file sharing in office
Borrow USB password	Borrow someone's USB with password
Post-it USB password	They use post-it notes for password of encrypted USB sticks

Using unencrypted drives

Fear for encryption	Fear for loss of access
Unencrypted backup	for backup reasons
USB at home	Download blocked information, transfer work data
Trust colleagues	Shows confidential information to other people. They know information is confidential so they won't share anything they are told. trust the others that they know policies
USB misconception	Deleting data from unencrypted USB immediately after use
USB policy awareness	No idea they had to use company ones

Not using USB

USB risky	Avoid usb: virus
Encryption problems	Authentication fails in crucial moments, easier to carry laptop around, not enough capacity
Email to personal account	Sends documents at home address to ensure access (sometimes cant access from outside)

Email filtering, Website blocking

Email filtering inconsistent

Email filtering inconsistent	Infected emails pass through firewall, useful ones dont

Website blocking problematic

Website blocking problematic	Not well targeted, inconsistent website blocking
Website blocking annoying	Frustration from website restrictions, often blocks work-related sites
Download information at home	And bring in the office when websites are blocked
Own assessment of external content security	check downloads before bringing it in (think they could spot it if malicious), but did not have time to do so
USB use at home	Using USBs on home machines

Security helpdesk experience

Slow helpdesk	Some weeks to sort out problems via helpdesk, Support terrible
Software access slow	Time to get S/W on laptop “about a week” p48
Not using helpdesk	Horrible service

Security experience and perception

Majority compliant	Perception of a compliant environment within organisation
Security culture	(from employee perspective) most people follow most of the rules most of the time
ISec highly regarded	No one fired for carbon footprint
Non-compliance prevalent	no way people follow all the rules all the time
Experience impact	people longer in organisation understand what they should/not do, people long in the organisation know what is required from them
No separation	Chinese walls exist (not really enforced though - people know each other too well)
Contractor access	laptops given to contractors without much care taken
Contractors less motivated on security	contractors need to be motivated a bit more to follow rules
Productivity conflict	Policy sometimes conflicts with business -> need to bypass, Rule breakers have reasons for doing so
Productivity slowdown	colleagues have been unable to work for weeks
Login slowdown	Takes about 20 mins to log-on on the good days,

Enforcement and sanctions

Behaviour driver: sanctions	would like to be aware so that they cannot be blamed for things they are not aware of
Sanctions drive behaviour	careful about sec policy as they have seen people suspended for relatively minor things
Misbehaviour warnings	warnings for people that misbehave, e.g. people given warnings for leaving piles of documents lying around
No sanctions	they can get away with missent emails and misplaced usb sticks, no one cares for screen lock
Health and safety prevails over security	Nowhere near as health and safety

Security behaviours

Screen lock

Screen lock awareness	On the need to do it, potential risks
Screen lock sometimes	Not always, sometimes forget, when coming back quickly not doing it
Screen lock motivation	open plan office, colleague peer-pressure
Auto-lock reliance	“Will lock itself anyway”

Laptop usage

Label on laptop	Company label – everyone knows who it belongs to, employee name on laptop
Takes laptop home	To be able to work if something happens
Protect laptop: awareness	Put it in boot, don't leave it in the office
Laptop risk awareness	That data can be accessed easily
Laptop protection measures	Make sure not leave it anywhere, don't like travelling with them, "biggest risk to the organisation", need to be careful with the information they put on laptop as they travel a lot, lock it in car boot, make sure it is not obvious they carry a laptop, hide it somewhere when leaving house

Password use

Protection perception	Presence of passwords meaning that no one can hack a system
No write password	Aware on sensitivity

Password choice and handling

Burden: many passwords	Too many to remember, hard to keep track, hard to manage all of those
Set passwords same	All passwords for all systems set to the same
Writing password allowed	Thinks policy allows writing down password
Password in document	Write in a word document, or on encrypted USB
Password in PDA	Store list of passwords on pda
Password in book	Writing at back of book to remember, full page of passwords
Protect physical copy of password	On paper in desk, post it in drawer - lock

Password changing

Password change: annoyed	need to be reset at different points in time
Access loss	If passwords expire and they go on holiday, need to remember to change before they go to avoid being locked out
Never changed password	Never changed given password
No password change	Not forced so not do it
Negative effect	"if they didnt have to reset so often would probably have a stronger one"
Simultaneous password change	Change all passwords together when a change needed (if all are set to the same)
Simple password change	changed slightly every month
Add month to password	Add month at the end when they need to change
Last digit change	Change one digit at a time when passwords require change
Own password mechanisms	Not allowed to use months so uses summer01, summer 02

Password sharing

Password sharing reason	See others email when covering for them, access right takes ages, "when they need to get things done", Has left a senior manager working on their laptop and assumed they would lock it
Password sharing – peer pressure	"Feels uncomfortable but reservations wouldn't be listened anw"
Password sharing mechanism	Share passwords through the phone
See other's mail when	When on leave, covering for them

covering	
Trust colleagues	shows confidential information to other people. They know information is confidential so they won't share anything they are told. trust the others that they know policies
Manager trusts employees	On policy awareness
Generic accounts	On rarely used site (passwords keep expiring)
No password sharing	Too risky

Document handling

Document storage

Network drive

Network drive	Store files on personal network drive
Network drive motivation	Backup
No backup	Data locally stored not backed up

Locally on their computers

Work on documents locally	Data stored on laptops
Laptop password protected	Password protection makes laptop safe
Storage misconception	Confidential stuff on desktop, nothing on c drive though so safe
Work locally motivation: connection problem	VPN problems, no internet, lazy
Store locally: driver	Storing data locally to access when network drive is unavailable (e.g. home, train, other offices)
Network drive problem	Drives inaccessible or too small

Also using personal computers

Own computer motivation: connection issues	When connection not good
Own computer use	Works on corporate data at home on personal computer

Use two computers for productivity reasons

Two devices	For employees that work in more than one subsidiaries

Document sharing

Contractor Risk	people are aware they shouldn't pass some information to contractors
Information separation	Tries to keep information separate from different divisions, need to keep information separate between regulated and unregulated parts of the business
Email sensitive	emails can flow around without being monitored
Email document sharing	Use emails to share documents
Password protect sharing	If information is deemed as sensitive, send password separately When sending things outside make sure recipient correct, password protected files

Physical documents – Clear desk

Clear Desk awareness	Clear Desk motivation: sensitivity awareness shouldn't leave confidential stuff lying around
Clear desk driver: awareness	Open plan office, colleague pressure (jokes)

Secure disposal	For documents that they think are confidential

Clear desk - not doing it

Clear desk violation	No risk, physical security good so no risk
No clear desk enforcement	Clear desk inspections were done in the past, not anymore
Laptop physically unlocked	On desk unlocked (screen lock pointless in that case).

Physical Security

Passive on physical	Outsiders would be picked by someone else
Physical security perception	Physical security not hard to get into office, Easy intrusion

Relationships between themes

Cause	Effect	Examples
Employee risk awareness	Laptop Usage, Screen Lock, Password Sharing, Document storage and sharing, Physical documents, Clear desk	Write password in protected document, not sharing passwords with colleagues, not storing information on laptop
Confusion on security purpose	Employee risk awareness	Downplaying risk: Compromising information is hard Considering information they use as not-sensitive
Policy awareness	Laptop Usage, Screen lock, Password choice and handling/changing/sharing, Clear desk, physical documents, USB stick use	Locking screens, securely disposing physical documents, clearing desk, using encrypted drives
Policy overload	Policy awareness	Too much information to read, impossible to know everything
Security Culture	Risk awareness	No-one fired for carbon footprint, but has happened for security so security must be important
Encrypted USB stick problems	Document sharing/storage, laptop usage, USB stick use	Encrypted USB drives provided by organisation too small, so alternative file-sharing methods such as using unencrypted drives or emailing files had to be used.
Storage problems	Document sharing/storage, laptop usage, USB stick use	Insufficient space on network drive Experienced problems accessing files needed from home or while travelling Employees justified copying files to laptops because Network drive is full - Copying files locally
Password overload	Password choice and handling/changing/sharing,	Large number of passwords required for various corporate systems resulted in employees being unable to recall those from memory. Led to writing their passwords down (on laptop or document)
Email filtering and website block	Document storage and sharing	Websites needed for work purposes blocked Downloading content at home and bringing it in the organisation
Communication problems	Confusion on security purpose, policy awareness, security culture	Not explaining how they should behave Rarely read Mixed with other things
Training	General Information security awareness, Confusion on security purpose, policy awareness, security culture	Most things common sense, Training occasionally and not relevant, security induction at team talks Currently tickboxing
Support problems	Security culture, USB stick use, Password sharing	Not using helpdesk – “support horrible” Getting access to software is slow
Other security problems	Security culture	Slowdown caused by security – negative feelings: takes 20 minutes to log on on good days Violators have reasons to do so – problematic security

Appendix G: Axial coding results

Company A

Category	**Properties** characteristics or attributes	**Dimensions** values of a property	**Conditions** elements of the security implementation, employee knowledge and beliefs that drive security behaviours	**Actions/Interactions** behaviours or beliefs of employees that resulted from the identified conditions	**Consequences** conditions from employee behaviours and impact on organisation
Risk / need for security awareness	Understanding of security risks, potential impact to the organisation, reasons driving understanding	Risk awareness and understanding	Regulation for data protection and handling of sensitive information	Chinese wall business separation behaviours Need to know information sharing	Risk mitigation Avoid penalties for organisation
			Employee own risk awareness (need to uninterrupted information access, information useful to competitors, outsiders could damage the organisation, reputation damages)	Understand the need for security to exist in the organisational environment Realising the impact loss of access can have on their workflow	Understand the need to follow security policy when using sensitive information
			Confidentiality agreements exist		
		Downplaying own security responsibility	Problematic organisational security communication Lack of security training	Employees believe information they handle is not-sensitive (confidentiality, not security) Outsiders would be picked up by someone else or have right to be there (not easy to get in)	Minimal motivation to behave securely Insecure behaviours Puts organisational information at risk
		No perceived security risks		Employees believe no security risks exist in their role	

Policy awareness	Aware of policy content	*Fully aware*: of security policy content	Aware of policy importance	Visit policy website and actively try to stay up to date	Increased policy awareness More likely to follow recommended practices
		Unaware: of policy	Lack of awareness regarding their role Some still aware that they should protect confidential documents	Ad-hoc password behaviour, information handling/sharing strategies	Self-devised security solutions Risky data handling behaviours No action against non-compliance Violations become norm
		Partly aware: aware of some elements of the policy	Aware on role-related clauses	Encrypted USB use Clear desk and screen lock Refusal to share passwords	
			Believe not applies to them (e.g. challenging strangers)	Not following recommended practices	
			Training problems (training is superficial on security, provided only to new people) Communication problems (inconsistent, security included among other things, seems less important than health and safety)	Downplaying security importance Lack of accurate risk awareness Misconceptions, own understanding Own interpretation of desired behaviours (e.g. “should write password down”)	
			Content problem: Overloaded, vague, inconsistent, unrelated to role Perceived as common sense	Ignore policy content Dismiss policy usefulness Devise own practices (e.g. own USB use, own password management strategies)	
			No enforcement	Reduced employee motivation Policy appears unimportant	

Secure behaviour drivers	Elements of the organisational environment that incentivise secure behaviour	Official (under organisational control)	Effective security communication Architectural means make compliance easy (provided encrypted USB drives, personal network storage backed-up)	Understanding benefits of security mechanisms and use those Challenge colleagues when needed	Secure state
			Low cost of compliance	Screen lock easy to do	
			Clear Desk enforced by property not security	Not leaving documents around	No connection between actions and information protection
		Unofficial (no central organisational control)	Responsibility Manager pressure Peer pressure Past events	Secure behaviours Actions to protect computers Screen lock	Secure behaviours based on own employee understanding Security culture developed out of organisational control Collaborative team level enforcement

Time impact	Time-related information security overheads – Security slowing down primary task	Mechanism problems	VPN Slow encrypted USB sticks slow productivity focus	Unencrypted USB drives Copy data locally	Increases data leak risks Lack of perceived security usefulness (or corresponding support) Increases need to come up with ad-hoc solutions
			SharePoint slow to setup	USB and email file sharing	
		Process problems	Access control setup slow Slow IT support Password reset slow	Share passwords Frustration	
Disruption	Security blocking primary task – unable to complete tasks unless they bypass security	Mechanism problems	Filtering and blocking problematic Block work-related information	Send it as different file type Download at home and bring in on unencrypted drive	People feel not trusted by excessive blocking Increasing virus risks
			Personal network drives full	Store files locally Recognise increased risks	Feel central security support inadequate Non-compliance habituation
			Shared drives problematic	USB and email file sharing	
			Connectivity problems (VPN, lack of connection)	Send files to home accounts Store files locally	Increases data leakage risks Depend on employees to keep personal computers/email accounts secure
		Process problems	Encrypted flash drive procurement problems – not everyone has one	Use unencrypted ones Store information locally Email (personal and business accounts)	Security appears problematic Non-compliance justified for employees

Increased cognitive load	Hard to manage mechanisms	High mental effort required – can be impossible	Different services require different passwords	Write passwords down Own mechanisms to protect passwords	Inaccurate risk understanding, dangerous to let them choose
			Too much in the policy No role-specific communication	Need to decide what they think is more relevant	
Organisational adaptability	Organisational ability to accommodate changes to the environment	Flexible	Can request removal of websites from blocked list	Slow process No alternatives provided	Employees need to come up with own solution
		Inflexible	No effective delegation of responsibilities	Password sharing Access using other's accounts	Violations become norm
Team level security communication and mediation	Elements of information security management happening at team-level	Security communication and support	Lack of central communication Lack of security training Reliance on managers	Employees seek support from line managers Advice between peers Managers advice on security challenges	Ad hoc – based on manager understanding and perception Varies by location and manager - inconsistent behaviours around organisation
			No security guidance for managers	Based on own best practice and understanding	
		Permissions, access control decision making	Access control decision making by managers (authorising access to resources) Management authorisation for information access	Ad hoc – based on manager understanding and perception	Varies by location and manager

Security perception	Overall perception of organisational security	Positive	Required to protect organisation	Motivation to comply	Easy to use mechanisms and processes are used
		Problematic	Impacts productivity	Non-compliance justified	Justification for coming up with own solutions Increasing organisational risks Accentuates non-compliant, ad-hoc culture
			Blanket rules No effective guidance Access control housekeeping problematic (revoking not quick) Feedback goes unnoticed No attempts to improve Sanction based People just comply to avoid trouble Job security – lack of motivation No enforcement Varies by location	If security appears to demand reasonable time/effort AND employees understand role-related risks they follow recommended practices Security perceived as inflexible and not serving employee priorities Security rules perceived as unimportant Employees doing what they believe they can get away with	
Culture perception	Employee perception of the overall organisational security culture	Security important	Colleagues willing to comply and be secure		Employee participation in protecting the organisation
		Security unimportant	Productivity driven culture Health and safety more important Lack of awareness on many security issues Oversharing information Contractors have different values than employees Culture static - Need to be more proactive	Perception of security as non-willing to improve Perception as less important than other organisational issues	Employees disconnected from security Justifies doing “own thing” on what they perceive to be right for protecting information they handle

Company B

Category	**Properties** characteristics or attributes	**Dimensions** values of a property	**Conditions** elements of the security implementation, employee knowledge and beliefs that drive security behaviours	**Actions/Interactions** behaviours or beliefs of employees that resulted from the identified conditions	**Consequences** conditions from employee behaviours and impact on organisation
Risk / need for security awareness	Understanding of security risks, potential impact to the organisation, reasons driving understanding	Risk awareness and understanding	Awareness on the importance of information they handle, potential breaches, impact to the organisation and the need for security	Actions to protect laptops Not share passwords Screen lock Clear desk	Protects organisation and employees
			Communication of relevant regulation on sensitive information	"Need to know" information sharing Password protecting important documents NDA people are more aware on the need to be careful with information.	Distrust – creates problems in planning and delivery – Legal team needs to be involved
			NDA presence on some projects		
		Downplaying own security responsibility	Problematic organisational security communication (among other things, generic, not done, role-based) Problematic security training (CBT based, generic, tickboxing)	Rely on managers and colleagues	Ad-hoc culture creation, out of organisational control
				No understanding of data classification	Less care in protecting it
		No perceived security risks		Downplay sensitivity of information they use	Communication partially influence employee actions

Policy awareness	Aware of policy content	*Fully aware*: of security policy content	Policy awareness	Actively look for policy updates	Increased policy awareness More likely to follow recommended practices
		Partly aware: aware of some elements of the policy	Not everything relevant Aware on role-related clauses Policy perceived as common sense	Own mechanisms (e.g. use USB, erase afterwards) Downplaying some risks	behaviour has some security merit – but not aligned with policy "common sense" risk understanding can be inaccurate
			Policy on website	Not check	
			Aware of privacy marking existence Marking depends solely on owner Admit to not knowing how to use these	Gets support from line manager Overclassify	Potential of desensitisation Microculture development
		Unaware	Unaware of marking guidelines	Information left around – picked up by clear desk inspections ("don't happen often") No reprimands or enforcement	No understanding on handling documents marked by others Non-compliant culture
			Unaware of physical security policy	Not wearing pass Not challenged	Non-compliant culture

Secure behaviour drivers	Elements of the organisational environment that incentivise secure behaviour	Official (under organisational control)	Awareness about clear desk Hot desking Lockable drawer Secure disposal bins Clear desk enforcement	Clear desk compliance	Good architectural means - low cost of compliance
			VPN provides adequate access – reliable Personal network storage	No local file storage	
			Responsive helpdesk Reported problems followed up	Report problems	
			Password resets easy	Uninterrupted access	
			Access control easy to setup	No password sharing	
			Usable password manager	No writing down	
		Unofficial (no central organisational control)	Responsibility Manager pressure Peer pressure Past events	Secure behaviours Actions to protect computers Screen lock	Secure behaviours based on own employee understanding Security culture developed out of organisational control

Time impact	Time-related information security overheads – Security slowing down primary task	Mechanism problems	VPN Slow	Local storage	Computers are vulnerable
			Encrypted USBs sometimes don't work	Use unencrypted ones	Disgruntlement - interference with primary task Technology perceived as hindrance to complying with policy.
		Process problems	SharePoint slow to setup Access control setup slow Slow IT support Password reset slow	Perceived inability of the technical side to get some things right Some generic accounts appear to exist Sharing files through multiple formal/informal channels	Reduced accountability Reduced perceived support
Disruption	Security blocking primary task – unable to complete tasks unless they bypass security	Mechanism problems	Network drive small Connectivity problematic Encrypted drives - feel safe	Reliant on local storage Ad-hoc backups (to external drives – sometimes personal) "Unintentional backups" onto local laptop systems,	Laptops are vulnerable to cold boot attacks No backups exist Data from past projects stored on local machines forever
			Forget encrypted USB password – lose access	Carry laptop with data	
			Sharing drives hard to manage	Share information through emails Also third party services used	Emails stored locally No accountability and audit possible Dependence on third party security
			Inconsistent email filtering Website blocking problematic - Prevents access to blogs useful for work	Access the information at home	Interference with primary task - disgruntlement Increased risks
			Password manager not work for all systems	Write passwords in documents or on paper	
			No lockable space	Clear desk problematic Need to carry documents with them	Potential loss of information

Increased cognitive load	Hard to manage mechanisms	High mental effort required – can be impossible	Various passwords for different systems Password change rules across different systems	Keep passwords same Passwords similar after changes Write passwords down	Increasing risks
			Too much in the policy No role-specific communication	Own interpretation Role-specific awareness Not checking website Not everything relevant Colleague/line manager support	Ad-hoc security culture Inaccurate risk perception can lead to dangerous behaviours
			Marking guidelines confusing	Not using those	No understanding on handling documents marked by others Non-compliant culture
Organisational adaptability	Organisational ability to accommodate changes to the environment	Flexible	Can request removal of websites from blocked list	Reported problems followed up	Risk of employees not reporting problems
		Inflexible	Not many employees report concerns or problems	No reporting culture	

Team level security communication and mediation	Elements of information security management happening at team-level	Security communication and support	Managers not know complete policies Problematic central communication and training (irrelevant, generic, inconsistent and overloaded) Reliance on managers not formalised	Communication at team meetings Security support by line managers and colleagues Devise own adaptations to unsatisfactory security measures or Introduce own novel solutions	Solutions deployed are based on their own understanding of what the security experience should be like. May not manage the organization's risks adequately Culture defying central security
		Permissions, access control decision making	Employees not fully aware of policies – also partially dismiss their usefulness Managers not know complete policies	Ad hoc – based on manager/colleague understanding and perception	Varies by location and manager
			Access control decision making by managers (authorising access to resources) Management approval for information access		
Security perception	Overall perception of organisational security	Positive	Protects the organisation adequately Closed-build, encrypted password protected laptops Considered in requirements	Importance of security well understood Employees see value in security	Compliance motivation
		Problematic	Impacts productivity (e.g. email filtering/access problems, password reset problems)	Negative attitude Insecure behaviours justified	Justification for coming up with own solutions Increasing organisational risks Accentuates non-compliant, ad-hoc culture
			Security and compliance measured using CBT completion rates. Too many CBTs Information appears irrelevant/common sense	Communication perceived as unimportant Self (or team)-devised security behaviours	
			Access revoking problematic Should be doing more - No enforcement Information oversharing prevalent	Central security appears ineffective	

Culture perception	Employee perception of the overall organisational security culture	Security important	Employees want to comply/contribute to security Challenging colleague behaviour	Mechanisms demanding reasonable time/effort are followed IF employees understand why	Employee participation in protecting the organisation
		Security unimportant	Productivity driven culture Security considered tickboxing Lack of awareness on many security issues Varies across locations Need to be more proactive	OK to bypass security when it creates primary task problems	Employees disconnected from security Justifies doing “own thing” on what they perceive to be right for protecting they handle

Trust

Category	**Properties** characteristics or attributes	**Dimensions** values of a property	**Conditions** elements of the security implementation, employee knowledge and beliefs that drive security behaviours	**Actions/Interactions** behaviours or beliefs of employees that resulted from the identified conditions	**Consequences** conditions from employee behaviours and impact on organisation
Assurance	Assurance mechanisms in place and impact on employees	Understand need for restrictions	Understand potential problems to the organisation by a security leakage	Accept the need for security mechanisms and policies to protect the organization Understand their contribution in protecting the organisation	Motivation to behave in a trustworthy way
		Mechanisms and policy compliance	Desired behaviours outlined in policy Mechanisms implemented to prevent insecure behaviours Potential sanctions defined in policy for bypassing security	Temporal incentives: Sanction avoidance	No culture development – no long term compliance incentives Not taking advantage of employee goodwill and motivation
organisation-employee trust	Trust shown towards employees and impact on security	Employees are trusted by the organisation	Policy clauses defining desired employee behaviour without enforcing it (e.g. don't share passwords, use encrypted drives) Communication of related risks and the need to protect the organisation	Employees recognise organisational reliance on them Intrinsic compliance: • Ability: Employee knowledge and risk awareness to protect the organization • Motivation: understanding responsibility - propensity to do good	Dependency on employees – can expose the organisation if they do not act as required Benefits of implementing trust-based rather than assurance-based security (cheaper, long term effectiveness etc)
		Breaking trust	Problematic assurance mechanisms slow down or disrupt primary task	Need to bypass mechanisms or ignore policy Recognize breaking organization-employee trust	Drains capacity to behave securely Violations considered justified Non-compliance culture development

inter-employee trust	Existence of trust relationships between employees and impact on security	Trust between colleagues	Close relationship with their colleagues Policy demands no inter-employee trust (No password sharing, No information sharing etc)	Trust relationship conflict	Need to decide which trust relationship to preserve
		Prevailing over organisation-employee trust	Conflict between trust relationships Inter-employee trust relationships prevail Trust enabler to productivity when security is problematic	Self-devised security mechanisms	Long-term reliance on collective trust violations Security spins out of organizational control Behaviours out of sight of security management Culture where breaking security is justified

Appendix H: Grounded theory emerging themes

Company A

	Total	Percentage		
access control	83	70.34%	Number of themes	47
awareness	98	83.05%		
burden	55	46.61%	Average per employee	20.3559322
circumvention	32	27.12%		
circumvention driver	96	81.36%	Stddev	4.927483326
clear desk	85	72.03%	Median	20.5
communication	108	91.53%	Average per theme	51.10638
computer	1	0.85%		
contractors	44	37.29%	Stddev	35.82833
culture	80	67.80%	median	46
data sharing	73	61.86%		
data storage	65	55.08%		
document handling	11	9.32%		
email documents to personal account	3	2.54%		
email filtering	18	15.25%		
frustration	17	14.41%		
helpdesk	38	32.20%		
hot desk - no hot desking	3	2.54%		
insecure behaviour driver	53	44.92%		
laptop	72	61.02%		
length of service	105	88.98%		
misconception	27	22.88%		
outsourcing	23	19.49%		
own mechanism	38	32.20%		
password	103	87.29%		
physical security	76	64.41%		
policy	89	75.42%		
process problem	8	6.78%		
reprimands - for inappropriate emails	1	0.85%		
role	113	95.76%		
screen lock	66	55.93%		
secure behaviour driver	110	93.22%		
security driver	88	74.58%		
security implementation	46	38.98%		
security perception	87	73.73%		
security problems	17	14.41%		
sensitivity - people don't know what to redact	1	0.85%		
separation - personal from work devices	5	4.24%		
social engineering	15	12.71%		
support	24	20.34%		
training	75	63.56%		

trust	46	38.98%
USB	92	77.97%
vendor	2	1.69%
vetting	27	22.88%
VPN	34	28.81%
website blocking	49	41.53%

Company B

	Total	Percentage
access control	55	67.07%
awareness	77	93.90%
burden	56	68.29%
circumvention	9	10.98%
circumvention driver	44	53.66%
clear desk	60	73.17%
communication	72	87.80%
contractor risks	2	2.44%
culture	66	80.49%
data classification	43	52.44%
data sharing	72	87.80%
data storage	69	84.15%
document handling	18	21.95%
email filtering	14	17.07%
experience of security problems	15	18.29%
helpdesk	10	12.20%
home working security	1	1.22%
insecure behaviour drivers	51	62.20%
laptop use	56	68.29%
length of service	73	89.02%
manager responsibility	13	15.85%
misconception	17	20.73%
network drive	30	36.59%
own mechanism	24	29.27%
password	64	78.05%
physical security	49	59.76%
policy	56	68.29%
role	54	65.85%
screen lock	67	81.71%
secure behaviour driver	72	87.80%
security driver	66	80.49%
security hygiene	1	1.22%
security perception	63	76.83%
separation	13	15.85%
shadow security	15	18.29%
social engineering	17	20.73%
support	32	39.02%
training	67	81.71%
trust	20	24.39%
USB	20	24.39%
vendor access	8	9.76%
vetting	1	1.22%
VPN	12	14.63%

Number of themes	46
Average per employee	20.69512
Stddev	4.98703
Median	20.5
Average per theme	37.48889
Stddev	25.15253
Median	32

website blocking	13	15.85%
yammer user	30	36.59%

Appendix I: Category list and example extracts

Shadow Security - Company A

Category name	No	Percent
Access control decision making by managers, Management authorisation for information access	87	73.73%
Access control setup slow, Slow IT support, Password reset slow	61	51.69%
Ad hoc – based on manager understanding and perception - Varies by location and manager	16	13.56%
Ad-hoc password behaviour, information handling/sharing strategies	89	75.42%
All employees realise the impact loss of access can have on their workflow	87	73.73%
Architectural means make compliance easy	29	24.58%
Aware of policy importance	57	48.31%
Aware on role-related clauses	38	32.20%
Believe policy not applies to them	51	43.22%
Can request removal of websites from blocked list - Slow process, No alternatives provided	6	5.08%
Challenge colleagues when needed	30	25.42%
Chinese wall business separation behaviours	27	22.88%
Clear desk and screen lock	52	44.07%
Clear Desk enforced by property not security	3	2.54%
Colleagues willing to comply and be secure	51	43.22%
Communication problems	106	89.83%
Confidentiality agreements exist	17	14.41%
Connectivity problems, Personal network drives full, Shared drives problematic	16	13.56%
Contractors have different values than employees	43	36.44%
Culture static - Need to be more proactive	36	30.51%
Devise own practices	104	88.14%
Different services require different passwords	31	26.27%
Dismiss policy usefulness	32	27.12%
Downplaying security importance	28	23.73%
effective security communication	65	55.08%
Employee own risk awareness	101	85.59%
Employees believe information they handle is not-sensitive	75	63.56%
Employees believe no security risks exist in their role	39	33.05%
Employees doing what they believe they can get away with	16	13.56%
Employees seek support from line managers, Advice between peers, Managers advice on security challenges	68	57.63%
Encrypted flash drives procurement problems – not everyone has one	19	16.10%
Encrypted USB use	45	38.14%
Filtering and blocking problematic, Block work-related information	38	32.20%
Health and safety more important	66	55.93%
If security appears to demand reasonable time/effort AND employees understand role-related risks they follow recommended practices	104	88.14%
Ignore policy content	52	44.07%
Impacts productivity - Non-compliance justified	90	76.27%
Lack of accurate risk awareness	88	74.58%
Lack of awareness on many security issues	94	79.66%

Lack of awareness regarding their role	56	47.46%
Lack of central communication, Lack of security training, Reliance on managers	100	84.75%
Lack of security training	73	61.86%
Low cost of compliance	47	39.83%
Misconceptions	27	22.88%
Need to decide what they think is more relevant	47	39.83%
No effective delegation of responsibilities - Password sharing, Access using other's accounts	73	61.86%
No enforcement	7	5.93%
No security guidance for managers - Based on own best practice and understanding	9	7.63%
Not leaving documents around	31	26.27%
Outsiders would be picked up by someone else or have right to be there	58	49.15%
Oversharing information	24	20.34%
Own interpretation of desired behaviours	72	61.02%
Own mechanisms to protect passwords	45	38.14%
Perception as less important than other organisational issues	68	57.63%
Policy appears unimportant	53	44.92%
Policy content problem	44	37.29%
Policy perceived as common sense	14	11.86%
Problematic organisational security communication	103	87.29%
Problematic security perception	111	94.07%
Productivity driven culture	18	15.25%
Refusal to share passwords	31	26.27%
Regulation for data protection and handling of sensitive information	95	80.51%
Required to protect organisation - Motivation to comply	87	73.73%
Responsibility, Manager pressure, Peer pressure, Past events	87	73.73%
Secure behaviours, Actions to protect computers, Screen lock	43	36.44%
Security perceived as inflexible and not serving employee priorities	80	67.80%
Security rules perceived as unimportant	50	42.37%
Send it as different file type, Download at home and bring in on unencrypted drive	7	5.93%
Share passwords, Frustration, Write passwords down, take own measures to protect password storage location	100	84.75%
SharePoint slow, USB/email file sharing	44	37.29%
Some still aware that they should protect confidential documents	56	47.46%
Store files locally, send to home accounts, Recognise increased risks, USB and email file sharing	83	70.34%
Too much in the policy, No role-specific communication	76	64.41%
Training problems	75	63.56%
Understand the need to follow security policy when using sensitive information	98	83.05%
Understanding benefits of security mechanisms and use those	29	24.58%
Understanding the need for security to exist in the organisational environment	102	86.44%
Unencrypted USB drives, Copy data locally	39	33.05%
Use unencrypted ones, Store information locally, Email (personal and business accounts)	83	70.34%
Visit policy website and actively try to stay up to date	5	4.24%
VPN Slow, encrypted USB sticks slow, productivity focus	88	74.58%
Write passwords down	56	47.46%

Risk / need for security awareness

Regulation for data protection and handling of sensitive information - Chinese wall business separation behaviours
P65: Because they're in tune with a couple of other things like the regulatory model, separation and stuff like that, so having to do things for a reason even though it might not seem like it's a good thing

Employee own risk awareness:

need to uninterrupted information access
P114: We are so IS dependent, that when it goes down, it affects us greatly

information useful to competitors, outsiders could damage the organisation, reputation damages
P3: I am more aware of IT in general and so I know how sensitive this stuff is and how easy it is to leak it out. It's more self-awareness that keeps me. I can't say that everyone thinks like that, obviously.

Confidentiality agreements exist
P55: We have a lot of confidentiality agreements between us and a customer, obviously we won't share that information and hope to God that they don't either.

Understanding the need for security to exist in the organisational environment,
P79: Security *implications* well clearly were they to be compromised there'd be massive impact so it's very important in that respect and there are increasing reports of systems around the world being attacked

Understand the need to follow security policy when using sensitive information
P36: So if it's HR Payroll data, make sure that we pull the employees Social Security, date of birth out and scrub the data before we publish it to whoever's asking for it.

Problematic organisational security communication,
P66: I think it goes back to what I was saying before which is I don't think enough is known or it's coming across in the right way or to the right audience.

Lack of security training
P67: They're given a building induction and a company induction, but it's pretty limited in terms of computer security.

Employees believe information they handle is not-sensitive (confidentiality, not security),
P104: Not at my level. there's obviously other people here, you know operational managers and things like that that might have more commercially sensitive information but at my level I wouldn't have anything that's that sensitive.

P47: Oh, Information Security rather than commercial confidentiality?

P51: So it's not strict Information Security, it's more commercial information that we have to be aware of.

Outsiders would be picked up by someone else or have right to be there (not easy to get in)
P72: That's not something I would do as my general process and then you'd send out the details so, I think they have to present ID at the door, the security desk that was their name and possibly that they work for a certain company.

Policy awareness

Aware of policy importance
P75: So I think this company's quite good at explaining why we need to have security in this manner

Visit policy website and actively try to stay up to date
P40: actively seek that out and read it and know that that's where I'm going to go to find the information

Lack of awareness regarding their role, Some still aware that they should protect confidential documents - Ad-hoc password behaviour, information handling/sharing strategies
P29: Probably, I would say around 15. I: So how do you manage that? P: On an Excel document.

P111: at times we do have to transfer the data to our laptops because the network is slow, response times can be really bad and some of the files are quite large that we use, so we transfer them to our laptops to work on and then transfer them back at the end of the day. I: And then presumably you would delete it from your own laptops as well?

Yes and then from, obviously the recycle bin.

Aware on role-related clauses
P66: You know you've got (*what*) you can and can't do, what you can send through your emails. You know the virus software that's going on, your security ID passwords, checklists, everything like that that goes on. So yeah little bits and bobs I suppose.

Encrypted USB use, Clear desk and screen lock, Refusal to share passwords
P72: Not to use your own memory sticks but to use the memory sticks that we've now got where you have a password for them, they're approved memory sticks that the company's got

P48: That's something I always do every time. If I go to the printer that's about ten steps away probably not but every other time I do. It's just a habit that you get into.

I: So would you ever share your account with anybody else? P104: No, no, everyone that works, that needs access will have it.

Believe not applies to them (e.g. challenging strangers) - Not following recommended practices
P89: I'm relatively new and there's a lot of people coming from outside reception that would come – but because everybody else is okay with them, I think it's okay.

Training problems (training is superficial on security, provided only to new people),
P55: I've never had any formal training. Um, everything we've been made aware of was on the induction day, "This is your password," and you're drummed in then, "Don't share it," but there's been no formal half day workshops or anything.

P8: Um, any training about security? Not really. I do know that, coming into the company, I don't know if it was a training type thing or like I said, something I just signed, but about internet usage and stuff like that, supposed to be for the company using that stuff, not really wandering around the internet

Communication problems (inconsistent, security included among other things, seems less important than health and safety)
P106: We might get an email to say, change it, but I think the five years in this office, one of the applications I've had, I've only ever seen one email to say, it's been noted, you know, whether IS has run a report to see whose changed their password.

P98: Um, that's generally a problem with most of the Company. You either get lots of communication that's not necessarily relevant and sometimes I think they miss the communication that is very relevant.

Downplaying security importance
P106: I just think it's low on peoples' priority list. I think we're so busy and we work in a culture where we prioritise everything we do and we pay compensation on job if they go.

Lack of accurate risk awareness
P79: I wouldn't think people do that. I mean I certainly on my desk is far from *clear*, but there's nothing that I consider risky or insecure left on my desk, scraps of paper notes in the margin and that sort of thing.

Misconceptions
P107: we have got firewalls and other protection, I know incoming emails are scanned for viruses, they are scanned for material that might be inappropriate, so I have got a fair degree of confidence that when things go out, when they are sent out or they come in that they are very sort of screened, and to a degree kept confidential.

Own interpretation of desired behaviours (e.g. "should write password down")
P56: I don't know the reason why. If I've ever had to take something to a formal presentation, if I'm travelling overseas or anything, then I'll use it, if I'm in the office, I'll just use a normal USB stick and then it just sits on there until it gets deleted again. And normally that's not a Company USB stick, that's one that I've bought or been given or something.

P3: I also made sure to delete them after I was done helping them out, so I don't have any use of it and I, I know that's sensitive information.

P55: Yeah, it's an encrypted stick, yeah. In the past I did have it written down in a book but I thought, "Well, what's the point of putting it in my book, if someone finds the book they've got access to everything." So I, I put them all on a small flash drive.

Content problem: Overloaded, vague, inconsistent, unrelated to role, Perceived as common sense
P46: Off the top of my head I, it's not something I could really talk about with any authority but I know we did have a computer training that we did fairly recently. Um, it was just things to do with confidentiality and a lot of it was common sense. To be honest with you, it's nothing I could just [inaudible] and can relate back it's just common, a lot it's common sense.

Ignore policy content,
P87: You don't have to read it, no. It's like the locked policies we have, you kind of know they're there, but nobody actually really sucks you down to say that you've got to read it, and understand it.

Dismiss policy usefulness,
P41: Well I mean, it is sort of like a very, I hate to use the word legalese, but it's a document that I've opened up the link before and I've skimmed through it and I said "I don't have a chance to read this." It seems to be very much in audit speak.

Devise own practices (e.g. own USB use, own password management strategies)
P95: So I always make a point, if I've ever had to give my ID to somebody, I reset my password as soon as I can afterwards… it minimises the risk … I trust people I work with but the point is that you still take the contingency measure.

No enforcement - Reduced employee motivation, Policy appears unimportant
P52: looking around the office and I can see lots of stuff lying around on people's desks that's been there for a long time. And I don't believe that the 'clear desk policy' is administered or audited on a regular basis. Perhaps the occasional walk but I can't recollect any signs of one recently.

Secure behaviour drivers

Effective security communication,
P32: I think the policies have taken steps and bounds since I passed out in the company 23 years ago…now it's a lot of online training. And I believe the company communicates very well about what their expectations are for their employees.

P86: "We've just been told not to mention it on social networking sites, because of the critical importance and the kind of environment we live in now, it's best not to share that kind of stuff. It's just company policy, that's the way they want it."

Architectural means make compliance easy (provided encrypted USB drives, personal network storage backed-up)
P17: I remember when I would go around, their hard drives would crash…lose all their documents. And we started telling people stop saving stuff to your hard drive. We have shared drives for a reason. I saw a lot of that, so I think people are getting better. I think over the past couple of years our IS security has gotten more involved than what we did.

P55: we use the security enabled ones. Well, we get a lot of gifts off suppliers that involve those and some people do use them but I bought for our team all us the security enabled flash drives.

Understanding benefits of security mechanisms and use those,
P95: I'd look at password protecting the sheet so that you couldn't open it or view it without having the password. If it was something that needed to be shared, then you could put it on a shared area providing you've got the password protection.

Challenge colleagues when needed
P99: just being wary of phone conversations et cetera so making sure that one doesn't talk about issues that people would not be otherwise aware of.

Low cost of compliance - Screen lock easy to do
P57: you can also just do Alt Control Delete and walk away, that's what I normally do - mainly because I don't want people looking, because e-mail could come in and somebody could see it, delete it, or whatever, and I might not see it when I get back to my desk. I can't imagine that anyone in my office that do that but, I mean, people send stuff to you, which is - you have no control over what people send to you, so I don't want to walk back to my screen and see something on my desktop which I didn't even put on my computer

P108: They are not allowed anything at all on their desks and they have a little locker, for their personal belongings, and a locked cabinet for their files, but they are not allowed to have any files at all out on their desk.

Clear Desk enforced by property not security - Not leaving documents around
P94: There's a very strong clear desk policy, it gets checked fairly regularly, we have sort of office walkabouts where people walk around. Looking at safety access, so hazards and that type of thing but they'll also check clear desk, a desk that's got masses of paperwork scattered everywhere and some of that is commercially sensitive, and that also, that tends to get picked up as well.

P96: There's a clear-desk policy and I like to think I'm quite tidy on my desk and I'd like to keep stuff out of the way, so stuff that is important goes in the drawer and gets locked away and then I've got some general folders and stuff on my desk.

Responsibility, Manager pressure, Peer pressure, Past events
P41: I don't think I've ever seen a company policy about it. It's just a given in the corporate culture that you would never sharing passwords… I guess what I'd say is not only is it a given for Company, I think it's just given, first time you picked up a computer and anything was password protected, it became pretty clear on and in the internet age, when you find out all the things that can go wrong on the internet, that's even more important. So I don't think it's because of a policy that I remember reading, it's just something that we're working on as a given.

P74: managers will go round and check if anything's left out that's confidential after normal office hours, and people are told that you shouldn't be leaving company confidential information out you should clearly mark it if it is company confidential, and then not leave it lying around

P115: it is certainly covered again in the team talk, it is certainly again covered when you join the company as part of your induction. I think it is more like a peer pressure that if you do forget to lock your screen, the chap who you are sat next to is more likely to come in and write a little message on your screen

P79: you know when there are recorded attacks on systems but…lots of businesses have been attacked, I mean I think if you could see the this attack happened on this company and the consequence was this, that puts it into perspective for you and you can see that actually this is real, I do need to be more careful.

Secure behaviours, Actions to protect computers, Screen lock
P52: Certainly in the team, everybody around me does the same thing. I don't think it's a conscious thing in the sense of, "Oh, there's an IS Security Policy that says I must lock my screen."

P46: 'cause the stress would be far too much to handle if I left it anywhere.

Time impact

VPN Slow, encrypted USB sticks slow, productivity focus
P18: So, I try to keep less and less on my local drive, unless I am working with a really big document, or something where I would think that if I am going to go through VPN, the speed issues might create a problem for me, saving the document type of thing.

P111: at times we do have to transfer the data to our laptops because the network is slow, response times can be really bad and some of the files are quite large, so we transfer them to our laptops to work on and then transfer them back at the end of the day.

P115: personal USB ones so you can, instead of ordering one through the company they have already got ones they just use their own.

P108: I think they will have had half a dozen or so individuals that needed this software to download the information to feedback to the team members taking part. I think it took about six weeks actually from when I put the request in, to when I actually got the software installed. I did get around it by installing it on my home laptop to be able to get some information back to the colleagues that are taking part to save them having to wait too long. And also the colleagues taking part there is a software disk in with the monitor when they take it so if they want to they can install it and have a look at their own data before it comes back to us, but it was just that we needed that software to be able to report back to them, so it could be who is winning the competition I suppose.

Unencrypted USB drives, Copy data locally
I: Do you know if there is a particular brand that you have to use or? P116: No, nothing. We just have one that we share in the office anyway. I: Is that password protected at all or? P: not to my knowledge no.

P49: You should use an encrypted one but, you know, for ease and generally because, I haven't got an encrypted one so I just use an unencrypted one, whip it across and then just delete the copy off the flash stick which isn't perfect but it's quicker, easier than having to follow the policy.

P102: I save most things to my documents or my desktop if I need to

P111: At times we do have to transfer the data to our laptops because the network is slow, response times can be really bad and some of the files are quite large so we transfer them to our laptops to work on and then transfer them back at the end of the day.

SharePoint slow to setup - USB and email file sharing
P64: but people send you links to sharepoint areas, saying here's the document in a certain area you don't have access to it because it's in a different sharepoint area that the one you have access to. You have to request access, or, more commonly, they actually send you a copy of the document across. Which obviously (is) against the whole value of having sharepoint access, where you don't send documents across.

Access control setup slow
P84: It's not very smooth. It takes weeks to get something up.

Slow IT support
P60: well we don't find them particularly useful in guiding us how we then go and resolve something.

Password reset slow
P97: Oh yes that's been done a few times. Usually on a Monday morning people forget or if you've just recently changed it and it can take about 15 to 20 minutes because Monday mornings is usually busy and any other time they do it there and then.

Share passwords
P51: sometimes people don't have access to information or systems that they need to do their job and therefore they're shared within teams. And I flagged that before that it shouldn't happen but it does. Because it can take so long to get something through that they might need to do their job. So it would be, "Use somebody else's account."

P91: That does happen sometimes. It's just partly to fill a gap in IS, you know - because we use lots of systems here, and they take ages to set up, and sometimes when someone joins a team, […] he actually only obtained access to the systems about four months later, when he was going to leave, so in the interim time, he was sort of using other people's logins.

Frustration
P44: (Changing passwords) it gets a little frustrating sometimes, but certainly I understand reasoning for it, there's nothing you can do. I wish they were all during the same timeframe so that you could sync everything, but they're all in different schedules, I don't have anything synced, they're all different.

Disruption

Filtering and blocking problematic, Block work-related information
P46: Yeah, we have a spam manager thing and so it will tell you…nine times out of ten it's just harmless, harmless stuff. And it doesn't seem to be consistent because I will have had an email from that source that's come straight into my inbox and yet on another occasion it will get blocked by spam manager.

P110: …so that you have got something that you do not quite understand, so you try and search for it on the Internet to try and find out a bit more about it and then something will be blocked because it is an educational reference. It does not quite make sense to me why it would be blocked...public information.

Send it as different file type
P2: the first trick that was taught to me was you tell them to send it as a different type of file…Change the extension so you can get the file so that you can get your work done.

Download at home and bring in on unencrypted drive
P70: ... oh that's just reminded me that Gmail you can't access that and the trouble is that's actually sometimes that would be useful to use as another way of sending emails. And I happen to know that someone was sending me a document that wasn't coming through because our fire wall was blocking it. He sent it to my Gmail account and it's still there now. And I was planning when I get an opportunity to print it when I get a chance…At home or somewhere yeah.

P115: Yes personal USB ones so you can, instead of ordering one through the company they have already got ones they just use their own...particularly it is to move obviously documents from one um, laptop or desktop to another so whether that, if they are a desktop user they might be taking it home to work on their own desktop or transferring it from their um, laptop onto somebody else's laptop for presentations, meetings those sort of tasks…you are not really supposed to take work home, but for certain Word documents, I am aware that it does happen.

Personal network drives full, Shared drives problematic - Store files locally
P33: Then I called and I got 500 more MBs. Then I called and I got 500 more MBs. So, it was, it's difficult for me because I have to call every month to get some additional space. (Easiest to do) for me is to store the work that I do on my office laptop.

P58: I know you have to request access to specific areas if you want to do something, for example, we've got a guy from university who's working with us for a few weeks at the moment. And he doesn't have access to various files and a lot of the system areas that are on our actual S drive, so we're just having to e-mail backwards and forwards bits of files…but that can make it quite difficult because of the nature of the project we've been working on spreadsheets that are shared, so two or three people using it at the same time and if we need to get this guy to do something for us as well, we have to sort of send it across to him to update it.

Recognise increased risks
P71: "I don't know how you get around that. But it's so easy to send emails to the wrong [*person*]".

P93: effectively, you will get onto the machine and once you've done that, then everything is accessible. such as outlook, there's no, server level of authentication or security, so, if anyone wants to keep their mail on their C drive, then potentially that could be an expose.

USB and email file sharing
P115: Yes personal USB ones so you can, instead of ordering one through the company they have already got ones they just use their own […] particularly is to move documents from one laptop or desktop to

another, if they are a desktop user they might be taking it home to work on their own desktop or transferring it from their laptop onto somebody else's laptop for presentations, meetings.

P107: we try and send as much as we can on, via the e-mail. I: And do they customer details and things like that? P: I guess they would yes. I guess you could identify the address from the information. For that respect for support information it is whatever the, the supplier requests.

Connectivity problems (VPN, lack of connection) - Send files to home accounts, Store files locally
P62: I do sometimes put it on an encrypted flash drive-y thing just in case I can't log on cause there are times when it doesn't like you logging on so I tend to put it on the flash drive, it seems to work just as well at home, when it's working, it's just as here and sometimes it seems faster at home, for some unknown reason.

P109: I store too much actually to be honest, on my hard disc, I have been told off for that a few times.

Encrypted flash drive procurement problems – not everyone has one - Use unencrypted ones, Store information locally, Email (personal and business accounts)
P59: there were lots of people that needed a portable means of carrying things around. And they were hit by and order for about 800 or something of them. And I don't think those orders were all approved, because the cost was just too much.

P30: …if I need to move a file from my computer to my co-workers computer right over there, they have the old communicator, we couldn't email a database. Which is stupid, because you could just zip the database and send it as a zip file and get around it anyway. But it was quicker sometimes to just throw it on a flash drive and chuck it over the cube wall. We just didn't really see the point in needing to buy an $80 flash drive to do that. The people that I work with, I'm speaking from my experience, they're all a lot smarter than me. They all have grad degrees and PHDs and stuff, and they write really good programmes, I would trust them to take some information off their computers. Especially if I had already worked with it in the past.

P49: So they will send me an email to fill in or ask me to look over it. And if I do need to make any changes I'll save another copy to the desktop send the copy I've just saved in an email and then delete the copy off the desktop.

Increased cognitive load

Different services require different passwords
P86: I think some of them require six characters, and the other one it has to be eight

P77: I know frequent password changes force people to use a password generating mechanism that's quite easy to guess, because you have to change your password every month, people would use a football team and just add on the number of the month, for instance, if it's May, it's gonna be Arsenal 5. I think people just go round robin, because they have to change their passwords so frequently. Because it takes you probably a week to remember what you've changed your password, and you're comfortable with it, and then all of a sudden you've got to change it again.

And quite a lot of the other people would write down their passwords and probably put them in their desk drawer, so I don't think that's very secure - I don't write my passwords down.

Write passwords down (ensure they don't forget those) - Own mechanisms to protect passwords
P57: I've got a book full of passwords, page full of passwords written down everywhere.

P58: I have got a list of passwords written down somewhere unfortunately. I just find there's too many to remember otherwise, and we've got a different username and password most of the time for each of each of the logins, so it's written down on a bit of paper.

P71: I've got a Microsoft Word document, which is 5 pages long now, that contains passwords for everything. Everything in my life, but mostly work, cause I don't do a lot of stuff on the internet personally…I think the amount of password-protected things leads you to the necessity to write them down, which introduces a risk.

Take own measures to protect password storage location
P58: I have got a list of passwords...I just find there's too many to remember and we've got a different username and password most of the time for each of the logins...it's written down on a bit of paper...it's locked in my desk when I've not got hold of it, probably along the laptop, which is probably not too clever.

P3: I keep them all on a note on my phone. And that's password protected as well so no one can…

P83: it's just in my diary in very small print.

Too much in the policy, No role-specific communication
P84: usually it's aimed at people who work in the larger offices rather than the operational field depots

P41: You've got probably ten hours of work to do in an eight hour day, you come to work, you look through some kind of weekly highlights of some important email notices you should know about and in one there's a link that refers you to three pages of PC security that you need to know about as an employee. Now, are you going meet that noontime deadline or are you going to go through that?

Need to decide what they think is more relevant
P60: You'd spend so much time thinking about every rule you might be breaking by doing anything that you didn't do anything.

P64: I've read through the policy and try and keep to the policy. Well, I won't say I know it off by heart. I guess you tend to read it, try and get out the salient points for yourself, two or three key cues what shouldn't you be doing, things like not using, common USB sticks to pass information around and things like that which is a recent one that's been put in place and we've got special USB sticks – and never leave a laptop in the back of the car and things like that.

Organisational adaptability

Can request removal of websites from blocked list - Slow process, No alternatives provided
P70: I think you can now phone them up, IS helpdesk direct and they'll do it there and then. Or you can do an electronic query type of thing and you'll go into a queue and at some point in the future they will contact you. Yeah it works in a day or so which is a bit annoying.

No effective delegation of responsibilities - Password sharing, Access using other's accounts
P81: It's not unknown for people out in the field to actually share laptops, and also share user IDs and passwords, for their convenience...it's not unknown for very senior people to share their passwords with their secretaries or PAs when, what they would see as a fairly menial task needs to be done and they want somebody else to do it for them

P97: There has been an instance where I have, I was off for a month earlier this year and because of the resolutions were coming through and no-one had an idea what these resolutions or this packs were not being resolved so I gave it to one of my colleagues for him to go to my e-mail to check for the resolutions and that's been the only instance I think.

Team level security communication and mediation

Lack of central communication, Lack of security training, Reliance on managers
P57: don't leave your laptop in your car, even if it's in a boot unattended, if you're putting stuff on a memory stick, make sure it's encrypted. You'll get a little things like that, and you'll see things on the Intranet, so there is a need for security, and people do tell you, I can remember that old manager - when I first joined, he used to go on at the end of the day, and when you left, like, contract stuff on top of the desk and went home he'd pull you up on it.

P100: We actually have monthly meetings, and that is where those things are highlighted. Monthly meetings where we discuss stuff across board...security stuff comes up before.

Employees seek support from line managers, Advice between peers, Managers advice on security challenges
P17: Well, like I said, we're a small group, so it's not like we have to reiterate things, told it once or twice and kind of understand so, we kind of look after each other as well.

P14: One gentleman that works in my group gave us a whole workshop at one of our team meetings, on how to create secure passwords. Not to use your pet's name and your birthday, you know, simple things that people could figure out, like your phone number.

P96: Well basically we were introduced to the security policy through my team leader. He outlined and gave us a site tour of what we can and cannot do."…"(in team talks we discuss)…if we have encountered what we could identify as a security moment it could be like you know a door being left open or your computer left being switched on or not been locked or any sensitive information lying on your desk, to be mindful of putting away security information also using a flash drive which are not company issued and stuff like that really.

P97: I think it's just kind of more, sort of, word of mouth and training, that you know you're not allowed to discuss that type of thing.

P66: as a manager you've obviously got to highlight what the areas of security are but you can only highlight more or less what you know. So you can only direct them to pages that are relevant, send them to speak to the teams that are relevant, people or if there's, if there's briefings going on they do some like brown bag lunches here, but it used to be just briefings, staff briefings. You know, you'd obviously get people involved in that but also you, you're constantly looking at yourself as a manager, checking that they're following the guidelines you'd expect. So when they are sending things out, you know, you're checking that they're not sending the wrong data to the wrong person.

They're not messing around...you know there has been instances where we've had to go through disciplinaries for people using email...you know IT abuse. So it's just moderating it really.

P95: Aside from that, if I thought there was more measures needed, then I'd speak to my manager and see whether they'd happy for it to be transferred into a different environment where they'd want it.

P108: "…I have got my immediate manager that helps me understand what I need to do and what needs to go out and not."

P29: "I know from my point of view being an analyst. If I were to ever share any information with any priority, even if I was not sure I would first go to my manager and ask him about it."

No security guidance for managers - Based on own best practice and understanding
P71: But predominantly the things I reinforce are the things I know *I* need to adhere to, so memory sticks, password protections.

P54: For managers I was thinking 'cause there's no induction, most people I suspect come in and don't get an induction. I would expect to tell them a little bit about their laptop and what they're supposed to do with it and how to use it. And a bit of the security stuff on that. But that's whether I can remember everything relying on me knowing what to tell people.

P118: I have sat down with every person that I have inducted and made very clear that if you go away from your desk lock your machines and not put sensitive documents on your desktop, try and back them onto a shared area, try to use (*secure*) cards etcetera, so that is still from a personal security point of view, it is not from (inaudible) or this is what the company believes is best security.

Access control decision making by managers (authorising access to resources), Management authorisation for information access - Ad hoc – based on manager understanding and perception - Varies by location and manager
P31: ...one of my supervisors requested access for me

P49: what would happen is, you fill in a form online saying you need this software, your manager would approve it saying, "Yes, you do need that software for this reason." It gets sent over to IS, they receive the request and send the software down to your laptop.

P53: Again, it's down to the area manager and no one else...the reason I diverted away from policy has been driven by a business requirement. And it's one of those things that's always been discussed with seniors and it's been seen as a work around because the policy doesn't fit the business requirement...

P79: the manager of each team is responsible for allocating permissions

"I: Are you responsible for their security awareness in any sense?" P98: "That's an interesting point. That's not something that has ever been particularly made clear to me. I suspect I would take that on board as a normal encompassing responsibility with regards to having people at work for me doing the right thing but I don't recall any specific guideline"

Security perception

Required to protect organisation - Motivation to comply
(on no password sharing) P70: Because it's something that I think we very infrequently do because once you're onto the main network obviously someone can access all the information, send emails as yourself, change all your permissions around. So I always avoid it. Sometimes it comes up as a bit of any solution and I've always refused to do that actually. More for personal reasons I would say. Not because I think there's particularly a big corporate risk, it's just, certainly for my own risk it's a significant risk to take.

P75: I'm kind of lucky because most of the team members that I deal with are within this (*sensitive*) section so they're already very security-focused. So they'd be the other way around, they would say "No, I don't want this to happen because it could open up - it could be less secure by doing this."

If security appears to demand reasonable time/effort AND employees understand role-related risks they follow recommended practices
P84: all this information was usually kept on paper form in boxes somewhere, and then usually sort of lost, so we got it all electronic and all on a shared area that we've got access to.

P72: you don't accidentally disclose information of one bidder to another, which means keeping information secure and kind of being aware about who you share it with and what information gets into the public domain, particularly during a tender process

Impacts productivity - Non-compliance justified
P91: I suppose I've got a skewed way of doing it, because I've never really given out any of my details to people, but I have used other people's...sometimes (*I feel*) a bit uncomfortable, you have to get a job done, and then that's how they'd justify it.

P42: So I have huge amounts of data that I have stored multiple gigabytes of email of storage going back over 10 years. Very much contrary to the written policies, but if I'm really expected to be able to use past experience, I need to be able to use my records for that experience. Email's one of the most convenient ways to do that.

Problematic security perception: Blanket rules
P60: I think occasionally we may be, possibly, overdo the rules or maybe sort of there's a little bit too much red tape that starts to make things counterproductive.

No effective guidance
P41: ...they tell you to do some things, but they don't really tell you how to do them

Access control housekeeping problematic (revoking not quick)
P66: But I would imagine there's still going to be instances where people still had access a week later or they've still got access to the shared areas...their profiles haven't been updated to reflect their changes. It sometimes takes a week, two weeks, maybe a month before they even get done and it's down to that person really more than anything chasing it to get it done. So if you've got someone who's not really bothered then they've probably still got access to it now.

P109: There is five or six people that have since left the business or, have gone elsewhere in the business but that they have the password.

Feedback goes unnoticed
P51: it was closed down five minutes later, I replied to the email and said I didn't think it should be closed down and I haven't heard anything more. My manager's now trying to chase it but that's been nearly a month, that call is unresolved...There's no channel to escalate it. And there's no ownership in IS I think is the problem because it isn't our own IS whereas before you'd know that you could go to that person's manager or they would know who to take it to who specialised in that.

No attempts to improve
P97: I mean they are talking about it, I can see there are flaws and it can be improvements so if anyone wanted to get data they could, I mean they have not followed, the USBs cannot be used but I think they just kept it at one level and just try and educate people instead of actually physically putting things in process.

Sanction based, People just comply to avoid trouble, Job security – lack of motivation
P71: I'd probably be more worried about the implications on myself, rather than other company. I don't think the company would be impacted that greatly, but it wouldn't be good.

No enforcement
P52: looking around the office I can see lots of stuff lying around on people's desks that's been there for a long time. And I don't believe that the 'clear desk policy' is administered or audited on a regular basis. Perhaps the occasional walk but I can't recollect any signs of one recently.

Varies by location
P109: I get down to (*location of other office*) quite a lot, specifically in dispatch area, it does not seem to happen as much, people just leave their machines open and walk away for a coffee or a cigarette or whatever

Security perceived as inflexible and not serving employee priorities
(Closed-built laptops) P66: You know if you want to download something sometimes, like for instance I build and design spreadsheets and sometimes I'll download that bit of code and I can't do anything with it. For me it's frustrating. But some of the things I want to take and use in some way that other people have done which would help me quicken my job up I can't do so yeah it can be frustrating.

Security rules perceived as unimportant
P87: the volunteers got big concerns really and the company doesn't seem to be doing too much about it.

P109: ...it is something that does worry me a little bit a lot of the systems that we have, they sit on a shared area where, anyone who knows the password can get in and change anything and the passwords are not really hidden that well, I mean, even if you did not really know, but you had a knowledge of the job, probably give you about five attempts and you could probably guess what it is anyway.

Perception as less important than other organisational issues
P99: What, IT security as compared to health and safety? I would say less than visible.

Employees doing what they believe they can get away with
P52: obviously there are cases and disciplinary cases where people abuse the policy and action is taken. I don't believe the management particularly follow up a lot of perhaps what the audit trail might show in terms of internet usage.

Culture perception

Colleagues willing to comply and be secure
P54: I think most of the people follow most of the rules most of the time

Productivity driven culture
P57: obviously security, you have to consider it. But it's never at the front of the supplier.

P84: they wouldn't've downloaded the policy and read through it, they'd've just used the common sense approach.

Health and safety more important
P62: We sometimes do go over the top, like all those messages about holding on to the handrail, now I always hold onto the handrail, because I tend to be clumsy and trip over but we got over the top, but I don't see security being driven from the top in the same way as safety and the carbon footprint.

Lack of awareness on many security issues
P50: And sometimes documents can't be sent. But in all honesty I'm not too sure about the Security Policy, I haven't been really introduced to it and in all honesty I've not read it. I actually have not received any formal training regarding Information Security, all I've ever been taught is how to create things.

Oversharing information
P111: We have a part of the site which is only for resource management staff only so only those people can see that part of the of the site, and then we have the different areas of the business that can only see

their part of the of the site. So it is quite a big concern sometimes because we have like three, four hundred staff potentially that could have access to it.

Contractors have different values than employees
P66: ...but also it's not just that but it's internally as well when we have contractors coming in who are replacing people who have been here longer for the sake of saving money...for instance at the moment we've had an instance where this person's sent out a couple of documents that really aren't for private viewing but they're unprotected you know.

Culture static - Need to be more proactive
P112: I think it probably remained about the same but at the same time I think they are going through a little drive of just doing it and then it just kind of stops so it is either full on, never leave your computer unlocked or nothing is said about it, but it is amazing like the difference from one building to the other, but considering, when someone starts they are not shown anything on security, that is probably not a good sign.

P100: I just think people should be encouraged to be a bit more vigilant because people don't really realize how serious it can be, so I think they should focus on security, highlight it more.

I: So, which way would you say the culture is moving? Is it that, security is getting tighter, or it is weakening? P110: To be honest from day to day things, I do not really see it moving to be honest.

Shadow Security - Company B

Category name	No	Percent
Access control easy to setup - No password sharing	43	52.44%
Access revoking problematic, Should be doing more, Information oversharing prevalent, No enforcement - Central security appears ineffective	29	35.37%
Actions to protect laptops	43	52.44%
Aware of privacy marking existence, Marking depends solely on owner, Admit to not knowing how to use these - Gets support from line manager, Overclassify	47	57.32%
Awareness about clear desk, Hot desking, Lockable drawer, Secure disposal bins, Clear desk enforcement - Clear desk compliance	55	67.07%
Awareness on the importance of information they handle, potential breaches, impact to the organisation and the need for security	78	95.12%
Can request removal of websites from blocked list - Reported problems followed up	3	3.66%
clear desk	42	51.22%
Communication at team meetings, Security support by line managers and colleagues, Devise own adaptations to unsatisfactory security measures or Introduce own novel solutions	65	79.27%
Communication of relevant regulation on sensitive information	28	34.15%
Downplay sensitivity of information they use	42	51.22%
Downplaying some risks	43	52.44%
Employees not fully aware of policies – also partially dismiss their usefulness, Managers not know complete policies, Access control decision making by managers (authorising access to resources), Management approval for information access - Ad hoc – based on	73	89.02%
Employees want to comply/contribute to security, Challenging colleague behaviour - Mechanisms demanding reasonable time/effort are followed IF employees understand why	77	93.90%
Encrypted USBs problems - Use unencrypted ones	10	12.20%

Forget encrypted USB password – lose access - Carry laptop with data	47	57.32%
Impacts productivity (e.g. email filtering/access problems, password reset problems) - Negative attitude, Insecure behaviours justified	66	80.49%
Inconsistent email filtering, Website blocking problematic - Access the information at home	30	36.59%
Information left around – picked up by clear desk inspections (“don’t happen often”), No reprimands or enforcement	20	24.39%
Managers not know complete policies, Problematic central communication and training (irrelevant, generic, inconsistent and overloaded), Reliance on managers not formalised	40	48.78%
Marking guidelines confusing, Not using those	30	36.59%
NDA people are more aware on the need to be careful with information	55	67.07%
Need to know information sharing	28	34.15%
Network drive small, Connectivity problematic, Encrypted drives - feel safe - Reliant on local storage, Ad-hoc backups (to external drives – sometimes personal), “Unintentional backups” onto local laptop systems, of e.g. emails.	64	78.05%
No lockable space - Clear desk problematic, Need to carry documents with them	46	56.10%
No understanding of data classification	14	17.07%
Not everything relevant, Aware on role-related clauses, Policy perceived as common sense	34	41.46%
Not many employees report concerns or problems - No reporting culture	11	13.41%
Not share passwords	30	36.59%
Own interpretation, Role-specific awareness, Not checking website, Not everything relevant, Colleague/line manager support	66	80.49%
Own mechanisms	67	81.71%
Password manager not work for all systems - Write passwords in documents or on paper	52	63.41%
Password protecting important documents	34	41.46%
Password resets easy - Uninterrupted access	29	35.37%
Perceived inability of the technical side to get some things right, Some generic accounts appear to exist, Sharing files through multiple formal/informal channels	62	75.61%
Policy awareness - Actively look for policy updates	13	15.85%
Policy on website – Not check	25	30.49%
Problematic organisational security communication	45	54.88%
Problematic security training	71	86.59%
Productivity driven culture, Security considered tickboxing, Lack of awareness on many security issues, Varies across locations, Need to be more proactive - Perception of security training as non-important, OK to bypass security when it creates primary task p	72	87.80%
Protects the organisation adequately, Closed-build, encrypted password protected laptops, Considered in requirements - Importance of security well understood, Employees see value in security	44	53.66%
Rely on managers and colleagues	52	63.41%
Responsibility, Manager pressure, Peer pressure, Past events - Secure behaviours, Actions to protect computers, Screen lock	70	85.37%
Responsive helpdesk, reported problems followed up - Report problems	3	3.66%
Screen lock	37	45.12%
Security and compliance measured using CBT completion rates, Too many CBTs, Information appears irrelevant, Communicated information perceived as common sense - Communication perceived as unimportant, Self (or team)-devised security behaviours	68	82.93%
SharePoint slow to setup, Access control setup slow, Slow IT support, Password reset slow	63	76.83%
Sharing drives hard to manage - Share information through emails, Also third party services used	64	78.05%
Too much in the policy, No role-specific communication	29	35.37%
Unaware of physical security policy - Not wearing pass, Not challenged	19	23.17%
Usable password manager - No writing down	38	46.34%

Various passwords for different systems, Password change rules across different systems - Keep passwords same, Passwords similar after changes, Write passwords down	58	70.73%
VPN provides adequate access – reliable, Personal network storage - No local file storage	43	52.44%
VPN Slow - Local storage	61	74.39%

Risk / need for security awareness

Awareness on the importance of information they handle, potential breaches, impact to the organisation and the need for security
P46: Very sensitive information, like customer information in VIP accounts and all this kind of stuff.

Actions to protect laptops
P70: …my laptop is never left in the car. It is left in my home obviously in my home office and it's either there or at work and if I leave it at work unattended because I've gone off to a meeting or whatever then I would lock the screen as well as that's one of the other things we're encouraged to do

Not share passwords
P54: My view is that no one will get my password, so even if I'm dead and buried, they'll have to try and work it out. I'm sure there's a way around that somewhere, but no, they don't.

Screen lock
P25: Yes I always screen lock it before I walk away, but in any case it screen locks automatically after 15 minutes.

Clear desk
P4: …But then you have to be more careful as to what people can see or what papers you have on your desk...I tend to not have paper but just a few notes. I don't print anything out.

Communication of relevant regulation on sensitive information
P19: if we do not adhere to CBTs and other things like that we can be taken to Court by either the regulator because we are not compliant with the business standards and so on that are required by Law and that would have consequences in terms of potential fines as well as brand reputation or impact

NDA presence on some projects
P39: Very strict on competition law, we have competition law guidelines, we've all signed NDA's, documents of what you can and what you can't do basically.

"Need to know" information sharing
P58: Basically, it's on a need to know basis, if someone's job role requires that information and it's confirmed that they're allowed to have that information, then you would supply them with that information.

Password protecting important documents
P33: If I was to produce statistics about the whole of Company B's something or other, then it becomes much more significant…there are certain elements of security there. A) My PC's encrypted and B) I get the statistics through an encrypted link.

P73: Yes, yes, we would password protect them, not all the time because generally they may not be saved for very long. So we have a drive that's specific for our team and no one else has access to that. So it's quite secure, but if there's something on there that I no longer need then I would just delete it. But there will be occasions when I password protect.

NDA people are more aware on the need to be careful with information

P39: I can send stuff to Company B employees and I can send stuff to Company Z employees, but I can only send stuff that's relevant to their networks…Very strict on competition law, we've all signed NDA's, documents of what you can and what you can't do basically.

Problematic organisational security communication (among other things, generic, not done, role-based)

P18: A massive amount of anacronims that aren't defined and whoever's written it assumes everyone's going to read it and spend as much time on the document as they have and understands it like they do, which is clear not the case?

P34: The other thing is of course that whilst we state the policy and we sent a note out to everybody that was misusing encrypted USB sticks, we don't ratify or remind people about the policy on a regular basis or tell them what the consequences of not using a USB stick is.

Problematic security training (CBT based, generic, tickboxing)

P22: It's for our auditors to be happy…I think we could do with doing something a little bit more interesting and a bit more of a floor stand out in the foyer, and then some education through that way.

Rely on managers and colleagues

P62: I do remind them every now and again that it's probably not best to be emailing things around. But nothing more than that I think.

P73: not really because the team's quite big and there's quite a good mix of experience so you tend to find if there's something you don't know, someone else on the team does.

No understanding of data classification

P61: I don't think that's widely understood, the different security classifications and the different treatment that that should be

Downplay sensitivity of information they use

P67: With my sort of stuff I don't think they could do any harm to the company because a lot of it is just budget information and head counts. So they'd know who was where and what grade and what pay and stuff which is confident but it's not damaging to the company I wouldn't have thought.

P34: Whereas the problem is, they're probably right, 99.9% of the time the data is not confidential, the issue is for a corporation like us, it's that 0.1% that somebody does by accident and then leaves a list of people's phone numbers along with photos of the family and leave the stick on a bus.

P65: Yes, I guess I've seen, I don't know how sensitive- I've never seen customer information, for one thing, but I have seen marketing information which, again, would be useful not necessarily to me, but useful to a competitor, if they found that. Yeah, quite often you do see, probably not confidential, but quite often you do see documents left on printers, and you know that they've been there for like 24 hours, which is always strange.

Policy awareness

Policy awareness - Actively look for policy updates

P12: … provided you've done your CBT, the point of it is, so that you know where to go and find that information even if you can't remember it.

P78: The policies that have applied to us, I'm pretty clear on; I could probably, maybe go through and list 80/90%, where I'm not sure, then I do know where to look and the policies are all documented on our local intranet pages.

Not everything relevant, Aware on role-related clauses, Policy perceived as common sense

P43: The policies that have applied to us, I'm pretty clear on; I could probably, maybe go through and list 80/90% of, where I'm not sure, then I do know where to look and, the policies are all documented on our local intranet pages. So I've probably got something like an 80/90% understanding of the policies, and the finer detail I'll just go and find the documentation.

P52: I don't think if you go through the security one or any of them a light bulb doesn't flash and think, "oh I must remember that for the future, I didn't realise that or think about that." I think it's really common sense looking at them.

Own mechanisms (e.g. use USB, erase afterwards), Downplaying some risks

P46: Oh, in a follow up email once they've received the email. They'll phone me up to say they've received it and I'll send the password. I don't know if that's the right way but that's the way I was instructed to.

P55: But the other thing I tend to do with that sort of thing is to use a USB stick to record the data on and to delete the data once I've finished, so the data is never left with a permanent impression on my hard drive of my home computer.

P6: Not that I am aware of. There probably is but not something that I'm consciously think about on a daily basis...you can probably assume that if you were looking at an account problem and the person had an issue with their billing, their billing information it's probably more important that you keep that secure than the security of the password to their mail account. You can sort of be logical really.

P34: You only follow policy when you know and understand the reason for that policy and that you're impacted by the reasons for that policy. In most instances most people aren't impacted by the reason the data they think they're transferring, they don't see as confidential so it's fit within the policies where concerned.

P5: It's unlikely. But there's no password information or anything like that. All they can literally see is, "This bit's attached to this, and attached to this and to this." So… I suppose if someone was trying to work out the structure of our network then it might aid them in that, but it's not much use to anyone.

Policy on website - Not check

P46: Over the years we've been told not to do certain things. We also have some official policy that you can refer to if you think you're doing something wrong. I never used it. You can usually tell in your gut if you're doing something wrong. If I have any queries, I'll just ask my manager.

P57: I think one of the obligations when you start is to read security policies document, which to be honest is a huge document and don't know how many people actually do read it, but I suspect very few read it end to end. But that was certainly sort of part of the new starter activities.

Aware of privacy marking existence, Marking depends solely on owner, Admit to not knowing how to use these - Gets support from line manager, Overclassify

P64: There are a range from 'highly confidential' … In fact I think there's one above 'highly confidential'. I can't remember what that is, but yes, we do have a range and all of our documentation should be marked with that and generally speaking it is. I couldn't give you a definition of what each of those were, though.

P55: No, see that's something that does strike me as being a bit odd. I sometimes see documents that have got a classification label on them, which is confidential or whatever. But I don't think I've ever really come across strict definitions of what they mean.

P61: No, I don't think that's widely understood, the different security classifications and the different treatment that that should be.

P58: If I was to share something that I hadn't been advised I was allowed to share, that impacts my own personal performance and rather than share the information, I would check with someone more senior than myself whether I'm allowed to share that information with these people and whether they should have this information.

P45: So I don't necessarily think about the other level it's either sensitive information or not, and I just kind of do it on that because it's then kind of a bit of a safer way doing it.

Unaware of marking guidelines

I: You have a division, that's important. Do, do you have an official classification of data, for example, the customer data? P6: Not that I am aware of. There probably is but not something that I'm consciously think about on a daily basis...you can probably assume that if you were looking at an account problem and the person had an issue with their billing, their billing information it's probably more important that you keep that secure than the security of the password to their mail account. You can sort of be logical really.

P73: I would just mark them as confidential, I don't use an official classification. I: Are you aware of your classification? P: No, in honesty, I'm not.

Information left around – picked up by clear desk inspections ("don't happen often"), No reprimands or enforcement

P60: …I have seen marketing information which would be useful not necessarily to me, but useful to a competitor, if they found that…quite often you do see documents left on printers, and you know that they've been there for like 24 hours, which is always strange.

P62: In my personal opinion. I think there is still too much left lying around. I don't think it's difficult to find out about things if you look hard enough.

P53: Yeah, the security chaps go round at night when there's nobody around. They'll leave little notices saying they've "picked so and so off, it's in the security room if you want it" and things like that.

Unaware of physical security policy - Not wearing pass, Not challenged
P73: I think there is a policy, I don't know how strongly it's enforced because I don't wear mine around my neck, I always have it with me but I don't wear it so that it's visible.

P57: We don't challenge people if they're not wearing a pass. If we started doing that then I think everybody would because people just sort of fall in line, but I wouldn't say that we are security conscious. I don't think we're particularly lax but I don't think that's by choice. It's just a herd mentality. People just do what they've always done and it's sort of alright, is my impression.

I: So, if you see a stranger, your assumption is that they should be, somehow, there? P36: Well, if they got passed security somehow.

Secure behaviour drivers

Awareness about clear desk, Hot desking, Lockable drawer, Secure disposal bins, Clear desk enforcement - Clear desk compliance
P29:… you'd be in a lot of trouble anyway if you know, someone went past your desk, and any sort of paper work was left lying by your desk.

P72: They collect it and lock it away when they're at work and then take it away and it goes into a secure cabinet.

P70: I say, those sort of documents tend to only stay around for a short period of time because the only the place I've got to keep documents is my carry case and I like to keep that fairly light so I'll probably just get them shredded once we've been to the meeting.

VPN provides adequate access – reliable, Personal network storage - No local file storage
P18: Yeah initially when I first got a laptop and first started working from home there were some technical glitches but that was a year and half ago, since then it's been smooth.

P32: Yeah, it's the same. What you do is you have your password to log in to your laptop. Once you've logged it's effectively just a dead laptop because you can connect to your internet at home, but you can't connect to Company B's network at all until you log in with this PIN code that you've got that no one else knows.

P30: I use that rather than my C drive, because yes, if my C drive ever broke or my PC goes missing then I lose everything and people get access to it.

P81: so from my point of view everything's backed up on the central drive; I don't keep no Company B data at home on separate discs or hard drives.

Responsive helpdesk, Reported problems followed up - Report problems
P57: I think helpdesk broadly are okay…we realised you could literally log into anyone's machines, so it wasn't just customer services'; you could go round the director's and all sorts of stuff. I think we flagged that and it got changed quietly.

Password resets easy - Uninterrupted access

P59: Yes, home page; you find the password reset form drop-down box; it's fairly straightforward.

P19: So it works, shall we say, in terms of checking that people should continue to have access to systems.

Access control easy to setup - No password sharing

P14: No, you have to wait… Once you've got authorisation you're talking minutes, if not seconds. Generally the IT people are pretty good at return, giving you access work when the authorisation has been cleared.

P1: Everyone has their own discrete access…You have to log in on your own user name and password.

Usable password manager - No writing down

P41: it's like a little security tool and if someone boots an application up, it's auto-stored the user and password for it and therefore it will auto-populate and log them in, so you don't have to remember all the different users and passwords that they've got.

P37: we don't have to remember our passwords; it does it for you, which is great, so you don't feel tempted to write it down, so that's a great help.

Responsibility, Manager pressure, Peer pressure, Past events - Secure behaviours, Actions to protect computers, Screen lock

P19: we have a huge privilege of access to a lot of information about our customers that is at the heart of our business and that the trust our customers give us in holding that information is incredibly important.

P59: If laptops have been left on the desk overnight, I might be the last person to leave the office and I may have put them in a draw or taken them home with me and brought them back in the morning.

P4: If I had an attitude where I said "oh well let's not worry about PCI Compliance for these systems" then yes I think she (their manager) would be very worried.

P55: Someone who sits near me actually used to write them down in the back of their book, simply because they had so many. I kept pointing it out. It's also one of those things about people walking away from their desk and leaving their laptop unlocked. I know that it will eventually lock itself, but they go, "Coffee, do you want anything?" and it's like, "Okay, I'm fine," and they wander off, so I'll send someone an e-mail from them.

P80: I hear a lot of stories of people leaving them on tubes and stuff like that. Most of my experience is that when people have lost them it's been in a bar in their bag and their bags been stolen. Yeah well people who've lost it in a bar essentially had it nicked…their bag will just disappear.

Time impact

VPN Slow - Local storage and external backup

P51: Yes, and I'm actually in that situation now, would you believe. It may not be completely related to password, but my VPN stopped working on Sunday, which means I cannot log on at all, other than I can still get e-mails on my iPad, but for everything else I can't get on.

P50: It's establishing the VPN that's more painful and more awkward so it's that sort of thing. To be honest, say for example, you are up and down on the train, the connectivity is not there to keep the VPN maintained so you need to keep a local copy a lot of the time so that's the reason.

Encrypted USBs problems - Use unencrypted ones

P42: Well, sometimes it just hasn't worked and it's really let me down which is really annoying because it's not like I've forgotten the password or anything like that, it's just sometimes it just doesn't work.

P11: The stuff I've ordered from it can take weeks to come through. Yes it can be a pain that.

P23: if you are working with commercial documentation which tends to be pretty significant in terms of size, there just won't be a transfer mechanism for them other than 'I'm going to stick in on a USB stick'…if it's about me standing next to an employee that I know and trust and then putting it on a USB stick that I've just provided, handing it to me and me walking to my pc, that's fine. If we're going to post it or not personally accompany it then I would encrypt it.

P76: Some people do have personal USB sticks. If they've taken a picture of something that's outside then there's no need for that level of security.

SharePoint slow to setup, Access control setup slow, Slow IT support, Password reset slow

P8: if you're not the owner of SharePoint but are working on a project and you want to store stuff onto SharePoint so it's available more widely to a certain group of people, then not being in control of that SharePoint folder and having to go to the administrator to say, "Can I have this document? Can you give me access rights?"…sometimes that's a bit frustrating because it's a delay in doing that.

P23: But when I want to get into a file it's password-protected, "What's the password? Let me in." Or access to a Share Point. If your name's not down in the database, then you need to ask the administrator…it's a ten second job for the administrator, but the problem is 1) getting hold of that administrator and 2) ensuring that the administrator who doesn't know who you are, making sure that administrator realises that there's an urgency for you

P37: It's a new contract worker coming in. We've got an organisation who now manage all our contractors. They've been waiting for their log-in details. It takes a while to come through, can take a week; you have to plan ahead, and they hadn't got them, so they've been using their managers', apparently.

Perceived inability of the technical side to get some things right, Some generic accounts appear to exist, Sharing files through multiple formal/informal channels

P54: In advance of recruiting or knowing the names of the people I'm recruiting, I need to set up all of those accesses. So I set up a generic access for those people, so in the early stages, a number of people will be sharing a generic access while we go through the process of creating LAN ID and all of the various system accesses. It was in a controlled way that it was done but it was because of the urgency of getting those people onboard and the first part of the access set up via a generic access

P5: I think there's only one or two systems where we have a generic password, like a team password. Obviously the policy is that everyone has individual passwords. It's just some systems don't allow that, so I can only think of a couple that we've got, but in general, they're all individual passwords.

I: How do you arrive at a password, if it's a team one?

P: Normally someone will just e-mail it out, basically saying, "This is what it is, if you need to access that." If it gets changed, because some of them time-out, then they e-mail it around again saying, "It's changed to this." Yeah, but there's very few.

P48: Normally e-mail, there are SharePoint sites that are scarcely get used, most people just e-mail to each other still that's the way most people do it.

P40: Well, as a team we use Drop Box quite a bit. It's not formally mandated but Drop Box works very well with us. It's private enough for the team. That's how we have most of our work stack documents or any big documents. Outside of our team, some people have tried to share SharePoint documents and it doesn't work…What other ways? Sadly back to email again.

Disruption

Network drive small, Connectivity problematic, Encrypted drives - feel safe - Reliant on local storage, Ad-hoc backups (to external drives – sometimes personal), "Unintentional backups" onto local laptop systems, of e.g. emails.

P16: I used to use a network drive but it's filled up. They give you some sort of awful limit on the network, I have about four gigs worth of data of artefacts and important stuff that I need access to and I think on the network drive they allocate something like 50 meg, it's just useless. So it all goes on the laptop unfortunately.

P4: I've got a hard drive I plug into my USB to do back-ups and that drive doesn't tend to go out of my home.

P7: all the basic raw systems data will be on the corporate main frame, but the material that we extract for our use and you know I have probably 20 or 30 gigabytes of data sitting on my laptop, together with that backed up on hard drives and so on…and obviously I encourage my team to do similar sort of back up activity. I'm sure if we scream the place down we could probably find ourselves some hard drives somewhere.

P37: I have actually backed up my data recently on to a portable device, which I keep at home, and it is secure, only because I would prefer to do it for me, but they say that's our responsibility now, because that function has, again, been outsourced, and they don't have that capability…it's my responsibility to back it up to the hard drive if there's enough room available.

P69: I've got it in my bag in fact. I do this once a week. We've got an external western digital, so that drive is also encrypted and password protected as well and basically we run a back up of our laptop probably once a week to back the files up but again we can't get into that without the correct details.

Forget encrypted USB password – lose access - Carry laptop with data

P42: Well, sometimes it just hasn't worked and it's really let me down which is really annoying because it's not like I've forgotten the password or anything like that, it's just sometimes it just doesn't work. If I go to a supplier's premises or anything like that with my laptop

P28: USB sticks are the most protective sticks in the world. I had two and I couldn't remember the passwords for the life of me, so I can't use them.

Sharing drives hard to manage - Share information through emails, Also third party services used
P6: It depends, our team one seems quite clear but I've worked on various projects before and had problems being able to access certain directories. It can be quite frustrating and then you have to get the administrator to give you access and it can take time.

P23: I love the way people believe e-mail is the only way of communicating. It's not. If you need something doing quickly, you need to ring someone.

P40: Well, as a team we use Drop Box quite a bit.

Inconsistent email filtering, Website blocking problematic - Access the information at home
P10: We looked at it and thought "Why has this been blocked?" "Why?" We never found it. They thoroughly checked the document and couldn't see what it was picking up. It'd happen fairly frequently actually.

P66: Yeah. Company B tends to be the other way around, to be honest, so you get things classified as spam that aren't which is frustrating, particularly when some of them originate internally on our network.

P54: It's difficult to say. In my view, there's one particular site I was trying to get access to that had come back saying, "This site has been blocked," that in my view wasn't really … But then I could kind of see they were erring on the side of caution, so I just said, "Okay, fine, fair enough. I won't bother, I'll do it at home."

Password manager not work for all systems - Write passwords in documents or on paper
P44: I have the application that's installed so that updates the system as and when it needs to and if I need to manually go in there and change it I can do that by that method but I also have a back-up which is my outlook in notes.

No lockable space - Clear desk problematic, Need to carry documents with them
P23: I have a couple of key documents for me in my laptop bag. They are strategy presentations printed off. Like I've just done now, anything that's on the desk I put … everything; wallet, charger off the phone, I'll unplug it all and put it in my bag and leave my bag on the desk here. I'm not going to walk it around. I like to think I'm secure here.

Increased cognitive load

Various passwords for different systems, Password change rules across different systems - Keep passwords same, Passwords similar after changes, Write passwords down
P4: I would make them as simple as the system would let me get away with and I would record them in a word document. So it's not all that secure but if there's so many of them and 'remember me' won't work. I can't remember them all.

P10: You don't necessarily, you don't write them in a notebook, put it that way. I: So it's like a secure Word document on your computer or laptop or something like that. P: Precisely. Yes.

P56: Yes, so what I used to do is whenever the first one came up that needed to change, I'd then change them all to keep them in sync. It's not long really, 10 minutes, quarter of an hour you've kind of done it. It's just I think there's a tendency with that sort of thing to complain about it more than to actually just get on with it and do it.

Too much in the policy, No role-specific communication - Own interpretation. Role-specific awareness, Not checking website, Not everything relevant, Colleague/line manager support

P82: I obviously know the general jist of most of the security policies but I wouldn't say I know the in-depth detail of everything.

P39: They are very easy, I'll just have a quick look through one now. Yes they are fairly clear. It's basically common sense, common sense, common sense.

P7: Well for instance would be that if I am copying a draft report to some of my team to review, I might even though it's screamingly obvious to them, I might still reinforce the message in the covering email, by reminding them that this contains customer information, that sort of thing. So it's a sort of apologetic reminder that they need to do what I know damn well they will do. It's the way you reinforce those sort of messages…It's my personal way of approaching it, whether or not it's company policy I don't know. But again I think with a lot of these things, there is an element of common sense in them, making sure that the you know papers have all the right confidentiality markings on, which definitely is company policy and then reminding everybody if you're sending them a draft or something like that, or what the intended circulation is, who they shouldn't send it to if necessary.

I: Are you aware of the general security policies? P46: I know where they are. I: Do you ever refer to them? P: No. I: Have you ever read them? P: I've been here a long time. I probably have.

P30: Probably a broad principle, rather than detail, I'd have to say.

P58: Yeah, if I'm discussing something which is confidential I will make sure I tell them I tell them it's confidential, "please don't talk to anyone else about it." We recently had an incident where someone had joined by team and they had had an incident in the office. I needed to brief my team, "this is confidential, please don't talk about it"

Marking guidelines confusing - Not using those

P61: No, I don't think that's widely understood, the different security classifications and the different treatment that that should be.

I: Is there an official classification? P70: There is, yeah. I: Do you know the levels? P: No. I know one is more severe than the other but I couldn't tell you specifically what we're supposed to do and not do.

Organisational adaptability

Can request removal of websites from blocked list - Reported problems followed up

P57: But it was only when the password changed that we realised you could literally log into anyone's machines, so it wasn't just customer services'; you could go round the director's and all sorts of stuff. I think we flagged that and it got changed quietly.

P22: You can e-mail a particular group who will unbar it for you, and they'll let your line manager know that you're doing it. No it's pretty quick, I've not needed to do it recently, but it's pretty fast like that if people have a good reason to do something.

Not many employees report concerns or problems - No reporting culture

P46: I think the reality with most things is to stay ignorant. I wouldn't go up to the head of F and S if I was outside and say "I'll do this and I'll do that" and he'd go "you're not supposed to do that" , you'll get told off

P17: Probably, it depends- if I saw someone on someone else's computer and they were doing something, if it didn't know them, I don't know, probably ask my line manager what to do.

Team level security communication and mediation

Managers not know complete policies, Problematic central communication and training (irrelevant, generic, inconsistent and overloaded), Reliance on managers not formalised - Communication at team meetings, Security support by line managers and colleagues, Devise own adaptations to unsatisfactory security measures or, Introduce own novel solutions

P71: It would be filtered down from myself, or if there's anything I need to talk to them about it will be passed out to them all via a group e-mail. When they first join the company, for example, we do an induction where we cover things like security policies and we ensure that they do their CBTS and things like that.

P56: I think there is a general practice that your line manager is a bit more switched on to these things. So if you have these questions, it's really the line manager and then the line manager can either direct you, help you or just tell you to go and read it yourself.

Employees not fully aware of policies – also partially dismiss their usefulness, Managers not know complete policies, Access control decision making by managers (authorising access to resources), Management approval for information access - Ad hoc – based on manager/colleague understanding and perception

P52: I don't think if you go through the security one or any of them a light bulb doesn't flash and think, "oh I must remember that for the future, I didn't realise that or think about that." I think it's really common sense looking at them.

P57: I: And do you ever discuss security with them? P: No. I'd expect him to tell me if there was some significant change in policy or if someone in the team had done something naughty, but broadly, no.

P7: It's my personal way of approaching it, whether or not it's company policy I don't know. But again I think with a lot of these things, there is an element of common sense in them, making sure that the you know papers have all the right confidentiality markings on, which definitely is company policy and then reminding everybody if you're sending them a draft or something like that, or what the intended circulation is, who they shouldn't send it to if necessary.

Security perception

Protects the organisation adequately, Closed-build, encrypted password protected laptops, Considered in requirements - Importance of security well understood, Employees see value in security

P68: security is very high on our agenda, and like I say, from other departments, from the experiences of other departments, like customer services, they have to do the DPA checks, and if they fail a number of DPA checks, then they're reprimanded basically, for want of a better word, and the calls are recorded and listened into by their managers.

P35: that's the fundamental reason we try to engage security soon enough, because if you get too far down the road and the reason is, "No, you've got to stop what you're doing because you're doing it wrong," at that point you've gone so far down the road that you've got to backtrack and you may then end up having to launch a product without key features in it because you've not secured them.

P79: However if we were putting something brand new in, it wouldn't be acceptable for it to not get to the current standard.

Impacts productivity (e.g. email filtering/access problems, password reset problems) - Negative attitude, Insecure behaviours justified

P35: It's mainly usability. It's things like the whole password and log in thing was causing me a bit of an upset this morning. It doesn't seem to be able to make its mind up whether it wants my generic LAN password or it wants my Share Point password which sends me into a bit of confusion. Once you get there, there's limits on the size of files, it takes a long time to upload and it's not very clear whether it's uploading properly or not so all you get is the browser, the blue bar at the top, which goes a little bit of the way and stops and then, in my case, times out, so you've got no idea whether it's working, whether it's good or not. Whereas you're going through all those steps, in Drop Box you just pick it up and lob it in and it's done.

I: Have you used SharePoint before? P28: I've used them but I don't really like using them very much. I'm going on maternity leave next week and the guy taking over from me said, "I've assumed you've put everything on SharePoint?" It's just not my thing really. I don't really do that. I just don't really like the system. I have used them in the past when I need to share things with people when there are lots of people. It's just a personal thing. I never really got going with it.

P69: Yeah I store quite a lot of stuff locally on it…convenience, speed, getting stuff quickly. We don't have that much space really that we can share on our file as well. It's a bit limited and I've actually more space on my laptop than I've got on my shared drive.

Security and compliance measured using CBT completion rates, Too many CBTs, Information appears irrelevant, Communicated information perceived as common sense - Communication perceived as unimportant, Self (or team)-devised security behaviours

P54: I must admit, a CBT is just one of those that you end up having to do. You're obliged.

P25: So I think the security one is every three years. Yes, part of my role is to make sure that people do those courses and chasing up line managers to make sure they do them. It's very difficult, some people just do them and don't complain and you know that's fine, but others, I think they see them as being a waste of time and slows them down on getting on with their real job, as they might put it.

P45: Yeah, yeah, there are. There are, and what you should do with your laptop, you know, where you should and shouldn't leave it, and stuff and nonsense.

P56: So yes there have been odd occasions when I have done some work on my own computer. I know that security frown quite a lot on that, they don't like that and their principle is if you need the tools for the job, the company should be providing those tools, which is a fair statement, but sometimes I know that I can do things with my personal computer … different operating system, I can do something with my own computer and do it very quickly, that I just can't do at all on my work one.

Access revoking problematic, Should be doing more, Information oversharing prevalent, No enforcement - Central security appears ineffective

P29: We've always had probably I feel the right level of security there anyway the only thing is probably pick on as I said is if you had certain people who had access to folders who probably should no longer have access to these folders. I probably say even throughout the company it seems to be, you know I had a request come through recently regarding the system which I haven't used for donkey's years. Saying, "Do you still require the system?" The answer is, "Well no; I haven't needed access to that system for about ten years or so to be honest…"

P23: Yes. 'View' is my default. I think I am the owner of the department's only group share, but people generally don't use that. People like to e-mail information, which is flawed in my mind, because if you host information online with the right levels of access, we don't need to actually … First of all there's this data concern. So if you imagine you send me an e-mail with an attachment that's quite big to 10 people. That person then replies, "Thanks," with the attachment; we've just doubled up our capacity when we don't really need it. That kind of bugs me. The other thing is, I don't know how many times in a day I get phone calls saying, "Have you got this file? Have you got that presentation?" I've just received an e-mail: "Can you all send in your slides. 'Reply all' so one can see what we're all putting together." It's completely flawed. Why are we doing this all over e-mail? What we should be doing is hosting this in a Share Point where we all load up our information, you can view each other's and that's the most up-to-date version. If I haven't got it, it's there, so if I get hit by a bus, they don't need my laptop; it's already on the Share Point.

P34: But I'm being totally honest and open with you, I think it's a case of rather than people not understanding the policy, it's the policy not being policed.

P9: There's not a rigidly enforced clear desk policy that I'm aware of. I do have an assigned desk in the office, so I don't hot desk or anything like that and I wouldn't call mine a clear desk

P55: So there was a notice came round driven by security, saying these things were available, so if you must use sticks, we recommend you use these one. So that was kind of the information and I actually proactively went and ordered it. It was up to the individual to take action.

P7: … there are always you know dozens and dozens of files on the thing, often with obscure names and things. I suppose if you were a baddie you could probably spend your life going through some of these files to see what you could find.

P48: Well the trouble with it, you kind of go 78% of the way on your own and then at some point you decide that you need the OK from the guys and they need to look through it. The issue for them is there are just not enough of them to really look at everything.

Culture perception

Employees want to comply/contribute to security, Challenging colleague behaviour - Mechanisms demanding reasonable time/effort are followed IF employees understand why

P28: Yeah, I think they do, I mean, people just leave stuff lying all around, I once went into a retail store and there was somebody's bank details lying around and I went absolutely mental.

P53: I've done a couple myself. Generally if somebody's said, "So and so, can you go and look at so and so's customer details. The account is this, the password is that," and we say, "You do not send passwords."

P67: Mandatory training is in place and I think people's brains are in the mindset that you've got to carry your pass, don't leave your laptop on show. It's sort of embedded into people, people that I know anyway.

Productivity driven culture, Security considered tickboxing, Lack of awareness on many security issues, Varies across locations, Need to be more proactive - OK to bypass security when it creates primary task problems

P66: if you are working with commercial documentation which tends to be pretty significant in terms of size, there just won't be a transfer mechanism for them other than 'I'm going to stick in on a USB stick'. I: So, whether to encrypt or not to encrypt, do you decide it based on the sensitivity of the information or ...? P: Yeah, it depends on the sensitivity of the information and, if you like, the nature of the transaction. So if it's about me standing next to an employee that I know and trust and then putting it on a USB stick that I've just provided, handing it to me and me walking to my pc, that's fine. If we're going to post it or not personally accompany it then I would encrypt it.

P22: Just an opinion, I would say we're far more focused on what we do and our results and the customers, than we are about things like that.

P50: Yeah sometimes you see people printing things out. It's the rare case that you'll go to the printer and find that somebody's printed something and it's ended up on their own printer or whatever else, that sort of thing. I think we've done good work in one location in minimising the risk of that because, I don't know if you aware of it but you have to go and collect your printing with your pass card. In other locations we don't do that.

P25: 'Oh my log in is locked out and I didn't want to delay this conference call, so I used my mates'.

P50: Because some of the security constraints are messy, for example, some of the SharePoint sites require different log-ins that some people now and, some people aren't that good at maintaining so therefore to avoid complexity some are just emailed.

P63: I have one from the company that's encrypted that keeps locking up, and you have to bin it because it locks up, but I have my own that's easier.

P77: Well, I mean, sorry, I do have a number of occasions to try and upload files and I've just resorted to doing the 'download to laptop, disconnect, upload' sort of thing because it's easier, I guess, if slower.

Trust

Category name	A	Pct	B	Pct	Total	Pct
Accept the need for security mechanisms and policies to protect the organization	104	88%	80	98%	184	92%
Close relationship with their colleagues	49	42%	30	37%	79	40%
Communication of related risks and the need to protect the organisation	66	56%	57	70%	123	62%
Conflict between trust relationships, Policy demands no inter-employee trust	113	96%	75	91%	188	94%
Contractors have same access	30	25%	1	1%	31	16%
Desired behaviours outlined in policy	65	55%	31	38%	96	48%
Employees recognise organisational reliance on them	83	70%	60	73%	143	72%
help each other - collaborative protection	11	9%	3	4%	14	7%
Inter-employee trust relationships prevail	108	92%	63	77%	171	86%
Intrinsic compliance: Ability: Employee knowledge and risk awareness to protect the organization	97	82%	78	95%	175	88%
Intrinsic compliance: Motivation: understanding responsibility - propensity to do good	44	37%	37	45%	81	41%
Mechanisms implemented to prevent insecure behaviours	105	89%	71	87%	176	88%
Policy clauses defining desired employee behaviour without enforcing it	48	41%	25	30%	73	37%
Potential sanctions defined in policy for bypassing security	25	21%	10	12%	35	18%
Problematic assurance mechanisms slow down or disrupt primary task - Need to bypass mechanisms or ignore policy	105	89%	74	90%	179	90%
Recognize breaking organization-employee trust	84	71%	48	59%	132	66%
Self-devised security mechanisms	96	81%	68	83%	164	82%
social capital development	10	8%	4	5%	14	7%
Temporal incentives: Sanction avoidance	40	34%	23	28%	63	32%
Trust enabler to productivity when security is problematic	43	36%	17	21%	60	30%
Understand potential problems to the organisation by a security leakage - understand contribution to organisation protection	104	88%	72	88%	176	88%

Assurance

Understand need for restrictions

Understand potential problems to the organisation by a security leakage
PA60: Certainly from financial information we have a lot of knowledge and information that could affect stock market value of the company. You know we hear about recent things that maybe in advance to the public.

PB11: I guess in the area that we cover there is a risk there that if the policy wasn't enforced people could access customer's information and sell it on.

Accept the need for security mechanisms and policies to protect the organization
PA18: I feel that's much more safer because okay, I am responsible. I know what I'm doing, but still, sometimes I can just make a mistake and here I go. I downloaded something which is in fact affecting everybody else, so and the company will just sort it out, if we get into any trouble and especially with the kind of information with your work, with regulators and all that stuff, I mean I'm sure, the servers will (be) much more secure.

PA78: There are certain things and certain criteria that you need to be abiding by and which has to stay within the confines of the company, and you're employed, by the company to be able to keep really hush about that

PA102: …I think there's a balance to be struck between giving people trust and appreciating their common sense and their intelligence and also protecting one's system from the occasional stranger who walks through the area.

PB70: So there's always that reminder and then everyone I work with is very security conscious in any case, it's kind of securing things but also not talking about things because a lot of the projects I work on are quite commercially sensitive in terms of if the competition were to get wind of them it would weaken our market position.

Understand their contribution in protecting the organisation
PA77: I think it's almost like a badge of honour for the chaps I work with and they feel quite proud to be working in that environment, so they're quite happy that it's secure and it's considered a secure location, so they're quite happy to go along with any policies that are implemented.

PA99: …I think there's a balance to be struck between giving people trust and appreciating their common sense and their intelligence and also protecting one's system from the occasional stranger who walks through the area.

PB58: If laptops have been left on the desk overnight, I might be the last person to leave the office and I may have put them in a draw or taken them home with me and brought them back in the morning.

PB71: I make sure that the documents that we send out are marked relevantly or only shared with the necessary parties, things like that really. We just ensure that we're not doing anything untoward really.

Mechanisms and policy compliance

Desired behaviours outlined in policy
PA114: ensuring that you know, my team are actually aware of information security policies, processes, call it what you will, of which there is a plethora on our Infonet.

PB11: there's also pages on the intranet so the security team have their own section on the intranet where you can go and look for specific information if you're unsure of what the policy might be around a particular type of access.

Mechanisms implemented to prevent insecure behaviours
PA72: Not to use your own memory sticks but to use the memory sticks that we've now got where you have a password for them, they're approved memory sticks that the company's got

PB47: If I want a contractor to go in there I have to fill out an access form telling them exactly what they're doing, where they're going to go there, and how long they want it for; and once it goes past that, that access is revoked, and they can't get in there.

Potential sanctions defined in policy for bypassing security
PA71: I think the penalties for not following the security policies are increasingly getting harsher. I think as a result people are more mindful and I think also with various other things that have gone off in the external environment it does, sort of, heighten awareness.

PB14: It could be dismissal and potential prosecution I would imagine, dependant on the sensitivity of the data, I mean we're not allowed to talk about products to other peers in other companies, so we wouldn't do that. Obviously that's breaching data protection Act, it's breaching copyright, it can be breaching all sorts of security risks. So it's certainly not something I'd do.

Temporal incentives: Sanction avoidance
PA8: So there are people out there that are watching, enforcing, I guess.

PB72: one of their activities during the course of the evening is to patrol and if there are things left on desks to collect them, they make a record of where they were collected from and then contact the person who's there the next day to say that "they've left this and were they aware?"

PB73: The trust has always been there, but the consequences are also there if it's broken.

PB21: Because, they could do something on the system, and other people would think it was me. Because, if somebody used my password, they could do something detrimental, and then it would be me that would get (in trouble).

Organisation-employee trust

Employees are trusted by the organisation

Policy clauses defining desired employee behaviour without enforcing it (e.g. don't share passwords, use encrypted drives)
PA87: You don't have to read it, no. It's like the locked policies we have, you kind of know they're there, but nobody actually really – sucks you down to say that you've got to read it, and understand it.

PA93: I'm pretty free for whatever premise that I wanted access. It's not being audited. I could effectively, if I wanted to, get away with not having to focus too much time on security issues and more on delivery issues.

PA82: obviously I mean, if everybody is working on confidential information, it has been pointed out that at various meetings et cetera, that that should be done, as a matter of security.

PA71: I think the onus in our company these days is a lot to put the responsibility on the individual. But the consequence of that, is that quite often the consequence of *not* complying aren't just a risk to them

PB34: Now, we have an internal policy that says documents should be marked as 'confidence' or 'in confidence' and not everyone follows that particular policy. So, for example, the use of encrypted USB sticks is to ensure the right policy is used and maintained. Whereas at the moment, the policy stands and people know the policy stands but people don't always follow that policy.

PB56: I think it's encouraged, whenever you talk to the right people it's encouraged, but it's not enforced…So there was a notice came round driven by security, saying these things were available, so if you must use sticks, we recommend you use these one. So that was kind of the information and I actually proactively went and ordered it. It was up to the individual to take action.

PA57: somebody said "Oh, I'll set you up on this, I'll set you up on this" […] that's just because they were sitting next to me, that wasn't just their job, or anything, it's no one's particular job to set people up on different systems.

PB67: I guess it's judgement and what you're working on and whether the data is sensitive (inaudible) so head count, people's name and grades and stuff are obviously sensitive so I would put a password protection on that. But if it's just an overall (inaudible) that everybody can see then probably not. If it's budgets that need to be seen by everybody then probably not.

PA7: It's my personal way of approaching it, whether or not it's company policy I don't know […] reminding everybody if you're sending them a draft or something like that, or what the intended circulation is, who they shouldn't send it to if necessary.

PB74: Whenever I do transmit confidential information, it's on a needs-only basis so it's on a need-to-know principal. […] I will remind them as well, verbally, when I'm speaking to them that this matter's confidential and remind them that they're not to discuss it further. [...] You might grant access to all the

members in your team, you might grant access to a specific folder for a group of people. So it tends to be managed locally I believe with local admin rights.

Communication of related risks and the need to protect the organisation
PA7: We do get the communications. Once in a while we get, you know, emails, like corporate communications and, you know, things like that or, a specific system, they have their own emails that go out and says, you know, "This is happening," or, you know, "Do this, do that."

PB27: So, we have an intranet where basically what I would call…I suppose…for want of a better word company notices or points of information are portrayed. If there was a requirement to drive home some particular messages I would expect them to come through the intranet.

Employees recognise organisational reliance on them
PA7: We do get the communications. Once in a while we get, you know, emails, like corporate communications and, you know, things like that or, a specific system, they have their own emails that go out and says, you know, "This is happening," or, you know, "Do this, do that."

PB80: (talking about security implementers) so long as we tell them that we're going to do something, they'll trust us to do it, they won't necessarily come along and sort of sit behind you and make sure you're actually implementing that piece of design.

PB23: We tend culturally to be allowed more freedom and responsibility than some people might do…It's almost impossible in security terms to stop a human actually attaching a document when they shouldn't it's very difficult to get round that.

Intrinsic compliance - Ability: Employee knowledge and risk awareness to protect the organization
PA7: There's deeds, easements, things like that, that people, sort of secure information that anybody can just grab. So things like that they want to be more careful on, you know?

PB69: (talking about USB drives) No, they're more trouble than they're worth because you could potentially get into trouble with those things, leaving stuff on them that you shouldn't do, and leaving them lying around, they're just too easy to lose, so I don't use them.

PB17: we are using a lot data and we know the impact that has on the company and the customers if that gets into the wider domain

Intrinsic compliance - Motivation: understanding responsibility - propensity to do good
PA83: I think *all* the data I work with is very sensitive. And, from what I've seen, you know, the company is quite serious about securing its financial information and all the applications I deal with are password-protected

PB58: So maybe I'm not the right person to take those risks and make those choices, but I think we all have to share that that's part of the ethos of the company.

Breaking trust

Problematic assurance mechanisms slow down or disrupt primary task - Need to bypass mechanisms or ignore policy

PA2: …they'll take their company computer off the proxy, and while you're off the proxy, go home, log in, grab the files, save them, come back in, you're back on the proxy, you're okay.

PA52: Because they keep expiring. So we maintain a set of seven generic accounts for each position which are known only to the control room and are kept in a secure procedure which is administered closely and is only known to the control room.

PA13: I think the email, they block everything, sometimes maybe I just want to print out something, you cannot send email, so I just used a USB drive.

PB37: I mean, at the moment the IT policy, which I have to enforce as the delivery manager, is it has to be secure and (inaudible), and the mechanism we have to go through … and this takes time … is if the business doesn't want to pay for that, then it has to be escalated to senior level relative to the risk, and the business has to then decide, are they going to take that risk, yes or no? So you have to go through all those escalations to move the project forward, and the business will decide whether it's an acceptable risk or not, you know; so it's the right thing to do, but it takes time, and time is money, and it delays projects; and then the business owners are unhappy both ways, you know.

Recognize breaking organization-employee trust

PA31: There's a policy that they shortly after we moved to this building they made a big deal out of "Don't allow following access through doorways…and I don't think most people take that terribly seriously, and it's kind of hard to, it seems kind of impolite to say, "Sorry, no, I can't let you through, I'm going to have to slam the door in your face. Human nature tends to be I'll hold the door for you, so, so I think that's, those are kind of at odds.

PA53: The reason I diverted away from policy has been driven by a business requirement. And it's, it's one of those things that's always been discussed with seniors and it's been seen as a work around because the policy doesn't fit the business requirement.

PB56: So yes there have been odd occasions when I have done some work on my own computer. I know that security frown quite a lot on that, they don't like that and their principle is if you need the tools for the job, the company should be providing those tools, which is a fair statement, but sometimes I know that I can do things with my personal computer and do it very quickly, that I just can't do at all on my work one.

Inter-employee trust

Trust between colleagues

Close relationship with their colleagues
PA2: And because of that, a lot of times the field guys, they won't tend to trust you initially you've got to be there for a while…like now that I've been here three years, "Oh, I've worked with him a lot. Not a problem, I like working with him."

PA57: I mean SharePoint is good, but you have to be trusting for users to use it properly.

PB3: You work with them so much. God, the engineers that I work with for our company I spent hours with them on a daily basis, so you do get to know them very well.

Prevailing over organisation-employee trust

Conflict between trust relationships - Inter-employee trust relationships prevail
PA12: "*…as far as "Oh, this contractor wants to get something done quick, here use my ID for doing that. You know, and then I'll switch the password after. Okay, he's sort of protected it, but really is, you've just shared your ID, you just shared a password, and with a non-company person, you know, violation, but you need to get your work done.*"

PA70: "*…before when we had like our group meetings, even though we were contractors, we were also allowed in those meetings, but as an employee, I felt myself to be more a part of that group now, because now we belong to the company*"

PA9: "*…when that contractor was still there I wasn't told to treat contractors differently.*"

PA41: "*I saw this co-worker who was being hired as a contractor and I called the woman […] and she calls me back in a couple of days from now and she says "I checked it out and found out that that wasn't really another person, that was me…*"

PA90: "*…a lot of times the field guys, they won't tend to trust you initially you've got to be there for a while. Like now that I've been here three years, "Oh, I've worked with him a lot. Not a problem, I like working with him.*"

Trust enabler to productivity when security is problematic
PA2 (on password sharing)*: I have some level of trust with them, it's more if they have enough level of trust with me to be "Okay, here's the thing so you can log in and do it quick. I'll change it as soon as I come back so that we're secure and all that but I need you to keep working to get the job done."*

PA116 (on not locking their screens): "…because when you comment on it and say "Well you should actually be locking your screen when you walk away", the comment you get back is the fact that "Well you know we should be able to trust people around."

PA78: I mean the employees, you can share to the employees, because they don't talk amongst themselves because obviously they know the policies of the company as well. So when you're an employee of Company A and I speak to another employee of Company A, it's not a problem, because everybody knows what the security policies are with the company.

PA118: ... it is very rare for a new starter to have that kind of trust given to them within the first, let us say month or so. So it is probably between very trusting colleagues that passwords are handed across to each other.

PB3: I mean I assume that this is our building and it's all trusted people working in here and therefore I act appropriately on that basis. If my laptop gets nicked then I'll notch my estimations of the building down slightly.

PB18: well if someone's into the company and they need a certain document they know where to find it then pass it on.

I: So if someone asked you to share your password with them, you'd have no problem with that? PB6: No, as long as it's a trusted colleague.

PA30: "…*But it was quicker sometimes to just throw it on a flash drive and chuck it over the cube wall. We just didn't really see the point in needing to buy an $80 flash drive to do that. The people that I work with, I'm speaking from my experience, they're all a lot smarter than me. They all have grad degrees and PHDs and stuff, and they write really good programmes, I would trust them to take some information off their computers.*

Self-devised security mechanisms
PA95: So I always make a point, if I've ever had to give my ID to somebody, I reset my password as soon as I can afterwards…it minimises the risk … I trust people I work with, but the point is that you still take the contingency measure.

PB3: Well, it depends who's working on the platforms as well, what's been done; for example, if we've had to give temporary passwords to an engineer, or someone like that, we will change the password, give them their own password, and once they're done we will change them back, so nobody ever actually has the official passwords except the engineers themselves.

Appendix J: Survey results

Company A

Scenario A – File Sharing (Behaviour)

Jessica, a Business Analyst at a utility company, needs to share a large volume of files with colleagues in her department as part of a high priority task she is undertaking. These files contain “Confidential” company information for “internal use only”. Jessica has made the files available through Microsoft SharePoint, restricting access to certain team members. Some team members tell her they cannot access the files due to incorrect permissions, so Jessica has submitted a request for changes to be made to her colleagues’ permissions and escalated this due to the urgency. However, she knows from past experience that it may take up to 1 week for the changes to be approved and applied. If these files are not made available within the next 2 working days, this will severely impact delivery and quality. As not all of her colleagues require access to all the files, to manually distribute them would involve her identifying the subset of files for each person - this will be a very time-consuming task, so Jessica creates an archive of all the relevant documents and considers how best to deliver it to the group.
Option A: Request that those with access share their (main log-in) account details and passwords with those without to allow them access to the information.
Option B: Burn a copy of the files onto a CD/DVD and distribute to the work group.
Option C: Email the document archive directly to the general work group mailing list using your company email address.
Option D: Move the files to an unrestricted folder on the internal network to allow the work group to have continued access to it.

N	877	Number
1st	8.44%	74
2nd	29.76%	261
3rd	46.98%	412
4th	14.82%	130

Scenario B – Managing Permissions (Behaviour)

John is a System Administrator at a utility company responsible for deciding who has access to confidential information.
John normally reviews each request and then applies the most appropriate permissions, or the request is denied according to established procedures and guidelines. He undertakes this task every 24 hours to ensure there is no risk of maintenance schedules slipping due to a lack of access to records.
John is called away from the office on short notice by a family emergency and he is concerned about how this task will be managed during his absence. The system used to set the permissions does not easily allow him to deputise the task to another account, so he must find another way to ensure this activity is completed while he is away. He is also concerned that as the guidelines are not always clear and require some degree of discretion when granting access, deputising the task may mean there is a higher risk of incorrect permissions being granted. This makes the choice of who to trust this task to in his absence an important one.
Option A: Leave your password with your secretary, who although temporary, is a trusted employee, with instructions to use your account to resolve "emergency situations".
Option B: Leave your password with a trusted member of the department and ask them to handle "all decision making" while you are away.
Option C: Grant blanket access rights to the whole department (clone of the permissions of an individual with the most access rights) for the duration of your absence to forestall many of the access requests you are usually is asked to deal with.
Option D: Give out login details of a range of access permissions (used by temporary workers) with instructions that they be used where existing permissions do not allow access.

N	865	Number
1st	17.80%	154
2nd	52.49%	454
3rd	7.40%	64
4th	22.31%	193

Scenario C – USB Stick Usage (Behaviour)

Jason works for a utility company as a Commercial Analyst and is currently involved in an important project that requires him to present progress updates to clients, often in offsite locations.
Jason would normally use his laptop to take presentations to clients but his laptop is currently in for maintenance. Instead he decides to use an encrypted USB memory stick to transfer the required files to the client site. Unfortunately, shortly before he is due to leave for the meeting, Jason realises he lent out his encrypted USB stick and cannot recall who to. He knows he will not get a replacement at such short notice. In the meantime he still needs some way to transfer information. The presentation includes embedded media and is therefore too large to email and he knows that offsite locations cannot access the internal network.
Option A: Take the required data on an unencrypted USB stick - you have one to hand.
Option B: Borrow an encrypted stick from a colleague. You would have to also make a note of their password so you can access the data at the client's site. The colleague had asked that you do not share / erase the confidential data already on the stick.
Option C: An employee of the client has been visiting the utility company and is due to travel back with you. Use the available unencrypted stick to put a copy of the data onto their laptop and ask them to take it to the client's site.
Option D: Upload the files to a public online data storage service and recover them at the client's site.

N	133	Number
1st	36.84%	49
2nd	45.86%	61
3rd	9.77%	13
4th	7.52%	10

Scenario D – Tailgating (Attitude)

Agnes works for a utility company as a Customer Account Manager and often has meetings on site with external visitors.
Agnes is aware that visitors need to be supervised at all times and security / reception are made aware of all visitors. She therefore personally receives visitors and allows them entry/exit through the barrier door which requires an ID pass and further supervises them whilst they are on site.
Whilst collecting visitors she often sees unsupervised people without a visible visitor's badge waiting near the barrier door and occasionally ‘tailgate’ (follow closely behind another person) to get into the main building. Although Agnes appreciates that this is a security risk, she is also aware that this is a common occurrence which is normally overlooked.
Option A: Notify security that you have observed visitors tailgating past the barrier.
Option B: Confront the people you see tailgating directly and ask them to show you some ID (if they are not known to you) and supervise them back to reception.
Option C: Assume the people have access and have been checked by the reception staff and continue with your work so as not to disrupt their work or yours.
Option D: Confront the people and then report their names to either your manager or security.

N	359	Number
1st	34.26%	123
2nd	57.38%	206
3rd	4.46%	16
4th	3.90%	14

Scenario E – Document Control (Attitude)

Anne works for a utility company as a Compliance Officer and is responsible for managing and handling documents containing sensitive Critical National Infrastructure (CNI) information. Only certain people can access and use this information, provided they have gone through the appropriate vetting.
Anne recently received an angry phone call from Bob (Senior Manager) who is not happy that his staff no longer have access to important information they need. Anne explains the vetting procedure to him, but he is still not happy and asks to speak to her boss Cyril, who supports Anne and tells Bob that his staff require clearance to access the documents.
A couple of weeks later Anne reviews the access logs to the documents, and notices that Dave (who works for Bob) has been accessing a large number of CNI documents. Anne looks into this further and

finds that Dave is widely sharing this information to others in his team, none of whom have been through the vetting and managing of privileged information training.
Option A: Report your observations to Cyril, and urge him to tell Bob formally that this is not acceptable.
Option B: Send Dave an informal email, reminding him that sharing CNI documents with non-cleared employees is not allowed.
Option C: Initiate an audit of Bob's Department to attempt to track the use and distribution of the CNI documents.
Option D: Do nothing - If something goes wrong, Bob has to deal with it as he is the Senior Manager in charge of the department that is sharing the information.

N	796	Number
1st	72.99%	581
2nd	13.44%	107
3rd	13.44%	107
4th	0.13%	1

Scenario F – Information Disposal (Attitude)

James works for a utility company as a Senior Contracts Manager and regularly reviews confidential contracts, which contain sensitive commercial information and customer data. He prefers to review documentation in paper form, so he often prints out confidential documents to read and make notes on whilst travelling on the train to/from home. When he is finished with these documents, as an environmentally conscious person, he places them in the recycling bin. At home there is no secure disposal available so he uses the standard recycling service. The risk of 'dumpster diving' (people stealing documents from rubbish bins) has been communicated in a recent Internal Awareness Campaign. It specifically recommends disposing of confidential information in the confidential bin but James feels that this is overly cautious and does not always use the Confidential but the normal recycle bin as he thinks the paper will be destroyed when it is recycled anyway, so there is no need to be concerned.
Option A: James' working practises are acceptable; recycling the paper is good for the environment and destroys any sensitive information at the same time.
Option B: James should ensure any paper copies he makes are disposed of specifically in a confidential recycle bin to ensure they are securely shredded once he has finished with them – hard copies are a major source of information leaks.
Option C: James is right to work in the way that suits him best – without access to the company systems even if someone did get hold of a few bits of information they couldn't damage the utility company anyway.
Option D: James is being totally reckless with customer's information – the major threat caused by hard copies is to the customers via identity theft and he should stop printing out work unless it is absolutely necessary.

N	133	Number
1st	0.00%	0
2nd	71.43%	95
3rd	0.00%	0
4th	28.57%	38

Scenario G – Backing Up Information (Behaviour)

Emilia works for a utility company as a Finance Analyst and is a very conscientious individual who occasionally works from home in the evening to catch up on things she could not complete during the day.
Emilia normally uses the train to get home. She chooses to leave her laptop as she has recently had her laptop stolen when travelling home from work.
Emilia keeps a backup of all her work files on her personal computer so she can access files without having to connect to the utility company system as her home network connection is not always reliable. She knows this is against company policy, but she lives in a safe neighbourhood and does not consider this to be a great security risk. In order to transfer files to her home computer she uses a variety of methods.
Option A: Use one of your USB sticks to carry your current work with you on the train.

Option B: Email the files to your personal email account from your work account and download them at home.
Option C: Use an online storage service such as Drop box as an interim transfer location, deleting the files once you have made a local copy.
Option D: Log in to the company VPN and make local copies via that connection.

N	278	Number
1st	21.58%	60
2nd	5.40%	15
3rd	3.96%	11
4th	69.06%	192

Scenario H – External Threats (Attitude)

Andrew works at a utility company site, and he walks there each morning from the local station. One morning he notices a blue van parked outside the entrance gates. He thinks he has seen the van parked in the same spot several times before over the last couple of weeks. Andrew becomes suspicious so he notes down the van details so he can check again if it is the same van. A few days later, Andrew notices the same van parked in the same location. As he passes the van he observes two individuals, one of whom appears to be taking pictures of the building/people around the building. As soon as the individuals see Andrew, the van pulls away in a hurry.
Option A: Put it out of your mind; you have seen the van several times and nothing has happened at the site so it probably isn't a threat.
Option B: Report the incident to your line manager; it is better to report such incidents even if nothing has happened.
Option C: Report your suspicions directly to security so they can take the appropriate action.
Option D: Do nothing now but keep an eye out for the van in the future to confirm his suspicions. If it shows up again then report the incident.

N	347	Number
1st	0.29%	1
2nd	15.27%	53
3rd	84.15%	292
4th	0.29%	1

Scenario I – Information Requests (Behaviour)

Mohammed is a Contract Support Assistant at a utility company who manages 3rd-party contracts. One afternoon, he receives a phone call from Alison who used to work with him at the utility company but now works for one of the utility company's trusted 3rd-party companies. She asks Mohammed for some commercially sensitive information that is not publicly available through the company's web site.
While the company she works for is allowed access to the information, Mohammed is aware that there is a procedure 3rd-parties need to go through to obtain that information. Mohammed politely refuses the request and reminds Alison of the procedure she should follow. Alison now becomes very persistent and reminds Mohammed that they used to be colleagues as well as mentioning the names of several senior people in both companies, saying they will be extremely unhappy if she does not get this information that day. She further says she is still in contact with his line manager and will explain everything to him later, so Mohammed should be ok with providing this information today.
Option A: Accede to the request for information to ensure that the senior personnel are satisfied and Alison's productivity isn't hampered.
Option B: Send Alison the information she requested but immediately inform your line manager of the call and that information has been provided.
Option C: Ask Alison specifically which pieces of information she needs and send through a redacted or edited version of the documents.
Option D: Send the information through but password protect the file and wait until you have spoken to your line manager before releasing the password to Alison.

N	359	Number
1st	7.80%	28
2nd	5.01%	18
3rd	8.08%	29

4th	79.11%	284

Scenario J – Working Practises (Attitude)

Sanjeeta has worked with Kevin at a utility company for a number of years. Kevin has always been an effective member of the team, but is known for 'having his own way of getting things done'. A few months ago Kevin left the utility company to work for one of the utility company's Service Partners. They still maintain a close working relationship and are located at the same site. Recently Sanjeeta noticed that several confidential documents/records were missing and there was no audit trail of who had used them last.

Sanjeeta then recalls that Kevin had accessed the documents to resolve a query associated with a project he had recently been working on, so she decides to ask Kevin about the missing documents next time she saw him.

When asked about the missing documents, Kevin becomes very defensive and objects to being challenged, telling Sanjeeta that she should "stick to her own work and stay out of mine". Sanjeeta was very taken aback by this response.

Option A: Do nothing, Kevin's working practises have always been eccentric and this seems to be no more than a product of his usual attitude.

Option B: Discuss Kevin's behaviour with the department manager – it isn't acceptable for an individual in the department to have their own methods that conflict with the company best practice and policy.

Option C: Accommodate Kevin's work practises by adjusting your own, it will be easier and more productive for you both.

Option D: Call the Business Conduct helpline and make a report about Kevin's behaviour – it is suspicious that there appears to be no proper audit of his work.

N	877	Number
1st	0.91%	8
2nd	66.25%	581
3rd	0.91%	8
4th	31.93%	280

Company B

Scenario A (Attitude) – ID Badges

Jemima is a member of the Operations team working at the company headquarters. While sat working at her desk she notices someone she doesn't recognise walk past without a visible ID badge. This prompts her to do one of the following:
A) Nothing, the security badges are only used for accessing the building and once you are in serve no other real purpose.
B) Make sure that her own ID badge is visible, seeing someone without theirs reminds her that she should have hers on display.
C) Go and talk to the person and ask if they have a badge. If they have remind them to have it on display, if not then politely escort them to security.
D) Nothing, although security badges are meant to be visible at all times it is a formality and it is the job of the security guards to check not hers.

N	152	Number
1st	6.58%	10
2nd	18.42%	28
3rd	55.26%	84
4th	19.74%	30

Scenario B (Attitude) – Clear Desk Policy

When leaving his desk to go for lunch with some colleagues Darren, a member of the HR team, notices that one of them has left his screen unlocked. The rest of the people he is with don't seem to have noticed, or seem to be OK with leaving it as it is. Darren got into the habit of locking his screen some years ago while working in a different company. As his colleagues start to walk away he decides to:
A) Do nothing, the screen will automatically lock after a few minutes and this will keep things secure.
B) Do nothing, there is no risk here as no-one could get into the office without passing through security . The screen locks are there just as a formality.
C) Lock the screen himself.
D) Quickly find out who's desk it is from the group and ask them to lock it before they leave for lunch.

N	456	Number
1st	10.75%	49
2nd	1.32%	6
3rd	33.99%	155
4th	53.95%	246

Scenario C (Behaviour) – PasswordManager

Hina, a member of the Operations division, has recently been required as part of her job to use a new piece of software about once a week. This requires her to log in to the service using a new username and password combination. Unfortunately PasswordManager does not work correctly with this new software and fails to store or enter her password. Because of the lack of PasswordManager support Hina is worried about being able to use the service as she struggles to remember infrequently used passwords.
Assuming that Hina decides to continue using the service without the support of PasswordManager, if you were Hina, what would you do in these circumstances?
A) Store the password using a method of your own devising – you can be trusted to keep it safe.
B) Share your password with a trusted member of your working group so that if you forget it they can remind you.
C) Stop trying to remember the password and just use the password reset feature to generate a new password each time you need to use the service.
D) Re-use a password from another service that you have committed to memory.

N	152	Number
1st	43.42%	66
2nd	1.32%	2
3rd	19.74%	30
4th	35.53%	54

Scenario D (Behaviour) – VPN

Robert, an analyst in the Operations team, has a set of logs from secure company hardware that he needs to upload to the manufacturer's website for analysis. He is working from home and unfortunately while connected to the VPN he is unable to utilise the upload function on the manufacturer's site. It is necessary that the logs are analysed each day so he cannot wait until he is next in the office if he is to successfully complete this task.
Assuming that Robert decides to upload the logs via a different method, if you were Robert, what would you do under these circumstances?
A) Make a local copy of the logs, disconnect from the VPN and upload the logs over your home connection.
B) Email the logs to a colleague not working from home and see if they can upload the logs via a direct LAN connection.
C) Give the password to the server to a trusted colleague not working from home and ask them to download the logs from the server before uploading to them to the manufacturer.
D) Email the logs directly to the manufacturer's customer support email, and ask them to conduct the analysis and send the file back.

N	152	Number
1st	13.16%	20
2nd	61.84%	94
3rd	16.45%	25
4th	8.55%	13

Scenario E (Attitude) – Tailgating

Jessica is heading toward an access controlled entry door and notices a man she does not recognise gain entry by following close behind someone else who had tagged in at the door. The two men are walking close together although they do not appear to obviously be in conversation. The second man is holding a cup of coffee in one hand and his laptop in the other. His ID badge is not immediately visible. Jessica decides to:
A) Follow the man and ask to see his ID badge.
B) Find a security guard at one of the manned turnstiles and tell them what happened.
C) Return to her desk, she sees this sort of thing quite regularly and it is probably because his hands were full that he did not swipe through himself.
D) Do nothing, if he is up to some mischief the security guards will catch him later on.

N	164	Number
1st	21.95%	36
2nd	64.63%	106
3rd	11.59%	19
4th	1.83%	3

Scenario F (Behaviour) – File Storage

Concerned about the safety of his current work Shamal decides to back up his data, some of which is confidential. As he uses his own laptop under the 'bring your own device' scheme he usually stores all his work on his drive on the central server but he wants to have a second copy just in case something happens or he loses connectivity to the company network. He thought about using one of the common drives but none of the ones he regularly uses have sufficient space.
A) Create a local copy on the hard drive of your BYOD laptop, it is the only machine you work on so you know it will be safe and this ensures you will always have access to it if needed.

B) Use a common drive that you used for an old project and still have access to, as your credentials were never revoked. It has enough space although you do not know who manages it now.
C) Use an online service, such as Dropbox, to store the data as it is more under your control.
D) Back your work up onto a USB stick – you have ordered an encrypted one but while you wait for it to arrive you use a personal stick you have to hand.

N	164	Number
1st	39.02%	64
2nd	21.34%	35
3rd	21.95%	36
4th	17.68%	29

Scenario G (Attitude) – Secure Disposal

John works as a Sales Advisor in a store in London. During a busy period of the day he notices that a customer, served by one of his colleagues, has left their paperwork behind. John's colleague grabs the paperwork and throws it into a wastepaper bin under the desk. Seeing this John decides to: 27
A) Carry on serving customers in the store, all the rubbish will be thrown out at the end of the day anyway so it is no big deal, and using the shredder in the back area, locked by a keypad, is inconvenient when the bin is right there.
B) Make a note to check with his manager what the appropriate action would be, as it has been some time since he took the Data Protection CBT module and he cannot clearly remember the details.
C) Go and grab the paperwork out of the bin when he has a spare moment and take it to the shredder in the back of the store.
D) Go over immediately and ask his colleague to take the paperwork out of the bin and put it in the shredder, having documents lying around exposes both the store and the customer to the risk of identity theft.

N	292	Number
1st	0.34%	1
2nd	2.40%	7
3rd	6.16%	18
4th	91.10%	266

Scenario H (Behaviour) – Credit Check

Karina works as a Sales Assistant in a store. Her manager has asked her to increase her sales in order to meet the store's monthly target. In her experience customers can be put off by the need for credit and ID checks, and sometimes fail them altogether. She knows of a few unofficial ways of making the checks seem less of a problem, or to increase the chance of customers passing them.
A) Give the benefit of the doubt when encountering IDs with indicators of possible fraud, such as dates of birth that do not seem to align with the apparent age of the customer, or addresses in different cities.
B) Use your employee discount to offer the customer a more attractive deal.
C) Attempt multiple credit checks in quick succession in order to try to figure out which details are causing the problem and amend them.
D) Give information about the credit check to a few of your personal contacts so that they can prime potential customers on what they need to do to beat the system before referring them to the store.

N	292	Number
1st	20.21%	59
2nd	63.36%	185
3rd	9.59%	28
4th	6.85%	20

Appendix K: Company B communication plan improvements

Old communications plan

This existed when the researcher joined the organisation

Introduction

Security awareness is an essential part of our security management activities to protect the company from security incidents. We need to demonstrate an effective awareness programme is in place during audits to achieve and retain our security certifications including:

5. TISAC - 10 Steps to Cyber Security
6. PSN – Public Services Network
7. ISO27001 – Information Security Management
8. ND1643 – Ofcom Minimum Security Standards
9. ISO22301 – Business Continuity Management
10. PCI DSS – Payment Card Industry Data Security Standard

This Communications Plan details the programme of security awareness activities for 2014. It's aim is to enhance and promote security throughout the company as a 'business as usual' issue by raising awareness of current threats, promoting good practice and demonstrating security awareness of Company people.

Communication topic	Why (supports)
Current threats or major issues that have been in the press / emergency issues	Raise awareness of current threats.
Data theft	Illustrate the key stats regarding awareness of mobile device security and theft
Geek Tweet	To raise awareness and promote the fact that this is an up-to-date place to find security information
Security CBT	Re-launch revised security CBT
Privacy Markings	Guide people towards the security policies and making them aware of them.
Keeping data safe	Guide people towards the security policies and making them aware of them.
Glasgow 2014	Raise awareness and Glasgow games will impact the high street shops
Social Engineering	Make people aware of the types of social engineering and the need to validate any requests for access to buildings, customer data or company information.
SMIP	SMIP testing begins in June. Provide some awareness about the programme, and security changes that are being implemented and the on-going support from the business.
Data Protection and ICO on EU data	Data raise the profile of information security and impact of legislation protection (EU data)
Reporting IT Security Incidents	Launch new reporting process, (Dependant on SIEM area) reporting IT Security Incidents
PCI-DSS	Worked hard to get PCI, must maintain it.
Password Security	Some of these can be done together and are really guiding people towards the policies and making them aware of security policies
Virus and Malware	Some of these can be done together and are really guiding people towards the policies and making them aware of security policies
Acceptable use on Computers	Some of these can be done together and are really guiding people towards the policies and making them aware of security policies
BYOD	The policy needs to be revisited and HR Engaged before any launch.
Re-launch of Potential Security Issue form	Launch new reporting process, (Dependant on SIEM area)
How our certifications deliver benefit to the business	In support of ISO27001 and other certifications.
Wear it, Mark it, Clear it	In support of PSN. (repeat existing campaign)

New communications plan

Improvements required

1. All points relate to the importance of information in the company – could launch those separately as part of an overarching “Protect our information” campaign
2. Raise the profile of information security and impact of legislation protection (UK and EU)
3. Guide people towards the security policies and making them aware of them.
4. Make people aware of the types of social engineering and the need to validate any requests for access to buildings, customer data or company information

Actions taken

1. Added SOX (Sarbanes-Oxley) compliance requirements
2. Defined an overall theme (“Protecting our information”) and related communication to that
3. Need to identify the rationale behind each section – avoid risk of overloading
    a. What the current state is? What are the behaviours to be changed?
    b. How do we know? (metrics – data?)
    c. What are the current implementation constraints?
    d. Short term goals?
    e. What do we want to tell people about it?
    f. Long term goals - future improvements?
    g. …everything needs to align with security implementation change planning
4. Define audit-related deliverables
    a. Communication records
    b. Metrics showing improvements

Communications topic	Why (supports), current state	Ideal state	Implementation Constraints	What to measure	Short term goal	Long Term goal
Privacy Markings	Helps protecting information handling / sharing Avoids putting organisation / individuals at risk Employees aware what they are – not know how to use them Leads to overclassification	All information held or processed has its value assessed by its author or nominated business owner and corresponding privacy marking assigned. Individuals know how to mark and how to deal with sensitive documents when they see them	Not all people use all levels – target awareness based on this	Markings on documents left around found on site security clear desk checks	Improve understanding on how to classify documents, mark them and handle them	Same
Social Engineering	Prevent unauthorised information disclosure Information is a key asset and it is important that everyone considers all the impacts of disseminating information.	Employees can recognise a social engineering attack Employees refuse to share information before full verification of other party	Current implementation leads to password and information sharing through other channels	Abnormal access patterns	Reduce exposure to engineering attacks	Same
Data Protection	Employees sometimes downplay importance of information they handle Awareness is role specific Data sharing ad-hoc – using external services, emails Clear desk not always followed	Employees understand the importance of information they handle Centralised corporate file sharing and storage with adequate capacity, no cloud services used Audits – if all other areas covered there should be no problems with this	Shared drives highly visible to a lot of people No formal mechanism for file sharing exists DLP system needs to be deployed	Documents left around, number of support requests for file sharing mechanisms, DLP metrics on email sharing, volume of traffic to cloud providers, Utilisation of internal systems	Improved awareness on information sensitivity, utilisation of corporate systems for file sharing and storage Less documents left around	Fully integrated in employee day-to-day information sharing
Acceptable use on Computers	Secure backup / data transfer important for information confidentiality and availability No centralised backup / data transfer strategy USB drives need to be secure	Regular backups performed. Interval between backups should be linked to sensitivity, impact of loss, corruption or non-availability of the data. Any PC used by the company will enforce mandatory encryption of USB devices	Backed up network storage of limited capacity Encrypted USB system needs to be deployed	Behaviours before and after piloting deployment Data from reporting systems Screen lock	Secure backup / sharing of information Everyone has encrypted USBs	Ensure all organisational provisions support desired behaviours

Communications topic	Why (supports), current state	Ideal state	Implementation Constraints	What to measure	Short term goal	Long Term goal
Password Security	Sharing of passwords occurs in some rare situations Writing down passwords is prevalent	Passwords must only ever to be written down for emergency record purposes and then stored under protected conditions (i.e. in approved locked metal furniture); Employees should download and use password manager	Password manager problems and compatibility issues, expiry makes passwords difficult to remember	Password manager adoption Prolonged account inactivity Password reset requests Abnormal access patterns	No password sharing No writing down Password manager works flawlessly	Same
Access Control	Guide people towards the security policies and making them aware of them. Access revoking slow – line managers not taking action, accounts marked as inactive, taken down by access control teams	Access revoking for leavers done automatically through HR. Line Managers ensure security implications of leavers are addressed	None	Prolonged account inactivity Also list of line manager requests to remove someone from the system Time from dismissal to access removal	Procedures to restrict building, system and application access immediately for people who are dismissed or who abandon service.	Same
Virus and Malware	Danger to the organisation Lack of formally communicated USB policy creates risks	All systems and devices on the corporate network should be protected against viruses using approved antivirus software	None	Infected machines detected on the network	Identification of infections and appropriate actions taken	Same
Reporting IT security incidents	Current behaviours widely varying: from reporting everything to nothing Reporting concerns/problems allows: Early identification of potential compromises Potential areas for implementation improvements	All problems are reported Followed up by security management Impact of reporting communicated back to employees	None	Helpdesk reporting rates Time to respond Number of resolved problems	Employees are willing to report security concerns and seek support when in doubt	Implementation of mechanisms that allow report-driven improvements

Appendix L: General suggestions for improvements presented to Company B

Topic 1: Employee Awareness and Security Communication

Area	Current state	Changes required	Who needs to act	Delivery Constraints	Metrics Required
Simplify communication	Employees are aware on importance of information they handle, potential breaches, impact to the organisations and the need for security, policy existence, BUT sometimes downplay importance of information they handle Communication on security incident driven, irrelevant, generic, inconsistent and overloaded Communication done at team meetings and security support by line managers Do not expect their team to know full policy	Simplify communication, role-based through managers Managers should be informed about security risks, assess those and decide what applies to their teams Reduce employee need to filter though policy content	Security management Line managers	Requires additional communication to be included in line manager brief and team meetings Requires additional effort to plan and deliver	Use function of metrics presented in the remainder of this table as an awareness and security behaviour indicator Clear desk logs on document marking
Make CBTs role-specific, spread throughout the year	Too many CBTs that need to be taken at the same time CBT content perceived as common sense	Spread CBTs throughout the year Change nature of communicated information Introduce quiz both to engage with employees and measure employee security knowledge	Security communications delivery	CBT completion time depends on employees Development of quizzes and training material can take time Requires alignment with corporate communication strategy	Questionnaires included in line manager communication Employee questionnaires All metrics outlined in this table should improve with this

Topic 2: Information Handling

Area	Current state	Changes required	Who needs to act	Delivery Constraints	Metrics Required
Deploy centralised corporate file sharing with automatic backups	Data sharing ad-hoc though multiple formal/informal channels (emails, shared drives, SharePoint, USB sticks, third party cloud storage for collaboration) No centralised backup strategy, Ad-hoc backups, "unintentional backups" on local laptop systems (emails) Network drive space small, some unaware of its existence, store past and currently-working documents on laptop Confidential information taken home on paper or on devices where visitors/family members have access	Deploy centralised corporate file sharing with automatic backups (inform employees about this) Deployment of DLP system (control and monitor sharing practices) Communicate need to be careful with devices that hold company information	IT Security Security management Line managers	Cost of storage problem for network drive increase	Check volume of cloud storage use. Utilisation of internal file-sharing systems DLP metrics to identify changes in information sharing practices
Mandatory USB encryption	Capacity of encrypted USBs not sufficient, also often problematic when plugged in to other machines Employees need to find alternative ways to communicate information – use unencrypted drives	Mandatory encryption of USB storage OR Provide sufficient capacity encrypted USBs to everyone	IT Security Security management	Encrypted US software deployment, Cost of giving out USBs	USB metrics to assess use of unencrypted drives
Provide secure physical document storage	Everyone appears to understand the need for it BUT confidential information is left around People who have lockers appear more prone to comply	Secure lockers exist for employees, Nothing is left overnight on the desks	Property Security management	Provision for lockers can create cost and space issues	Numbers of documents left around (through clear desk checks)
Improve leaver process	Access revoking slow, line managers not taking action, accounts marked as inactive and taken down by access control teams	Line Managers ensure leavers form are immediately handed in Leaver access revoking done through HR	Security management HR Line managers	Need capability to re-activate old accounts for contractors that may go and return	Unused accounts should decrease after intervention, time for leaver account deactivation

Topic 3: Employee feedback and passwords

Area	Current state	Changes required	Who needs to act	Delivery Constraints	Metrics Required
Encourage reporting	Employees differ in willingness to report vulnerabilities, problems etc, often mentioning others would take care of it. Two reporting sources: Direct contact with security, through their line managers	Employees should report security concerns and seek support when in doubt – include this in communication Followed up by security managers and appropriate actions taken	Security management	Resources required to address reported issues and communicate impact back to employees	Calls for support Number of reported problems followed up Time taken to respond
Provide password management support	Sharing of passwords occurs in some rare situations Writing down passwords is prevalent	Fix password manager to work with all organisational systems	IT Service provider Security management	Additional effort required to introduce a working password manager	Password manager adoption Abnormal and inconsistent login attempts