Northumbria Research Link

www.northumbria.ac.uk/nrl

northumbria
UNIVERSITY NEWCASTLE

Information Security in the Workplace: A Mixed-Methods Approach to Understanding and Improving Security Behaviours

JOHN MATTHEW BLYTHE

PhD

2015

Information Security in the Workplace: A Mixed-Methods Approach to Understanding and Improving Security Behaviours

JOHN MATTHEW BLYTHE

A thesis submitted in partial fulfilment of the requirements of the University of Northumbria at Newcastle for the degree of Doctor of Philosophy

Research undertaken in the Faculty of Health and Life Sciences

December 2015

ABSTRACT

Traditionally, employees have been viewed as an enemy to information security (IS) within organisations, rather than as an organisational asset that can be harnessed to help protect company information. Existing research is largely fragmented with a distinct lack of theory-based approaches for the design and evaluation of behaviour change interventions. Furthermore, research has largely focussed on employees' compliance with IS policies and less so, the multitude of individual behaviours covered in them. This thesis presents a mixed-method approach to changing employees' security behaviour using theory to inform the design of an intervention.

The thesis identified influencers and barriers to specific security behaviours and developed an extended-Protection Motivation Theory model. The model includes information sensitivity appraisal as an important influencer for which a new scale (WISA) was developed and validated. The model was tested on three specific anti-malware behaviours: usage of anti-malware software, installing software updates and avoiding suspicious links within emails. The testing allowed the identification of the most influential factors for each behaviour and demonstrated how these factors differ between behaviours. A nuance that is lost when adopting the IS policy compliance approach and was also confirmed by the qualitative findings. The findings from the models informed the design of the behaviour change intervention.

Components of the model were utilised in an intervention to promote email security behaviour. The intervention comprised of a motivational component, together with a volitional component based on implementation intentions to help translate good "intentions" into good "security actions". The study found significant improvements in objective performance on email legitimacy tasks that were more sustainable with the addition of implementation intentions. Response efficacy was an identified barrier, demonstrated to influence anti-malware behaviours and was malleable to significant change during the intervention.

The theoretical and practical implications of these results are discussed together with suggestions for future research.

TABLE OF CONTENTS

LIST OF TABLES

XIII

LIST OF ABBREVIATIONS

AGFI.	Adjusted Goodness-of-fit Index
AMS.	Anti-Malware Software
BYOD.	Bring Your Own Device
CFA.	Confirmatory Factor Analysis
CFI.	Comparative Fit Index
DPA.	Data Protection Act (1998)
EFA.	Exploratory Factor Analysis
EM.	Expectation–Maximization
ES.	Email Security
HBM.	Health Belief Model
GFI.	Goodness-of-fit Index
GDT.	General Deterrence Theory
ICO.	Information Commissioner's Office
ISO.	International Organization for Standardization
IS.	Information Security
OCB.	Organisational Citizenship Behaviour
PBC.	Perceived Behavioural Control
PEOU.	Perceived Ease of Use
PMT.	Protection Motivation Theory
PU.	Perceived Usefulness
RC.	Response Costs
RCT.	Randomized Control Trial
RE.	Response Efficacy
RMSEA.	Root Mean Square Error of Approximation
SCT.	Social Cognitive Theory
SE.	Self-efficacy
SEM.	Structural Equation Modelling
SU.	Software Update
TAM.	Technology Acceptance Model

TPB.	Theory of Planned Behaviour
TRA.	Theory of Reasoned Action
WISA.	Workplace Information Sensitivity Appraisal

ACKNOWLEDGEMENTS

DECLARATION

I declare that the work contained in this thesis has not been submitted for any other award and that it is all my own work. I also confirm that this work fully acknowledges opinions, ideas and contributions from the work of others.

Any ethical clearance for the research presented in this thesis has been approved. Approval has been sought and granted by the Faculty of Health and Life Sciences ethics committee at the University of Northumbria in Newcastle.

I declare that the Word Count of this Thesis is 80, 746.

Name: John Matthew Blythe

Signature:

Date:

PUBLISHED WORK

Work from this thesis has contributed to the following publications:

Blythe, J.M., & Coventry, L. (2012). Cyber Security Games: A New Line of Risk. In Entertainment Computing-ICEC 2012 (pp. 600–603). Springer Berlin Heidelberg.

Blythe, J.M. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In Proceedings of CHItaly 2013 Doctoral Consortium (pp. 92–101).

Blythe, J.M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 103–122). USENIX Association.

Coventry, L., Briggs, P., Blythe, J.M., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Summary report for the Government office for science. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

CHAPTER 1: INTRODUCTION

Organisations are under constant attack from internal and external threats that put the integrity, availability and confidentiality of their information at risk. Reports indicate that 90% of large organisations and 74% of small businesses experienced a security breach in the last year (PwC, 2015). The implications of security breaches are wide-ranging from service disruption to reputational damage alongside potentially high financial costs incurred from the data breach. Figures indicate that the cost of a worst case security breach is between £1.46m-£3.14m for a large organisation and £75-£311k for a small organisation (PwC, 2015). Effective defence of organisations' information and systems is of upmost importance if it is to optimally function as a 21st century organisation.

Organisations adopt technical, procedural and human defences to protect against security threats. The technical countermeasures include firewalls and intrusion-detection systems. However, information security cannot be achieved solely through technological solutions (Herath & Rao, 2009b; Schneier, 2000; Vance, Siponen, & Pahnila, 2012). Organisations adopting a combination of technical, procedural and employee behaviour to protect their information systems assets and resources are considered to be more effective (D'Arcy & Hovav, 2007; Li, Zhang, & Sarathy, 2010; Schneier, 2000; Stanton, Stam, Mastrangelo, & Jolton, 2005; Vance et al., 2012).

Traditionally, employees have long been considered to be a weak link in the security chain (Dhillon & Moores, 2001; Mitnick, 2003; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Vroom & von Solms, 2004) as their behaviour is estimated to account for a large portion of security breaches. PwC (2015) found that 75% of large organisations and 31% of small businesses experienced a security breach that was staff-related and that 50% of the worst breaches were due to human error. Figures from the Ponemon Institute (2015) indicate that 25% of data breaches were due to employee (such as human error) behaviours, 29% were due to system glitches and the remaining 46% were due to malicious attacks (including organisational insiders).

There is a need to understand the role of employees as an organisational asset and as a key contributor to the defence of organisational information security. As such, research has moved towards understanding what motivates employees' protective security behaviour (e.g. Herath & Rao, 2009a, 2009b; Ifinedo, 2011, 2014; Vance et al., 2012), and the role unusable systems,

policies and procedures play in insecure practice (e.g. Albrechtsen, 2007; Bartsch & Sasse, 2012; Beautement, Sasse, & Wonham, 2009; Inglesant & Sasse, 2010).

Although employees have been identified as one of the most significant vulnerabilities in the information security of organisations, research to date is fragmented and little attention has been given to designing theoretically-based and empirically-validated behavioural interventions to improve their behaviour.

This chapter will outline what is meant by information security and how the thesis approaches understanding more about the role of employees within the context of information security.

1.1 | INFORMATION SECURITY AND CYBER SECURITY

Information security and cyber security are not easy terms to define. This is further complicated by their interchangeable use within research and the media. von Solms & van Niekerk (2013) argue that that while there is significant overlap in these concepts, they are not the same thing.

Information security, as defined by the ISO (2005), is viewed as the maintenance of the confidentiality, integrity, and availability of information and is known as the "CIA triad" of information security. The aspects of the CIA triad are explained as follows:

- Confidentiality – ensuring that data is kept private and its access is restricted. Not all information is of equal sensitivity and information considered sensitive needs a higher level of confidentiality.
- Integrity – ensuring that data is consistent, unaltered, accurate and trustworthy over its life span and accessed only by authorised personnel.
- Availability - data access is available when required and the computer systems that store and process the data must function as needed.

von Solms & van Niekerk (2013) argue that what distinguishes cyber security from information security is that the former places greater emphasis on the human element as an asset to be protected and a cause of vulnerabilities They argue that these assets can be both tangible (e.g. infrastructure) and intangible (e.g. an individual's wellbeing). They posit that information security is the protection of information and the technologies that store it, whereas cyber security is the protection of those that function within cyberspace, including people and organisations. They conclude with the following definition of Cyber Security:

> "The protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" [pg. 101]

The greater emphasis on the human element in cyber security definitions also corresponds with the increased focus on the human element as a source of security concern. Historically, computer security was concerned with the protection of information through technological means. However, in the last 10-15 years, attention has been given to the socio-technical side of cyber security exploring the interplay between end-users and security.

1.2 | CYBER SECURITY IN THE UK AND THE WORKPLACE

In 2010, the UK government placed cyber security as a Tier 1 priority, and on developing the UK's Cyber Security Strategy, outlined a four-year plan to help protect businesses and individuals from the many threats in cyber space (Cabinet Office, 2011). The increased focus and attention on the need for a more secure UK cyberspace is promising. An important aspect of the strategy is to ensure the public have the basic skills and knowledge to protect themselves from cyber security threats and that businesses are more cyber security focussed in their operation.

Although the focus and priority of cyber security has increased in the last few years, historically, numerous laws have been put in place that govern individuals and organisations in their use of data and computers. The Data Protection Act (DPA; 1998) is of upmost interest to this thesis as it covers the information security of personal data stored by organisations. To ensure compliance with the Act, organisations that store and process personal information must conform to the eight principles outlined within the DPA. Breaches of the DPA can have severe repercussions for organisations, who can be fined up to £500,000 by the Information Commissioners Office, the governing body of the DPA.

1.3 | INFORMATION SECURITY POLICY

Within organisations, the information security (IS) policy is an internal document that outlines how the organisation plans to ensure the availability, integrity and confidentiality of its information. The document specifies roles and responsibilities of its employees and the organisational procedures to ensure information security. Whitman (2004) highlights the aspects of a good information security policy:

> '[It should] outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for updating the p*olicy'* [pg. 52]

There are a number of standards and guidelines for information security management with the International Organisation for Standardization (ISO/IEC 27002:2013) standard being the most widely recognised and is increasingly used for defining information security practice in the

workplace. The standard provides best practice recommendations for information security management and guidelines in the following areas:

Table 1. ISO 27002: 2013 standard

ISO 27002:2013 standard
Information security policies
Organisation of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communications security
System acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance

This standard demonstrates the number of areas organisations must comply with should they wish to be certified by the ISO. The fourteen areas demonstrate the potentially vast amount of security behaviours that employees may be expected to perform.

However, organisations differ in the content of their policies as there is no "one size fits all" approach and a risk assessment should be used to decide which level of security is needed for their organisation (ICO, 2014). The expected security-related behaviours to be performed by employees will, therefore, differ between organisations as will the required level of information security. However, research has started to investigate some security behaviours required by employees and home users.

1.4 | SECURITY BEHAVIOURS

Security behaviours involve protective behaviours and the use of security technology. There is a lack of consensus on recommended security practices for home users and in the workplace. However, consideration of recent reports provides an indication of consistently recommended actions within government reports, research studies and survey instruments:

- **Account security/authentication** (e.g. use of strong passwords, password management, password change frequency) (Coventry, Briggs, Blythe, & Tran, 2014; Crossler & Bélanger, 2014; Cyberstreetwise, 2015; Furnell & Moore, 2014; Ion, Reeder, & Consolvo, 2015)

- **Use of security software (e.g. anti-virus, firewalls)** (Coventry et al., 2014; Crossler & Bélanger, 2014; Cyberstreetwise, 2015; Furnell & Moore, 2014; Ion et al., 2015)

- **Running the latest version of software/operating systems** (Coventry et al., 2014; Crossler & Bélanger, 2014; Cyberstreetwise, 2015; Furnell & Moore, 2014; Ion et al., 2015)

- **Anti-phishing/Scam prevention** (e.g. staying informed about risks, identifying phishing emails) (Coventry et al., 2014; Crossler & Bélanger, 2014; Furnell & Moore, 2014; Ion et al., 2015)

- **Privacy protection** (e.g. cookies, control of personal information) (Coventry et al., 2014; Crossler & Bélanger, 2014; Furnell & Moore, 2014; Ion et al., 2015)

- **Browser protection** (e.g. check HTTPs, secure websites, logging out of websites) (Coventry et al., 2014; Crossler & Bélanger, 2014; Furnell & Moore, 2014; Ion et al., 2015)

There are numerous safeguards individuals can put in place to protect themselves, however, these reports provide some basic hygiene behaviours that are useful for security protection. Behaviour in the workplace is much more complex as there are multiple assets, devices, locations, and threats that make information security behaviours more difficult to manage. Furthermore, some of those behaviours outlined above that are important for consumers may be automated by IT so may not require employee intervention.

Security behaviour in the workplace is largely conceptualised as a IS policy compliance behaviour, with less known about the behaviours that lead to compliance. IS policies differ depending on the organisation's security maturity and their protection needs. Despite these differences and lack of knowledge on specific behaviours, attention has been drawn to types of security behaviour in the workplace.

1.5 | TYPES OF EMPLOYEE SECURITY BEHAVIOUR

Stanton et al. (2005) explored end user security behaviour through 110 interviews with IT professionals, managers and employees. The interviews led to the development of a two-factor taxonomy of security behaviour varying across two dimensions (intentionality and technical expertise) resulting in six categories of user behaviour.
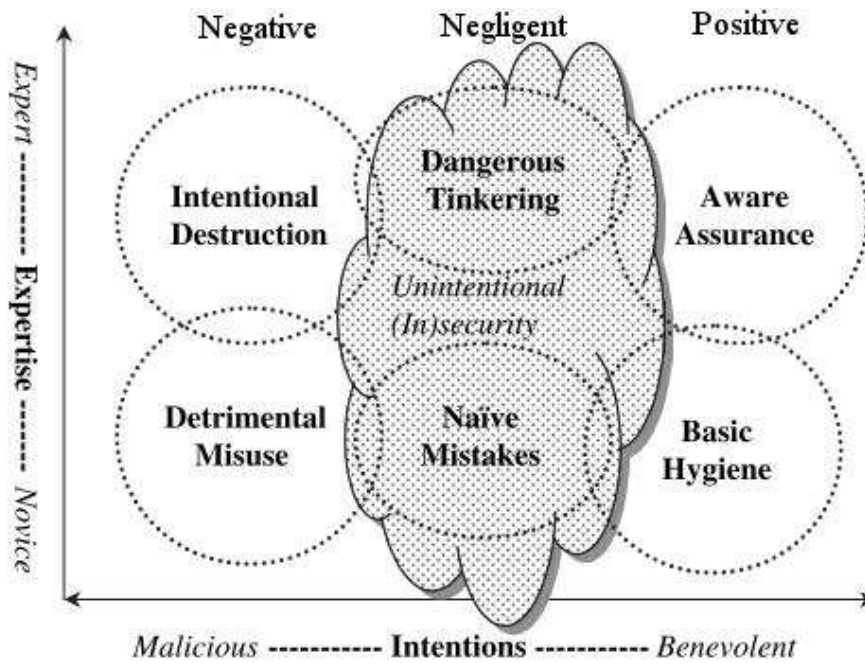
Figure 1. Two-factor taxonomy from Stanton et al. (2005)

- **Basic Hygiene**: behaviours that that require little to no technical expertise but have clear intention to protect information assets and systems (e.g. locking work computer when leaving station)

- **Aware Assurance:** behaviours that require more technical expertise (e.g. recognising a backdoor program on a work PC)

- **Naïve mistakes:** when there is no clear intention to do harm but the behaviours require minimal expertise (e.g. using a weak password)

- **Dangerous tinkering:** when there is no clear intention to do harm but the behaviours require expertise (e.g. setting up a gateway that inadvertently allows outsider access)

- **Detrimental misuse**: clear intention to do harm but behaviours require minimal expertise (e.g. using the work email to distribute spam)

- **Intentional destruction**: clear intention to do harm but behaviours require technical expertise

The work of Stanton et al. (2005) shows that there are different forms of employee behaviour with associated security outcomes. These can be divided into three forms of behaviour; positive protection-motivated behaviours (i.e. basic hygiene and aware assurance), negligent behaviours (i.e. naïve mistakes and dangerous tinkering) and negatively damaging behaviour (i.e. detrimental misuse and intentional destruction). The current thesis is interested in the positive and negligent behaviour of employees. Negatively damaging behaviour is often explored in relation to malicious organisational insiders and is beyond the scope of this thesis.

Positive and negligent behaviours are largely explored in relation to the IS policies of organisations. However, understanding the behaviours depicted within these policies has received less attention. Posey et al. (2010) identified protection-motivated behaviours through interviews with security professionals and employees. They argue that these are volitional behaviours that seek to protect the information security of the employee's organisation. They identified 67 behaviours that they clustered into 14 categories; these included those behaviours identified earlier on pages 4 and 5 which are important for consumers' behaviour. However, they also identified a number of behaviours that are important for organisational security such as co-worker reliance (e.g. reminds his/her co-workers of information security guidelines and protocols adopted by their organisation), immediate reporting of suspicious behaviour (e.g. immediately reports a co-worker's negligent information-security behaviour to the proper organisational authorities), and equipment location and storage (e.g. keeps the laptop or other electronic devices issued to them by their organisation with them at all times).

The review and study by Posey et al. (2010) indicated that there is a vast array of security behaviours that employees may be expected to perform. A combination of or lack of engagement in these behaviours may contribute to a successful security breach. Research, therefore, needs to address individual security behaviours in the workplace.

1.6 | RESEARCH QUESTIONS

The aim of this thesis is to develop and evaluate an intervention to improve the security behaviour of employees. Two research questions derived from existing behavioural information security research were explored using a mixed-method approach across four organisational studies:

1. What influences and prevents different security behaviours in the workplace?
2. Does a theoretically-grounded intervention using motivational and volitional approaches lead to and sustain security behaviour change?

1.7 | RESEARCH OBJECTIVES

The specific objectives of thesis were to:

- examine internal and environmental factors that motivate the different behaviours contributing to information security compliance (Study 1 & Study 3, Chapter 3 & 5);
- identify barriers to security behaviours and consider them within the organisational context (Study 1, Chapter 3);
- develop a qualitatively-driven framework to explain how factors influence information security behaviours (Study 1, Chapter 3);

- understand how employees appraise the sensitivity of work information by developing and validating a scale to measure this (Study 2, Chapter 4);
- explore an extended Protection Motivation Theory (PMT)-model (driven by the qualitative work and existing literature) to identify factors that influence three specific anti-malware behaviours (Study 3, Chapter 5);
- use the findings from the extended model to inform the motivational component of a behaviour change intervention (Study 3 & 4, Chapter 5 & 6);
- assess the feasibility of an intervention that combines motivational and volitional components to promote anti-malware behaviour (Study 3 & 4, Chapter 5 & 6).

1.8 | THESIS APPROACH TO ADDRESSING RESEARCH QUESTIONS AND OBJECTIVES
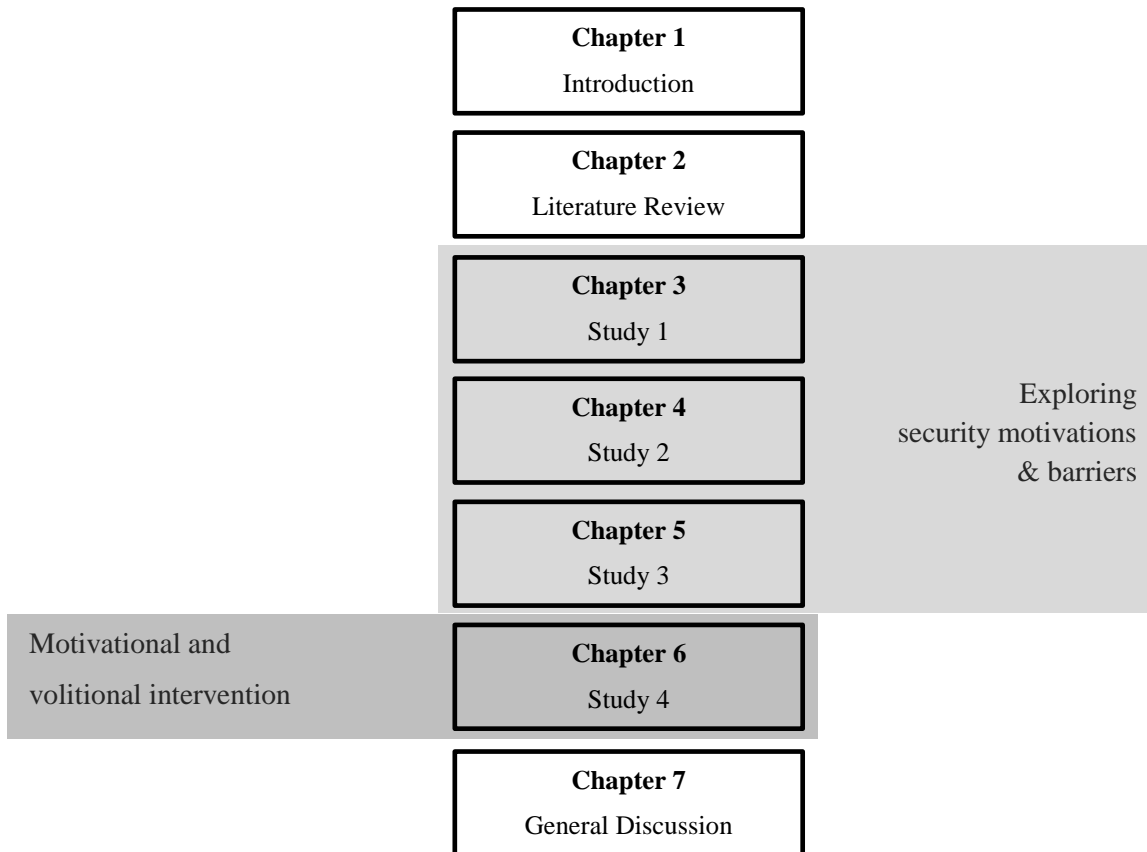
Figure 2. Thesis structure

The thesis seeks to adopt a motivational and volitional approach to understanding and changing behaviour. Studies 1 through to 3 seek to understand what motivates security behaviour in the workplace. Study 4 seeks to combine the findings from studies 1 to 3 into an intervention designed to motivate employees to engage in protective security behaviour, and the intervention is further enhanced by providing volitional strategies to help translate motivation into actual behaviours.

1.9 | OVERVIEW OF STUDIES

Overall, the thesis adopted a multi-method approach by first qualitatively exploring multiple security behaviours that contribute to IS compliance and factors that influence engagement or disengagement in these protective actions (study 1). The thesis then explored one specific factor in depth, information sensitivity, and developed a new scale to measure employees' appraisal of it (study 2). The third study explored three specific anti-malware behaviours to identify factors that explained intentions to engage in them (study 3). These findings informed the final study to design and assess an intervention that combines motivational and volitional components to promote anti-malware behaviour (study 4). The following sections of the introduction provide an overview of each study and their key findings.

1.9.1 | STUDY 1 (CHAPTER 3)

This study explored the underlying behavioural context of information security in the workplace, exploring how individual and organisational factors influence the interplay of the motivations and barriers of security behaviours. Using Protection Motivation Theory (PMT) and the Theory of Planned Behaviour, two consistently used models within behavioural information security research, the study explored factors from these models on behaviours that contribute to IS policy compliance. Alongside this, the study explored potential differences in organisational citizenship behaviours and psychological ownership between two companies. Two organisations took part, in which ten from each were interviewed and the data was analysed using framework analysis. The analysis indicated that there were seven themes pertinent to information security: Response Evaluation (response costs, perceived benefits and response efficacy), Threat Evaluation (threat models, severity, information sensitivity appraisal, and susceptibility), Knowledge (of security risks and protective actions), Experience (of security breaches and work experience), Security Responsibility, and Personal and Work Boundaries. The findings suggest that these differ by security behaviour and by the nature of the behaviour (e.g. on- and offline). Additionally, the study provided greater insight into how these factors may be conceptualised in a workplace setting and in the context of security. Levels of psychological ownership and organisational citizenship behaviour were not found to differ by organisation. Furthermore, the study indicated that PMT was an adequate theory to study security behaviour and led to the development of an extended PMT-model based on the qualitative findings and existing research to explore security behaviours in future studies of this thesis.

1.9.2 | STUDY 2 (CHAPTER 4)

The sensitivity of information is often discussed in relation to information security; however, study 1 raised the issue of a lack of a clear definition of information sensitivity. Furthermore, a lack of consensus in research has resulted in an absence of scales measuring how individuals

appraise information sensitivity so Study 2 developed and validated a new scale to measure employees' information sensitivity appraisal: the Workplace Information Sensitivity Appraisal (WISA) scale. Furthermore, the study aimed to explore sensitivity differences for company information pertaining directly to living individuals (Personal, Health, Financial & Lifestyle) compared to information that is organisationally-focused (IP, day to day, commercial & HR). The factorial, content, discriminant and criterion-related validity were assessed. The final scale comprises of five subscales: Privacy, Worth, Consequences, Low proximity interest by others, and High proximity interest by others. The WISA scale, alongside its five subscales, was found to have strong factorial validity which was confirmed across 8 target information types. The scale was found to have strong content validity and good criterion-related validity as it was found to significantly predict security behaviour. Finally, the scale was found to have adequate discriminant validity as 3 of 5 aspects of the WISA scale were found to be unrelated to organisational citizenship behaviour. Financial information was found to have the highest ratings for overall sensitivity followed by health and HR. They were also found to be the highest for 3 of the 5 sensitivity subscales, namely privacy, worth and consequences. Information about individuals (e.g. personal, health and lifestyle) was significantly considered to be of more interest to employees' high proximity interest groups (i.e. family and friends) in comparison to organisational-focussed information. For low proximity interest, the opposite effect is apparent with organisational-focussed information perceived to be of interest (e.g. IP, day to day, commercial) to low proximity groups (i.e. criminals, fellow employees & business competitors). Finally, the findings indicate that employees who work with a particular information type did not rate that information any more sensitive than employees who do not work with that information.

1.9.3 | STUDY 3 (CHAPTER 5)

Study 3 sought to understand whether security behaviours are influenced by different factors by assessing an extended-PMT model based on findings from existing research and study 1. By exploring a subset of security behaviours with employees (anti-malware behaviours), the study shed further light on the complications of adopting a policy-compliance approach in security research. Anti-malware behaviours have been relatively under-explored in existing behavioural information security research and exploring three distinct behaviours allowed comparison of their determinants.

The three anti-malware behaviours that were explored were; scanning USB sticks with anti-malware software (AMS security), installing software updates when prompted (SU security), and not clicking on suspicious links in emails (ES Security). The original PMT model was explored: threat appraisal (severity and susceptibility), and coping appraisal (response costs, self-efficacy and response efficacy). In an extension of PMT, psychological ownership, security

breach experience, organisational citizenship behaviour, responsibility and WISA were also explored in relation to the three behaviours.

Revising PMT using regression analyses allowed additional factors to be added to the model to provide greater insight into the influencers of anti-malware behaviours and identify which factors can explain most variance in the target behaviour. For AMS security, self-efficacy, response efficacy, response costs, WISA (consequences) and responsibility were found to significantly predict motivations to scan USB sticks for malware. For SU security, response efficacy, response costs, susceptibility and responsibility were found to significantly predict motivations to install software updates when prompted by devices. Finally, for ES security, self-efficacy, response costs, susceptibility and security breach experience at work were found to significantly predict motivations to not click on links within suspicious emails.

1.9.4 | STUDY 4 (CHAPTER 6)

The final study evaluated an intervention based on the findings of study 3. The intervention aimed to improve employees' email security behaviour, in particular being cautious with links within emails. The intervention was composed of motivational and volitional components. The motivational components were informed from study 3 in which self-efficacy, security breach experience at work, susceptibility, response costs and response efficacy were found to influence behaviour. The motivational component was primarily self-efficacy based, aiming to enhance employees' ability to detect phishing emails through enactive mastery, performance accomplishments and vicarious experience. Persuasive information also targeted the remaining influencial factors. The volitional component was based on implementation intentions, to bridge the gap between intentions and actual behaviour. A randomised control trial was adopted to assess the effectiveness of the intervention in which 59 participants were randomly allocated to one of four conditions; a combination of PMT and implementation intentions, PMT only, implementation intentions only and a control group. Participants self-report email security behaviour, objective phishing detection ability and self-report perceptions of their threat appraisal (severity and susceptibility) and coping appraisal (response efficacy, response costs & self-efficacy) were assessed at baseline, post exposure and at 1-week follow-up. The study found that those exposed to the combined intervention and the motivational-only had significantly better objective performance compared to the control group at post-exposure. The combined intervention had sustained performance compared to control after 1-week but there was a significant reduction in performance for the PMT-only group. This suggests that the motivational intervention alongside the goal setting led to sustained performance at 1-week follow-up compared to a control group. Further analyses revealed that these observed differences were for participants' overall accuracy in detecting genuine and phishing emails and approaching significance for participants' genuine precision detection ability but no effect on

phishing precision ability. Moreover, the study found no effect of the intervention on self-report email security behaviour. The study found that there was a significant improvement in some components of threat and coping appraisal perceptions regardless of condition. Response efficacy was the only perception to change significantly as a result of the intervention in which those exposed to the motivational components had significant increases in their perceptions of response efficacy.

1.10 | ORIGINAL CONTRIBUTIONS OF THIS THESIS

1. Demonstrated that internal factors appear to play more of a role in determining security behaviours than environmental factors (Study 1, Chapter 3)

2. Demonstrated that internal factors play differing roles for different security behaviours (Study 1 & 3, Chapter 3 & 5)

3. Showed that the behaviours that comprise IS policy compliance are influenced by different factors (Study 1 & 3, Chapter 3 & 5)

4. Developed and validated a new scale to measure information sensitivity appraisal in the workplace that predicts security behaviour (Study 2, Chapter 4)

5. Identified which factors from the extended PMT-model best predict three individual security behaviours (Study 3, Chapter 5)

6. Motivational intervention leads to enhanced objective security behaviour on email legitimacy tasks (Study 4, Chapter 6)

7. Demonstrated the benefits of a combined motivational and volitional intervention for sustaining behaviour change effects for objective email security behaviour (Study 4, Chapter 6)

8. Demonstrating that implementation intentions are an appropriate technique to sustain security behaviour and response efficacy perceptions (Study 4, Chapter 6)

9. Identified response efficacy as a barrier to security behaviour uptake (Study 1, Chapter 3) and a key determinant of motivation to perform security behaviours (Study 3, Chapter 5) and that response efficacy can be improved through motivational interventions and sustained through implementation intentions (Study 4, Chapter 6)

CHAPTER 2: LITERATURE REVIEW

Work from this chapter has contributed to the following publications:

Blythe, J.M., & Coventry, L. (2012). Cyber Security Games: A New Line of Risk. In Entertainment Computing-ICEC 2012 (pp. 600–603). Springer Berlin Heidelberg.

Blythe, J.M. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In Proceedings of CHItaly 2013 Doctoral Consortium (pp. 92–101).

Coventry, L., Briggs, P., Blythe, J.M., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Summary report for the Government office for science.

This chapter focuses on the existing literature exploring security behaviour within the workplace. The chapter is split into four sections to provide greater clarity of the research problem. The first section (2.1) discusses approaches to conceptualising security behaviour in existing research; the paradigms adopted will be evaluated and reviewed on their contributions to understanding what motivates behaviour. The second section (2.2) discusses research exploring what influences and prevents security behaviour. The psychological principles behind security behaviours will be reviewed and issues with existing research will be discussed in relation to organisational security behaviour. The third section (2.3) focusses on behaviour change and the approach to be adopted in this thesis. The final section (2.4) focuses on existing experimental literature exploring attempts to change security behaviour. The studies will be evaluated and theoretical approaches to behaviour change will be outlined. Taken together, the four sections identify the gap in the literature of why employees behave securely or insecurely, and shortcomings in previous attempts to improve the human element of organisational security.

2.1 | APPROACHES TO STUDYING AND CONCEPTUALIZING SECURITY BEHAVIOUR

Before understanding what motivates employees to behave securely, it is necessary to outline how security behaviour is measured, conceptualised and explored within research.

The quantitative studies in this domain focus on what leads employees to comply with their organisation's IS policy. These studies often test theoretical models, analysing hypothesised relationships with regression analyses and modelling. The majority of studies except Ng, Kankanhalli, and Xu (2009) and Workman, Bommer, and Straub (2008) define security behaviour as *"intention to comply with* the IS policy" and use this as an outcome measure. However, there is a lack of focus on specific behaviours in the workplace and those which do

focus on single behaviours tend to focus on private use of technology rather than workplace use (e.g. Crossler, 2010; Gurung, Luo, & Liao, 2009; Lee, Larose, & Rifon, 2008; Zhang & McDowell, 2009). Organisational studies that have focussed on specific security behaviours in the workplace have often been qualitative (e.g. Albrechtsen, 2007; Inglesant & Sasse, 2010), and thus have not hypothesised relationships.

The continued use of and focus on policy compliance can be attributed to the adoption of behaviour change models and theories from health psychology, where medical compliance was once one of the most frequently researched forms of health behaviour. However, shifts in research approaches led to more focus on medical adherence than compliance as the former is thought to provide more conceptual clarity about an individual's self-regulation and independence whereas compliance focuses on obedience to rules and procedures (Leventhal, 1993). Learning lessons from health approaches and applying them to security may, therefore, provide better alternatives to conceptualising and understanding behaviour. Currently, the usage of compliance in information security may not be suitable as there are a number of issues with organisational research that conceptualises security behaviour as "IS policy compliance".

Firstly, IS policy compliance implies that information security is an individual behaviour. However, the picture is not clear-cut as research by Posey (2010) found 67 protective behaviours in the workplace.

Secondly, this approach assumes that employees have knowledge of the content of their organisation's IS policy and awareness of their roles and responsibilities for information security. Whitten (1999) refer to this as an abstraction property in which security policies may be unintuitive and alien to users. Research has also noted difficulties for participants taking part in studies using an IS policy compliance approach. Sommestad, Karlzén, and Hallberg (2015) found that some participants had difficulties when answering at the abstraction level of overall policy compliance rather than questioned about a particular security behaviour. This abstraction problem also means that participants may adopt different frames of reference when answering questions depending on what is most salient to them in relation to information security. For example, one participant may think about passwords while another may think about using anti-virus software. Therefore, in the absence of a direct behaviour within questions, employees' frame of reference may vary making comparisons difficult.

Thirdly, organisations differ in their approaches to their IS policy. There is a lack of consensus about the content of these policies so there will be diversity in the behaviours that are depicted within them. Furthermore, companies vary in the way they deploy and manage their policies which is complicated by newer forms of security documents that complement the IS policy (e.g. home working policies, BYOD). Approaches to information security management will also vary

across organisations. Different levels of security maturity and legislative obligations (e.g. Data Protection Act (1998)) mean that there are differences in the policies across organisations. These findings may account for the inconsistent findings using the IS policy compliance approach. A meta-analysis by Sommestad, Hallberg, Lundholm, and Bengtsson (2014) exploring variables that influence compliance with IS policies found that they explained little variance and when used in multiple studies, there was considerable variation.

Finally, IS policies are rarely updated and they lag behind the evolving cyber threat landscape (Dlamini, Eloff, & Eloff, 2009) so the behaviours outlined within the policies may not the most desirable for combating newer security threats.

The implications of this paradigm are wide-ranging - from measurement difficulties to concerns for the theoretical underpinnings of these studies. A number of studies exploring what motivates and causes individuals to comply with their policies have identified behavioural determinants important for information security compliance. However, these determinants may not predict all the behaviours that comprise compliance. For example, factors such as social pressures may have more of an influence on password behaviour than preventative anti-virus behaviour. It is, therefore, important to understand how factors might differ in their influence on specific behaviours. Some research (e.g. Fishbein & Cappella, 2006) has also emphasised the importance of assessing the degree to which behavioural determinants influence specific behaviours and how they may vary depending on the behaviour and the population under investigation. However, previous studies have not explored these differences in employee information security behaviour. It is, therefore, important to explore the individual behaviours required for full compliance rather than generic compliance.

2.2 | FACTORS INFLUENCING SECURITY BEHAVIOURS

Existing research investigating what influences individuals' engagement in security behaviours has used theories from psychology and other disciplines to identify drivers of security. Studies may utilise components from behavioural theories or may study the whole theory in isolation in an attempt to explain as much variance as possible in the outcome variable (e.g. intention to perform behaviours, engagement in actual behaviours or attitude towards behaviours). Using models from behaviour change literature is useful to understand the processes that underpin security behaviours. By identifying the causes of secure and insecure behaviour, interventions can be designed to promote secure behaviour based on the strength of the relationships between the theoretical constructs, models and the security behaviour of interest. Furthermore, consideration of what determines secure or insecure practice allows a better understanding of what prompts and regulates the behaviour within the workplace setting.

Models from health psychology are particularly relevant as health behaviours are similarly sensitive to that of security behaviour. Within health, individuals have to undertake many preventative behaviours (Kasl & Cobb, 1966) such as sanitising hands in hospitals to prevent contamination. Similarly, in information security, individuals have to take preventative action (such as running their anti-virus scanner) to prevent their organisation experiencing a security breach.

Many models within psychology aim to understand the causes of individuals' behaviours and ultimately find ways to stimulate positive behaviour change. This review discusses those which have previously received the most attention within the information security domain. These theories will be discussed along with research that has demonstrated their efficacy for behaviour change.

2.2.1 | THEORIES OF BEHAVIOUR CHANGE USED IN SECURITY RESEARCH

This section outlines theoretical models that are consistently used within behavioural IS research. Weinstein, Rothman, and Sutton (1998) note that there is a distinction between continuum theories and stage theories of behaviour. Continuum theories posit factors along a continuum that contribute to the prediction of an action and according to continuum theories, the factors and the actions are considered to be the same for everyone. Stage theories, on the other hand, are a specific set of stages which an individual must progress through. The current section will focus on continuum theories of behaviour as they explain factors that influence and motivate behaviours. Lebek, Uffen, Breitner, Neumann, and Hohler (2013) conducted a literature review on employees' information security behaviour across 113 publications and found that four commonly used theories were the Theory of Planned Behaviour, General Deterrence Theory, Protection Motivation Theory and the Technology Acceptance Model. This literature review corroborates their findings but also adds the Health Belief Model as a commonly adopted paradigm and discusses these theories in depth and identifies overlapping concepts between theories.

2.2.1.1 | The Theory of Planned Behaviour
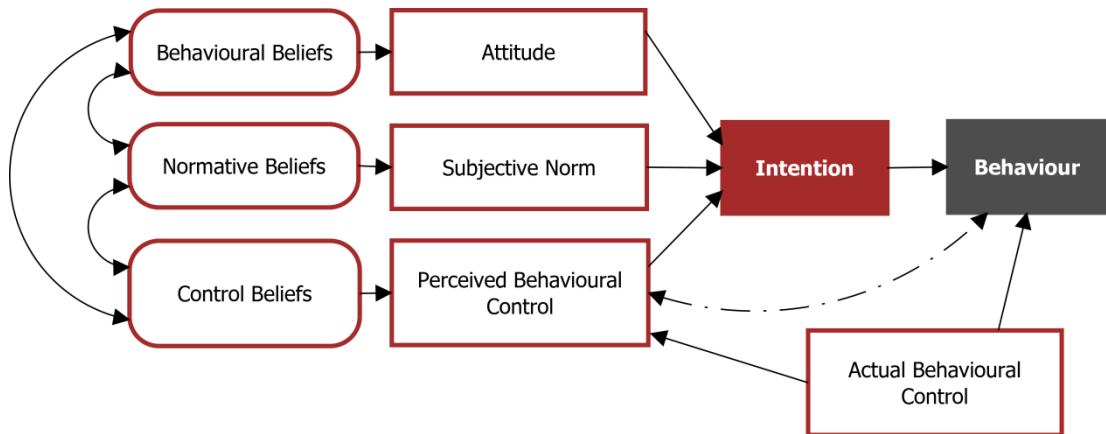
Figure 3. Theory of Planned Behaviour

The Theory of Reasoned Action (TRA; Fishbein, & Ajzen, 1975) and the Theory of Planned Behaviour (see Figure 3; TPB; Ajzen, 1991) are examples of continuum theories and are widely used to explain the relationship between attitudes and behaviour. These models contain attributes of value-expectancy theory that aim to explain and predict attitudes towards objects and actions, and in these cases security actions. Value-expectancy posits that attitudes are a function of beliefs and values (Fishbein & Ajzen, 1975). Expectancy refers to beliefs about how well a person can perform a task or activity, and value refers to the incentives or reasons for performing that task or activity. An individual's attitude towards behaviour is the result of the perceived likelihood of outcomes associated with the behaviour and the expected value or evaluation of those outcomes. The overall desirability of the behaviour is based on the sum of the expectancy and value of outcomes. The TPB (Ajzen, 1991) suggests that intention drives behaviour and that intention is in turn driven by attitude, subjective norms and an individual's belief in their competence to perform that behaviour (perceived behavioural control; PBC).

The TRA and TPB have identical attitudinal and social norm-related components and posit behavioural intention as preceding behaviour. The TPB (Ajzen, 1991) extends the TRA by adding PBC as a variable that affects intention towards behaviour and is the individual's perception of how easy it is to perform the behaviour, PBC can also act as a predictor of actual behaviour. Ajzen added PBC as the TRA did not account for behaviours that were not under volitional control. The addition of PBC allows an understanding of how people deal with situations where they may lack volitional control over behaviour by accommodating non-volitional elements in behaviours (Ajzen, 2002). However, research has debated the distinctiveness of PBC from self-efficacy (Manstead & Eekelen, 1998) with some research (Terry, 1993) arguing that self-efficacy is based on internal control factors whereas PBC is concerned with more external constraints. Other research has found self-efficacy to predict

intention (but not behaviour) and PBC to predict behaviour (but not intention) in the context of exercise (Terry & O'Leary, 1995).

The TPB further distinguishes between three types of salient beliefs: behavioural, normative, and control. These beliefs play a significant role in determining the three influencers of intention; attitude, subjective norms and PBC respectively. Behavioural beliefs are the expected consequences of performing the behaviour. The second type of beliefs is normative beliefs and these are about the views of significant others. The third is control beliefs and these are about the presence of factors that may impede or enable performing the behaviour.

Research has shown the predictive power of TPB constructs on intention and behaviour with ranges from 39% for intention and 27% for behaviour (Armitage & Conner, 2001) and 50% for intention and 29% for behaviour (Hagger, Chatzisarantis, & Biddle, 2002). The addition of PBC has been found to add 6% to the prediction of intention independently of variables shared with TRA in a meta-analysis by Armitage and Conner (2001). Recently, a review of over 200 studies exploring health behaviours found that intention and PBC explained 19% of the variance in behaviour and subjective norms while attitude and PBC explained 44% of the variance in intention (McEachan, Conner, Taylor, & Lawton, 2011).

Taylor et al. (2006) in a review of TRA, TPB and other health models to study and predict health-related behaviour change found no evidence that interventions based on TRA and TPB theories has contributed to either improved or reduced negative health outcomes in the UK, over and above that achieved by other theories or non-theory-based interventions. Recent discussion on the continued usage of TPB has discussed the utility of the model as it is not a casual model so provides little in the way of informing behaviour change and that its continued usage and interest is due to its correlational components (Sniehotta, Presseau, & Araújo-Soares, 2014). However, Conner (2014) argued that the model may be useful for examining the impact of interventions on components of the TPB, for longitudinal studies exploring the determinants of intentions, and for targeting these determinants within interventions.

2.2.1.2 | Protection Motivation Theory
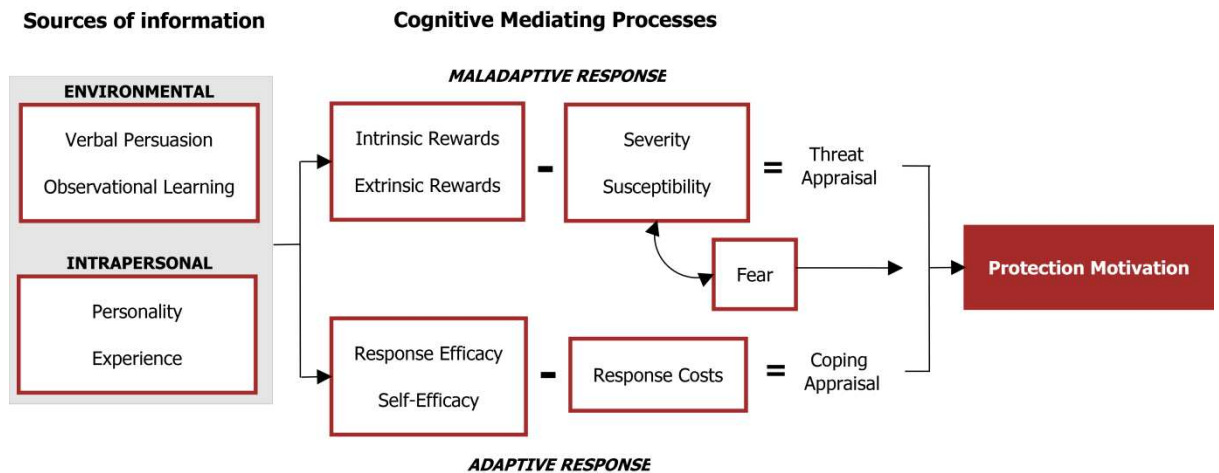
Figure 4. Protection Motivation Theory

Protection Motivation Theory (PMT) was developed by Rogers (1975) to explore the effects of persuasive messages and risk perceptions. The model was initially developed to explain fear appeals but has been further revised by Rogers (1983, 1984) to propose that we protect ourselves using threat and coping appraisals.

It is a core theory in understanding individuals' threat and coping appraisal processes and its links to motivating people to undertake adaptive (protection motivation) or maladaptive action. Maladaptive actions are those that place an individual at risk; this includes behaviours that lead to negative consequences (such as not encrypting a USB stick) or the absence of protective behaviours, which may eventually result in negative consequences. High intrinsic or extrinsic rewards of engaging in the maladaptive behaviours heighten the likelihood of undertaking maladaptive coping. Adaptive actions, in contrast, are protective behaviours that mitigate the threat stemming from threat and coping appraisal. According to PMT, information elicits either adaptive or maladaptive responses by influencing the threat and coping appraisal components. The sources of such information are either environmental (e.g. observational learning, verbal persuasion) or intrapersonal (e.g. prior experience).

Threat appraisals consider the factors that increase or decrease the chances of making an adaptive response by assessing the severity of the situation and perceived susceptibility to the threat. Coping appraisal considers the response efficacy (beliefs that adopting a particular behavioural response will be effective in reducing threats) and self-efficacy (belief in one's ability to execute the recommended courses of action successfully) of making an adaptive response. An individual's protection motivation stems from both the threat appraisal and the coping appraisal. Protection motivation is a mediating variable functioning to arouse, sustain and direct protective actions (Boer & Seydel, 1996).

Threat and coping appraisal are also part of the health belief model (Rosenstock, Strecher, & Becker, 1988) and the extended parallel process model (Witte, 1992), both of which explain how people appraise and respond to threats.

Milne, Sheeran, and Orbell (2000) in a meta-analysis of PMT found the average correlation between protection motivation (intention) and future behaviour was .40, a moderately strong relationship. Floyd, Prentice-Dunn, and Rogers (2000) in a meta-analysis of 65 studies using PMT found that the overall effect size was moderate (d=.52) for the prediction of over 20 health behaviours. Coping appraisal has been found to have the strongest associations with protection motivation (Bui, Mullan, & McCaffery, 2013; Floyd et al., 2000; Milne et al., 2000; Plotnikoff et al., 2010). Components of PMT have also been found to be useful in designing health interventions (Hodgkins, Sheeran, & Orbell, 1998) and persuasive fear appeals and high-efficacy messages produce the greatest behaviour change (Witte & Allen, 2000).

2.2.1.3 | Health Belief Model
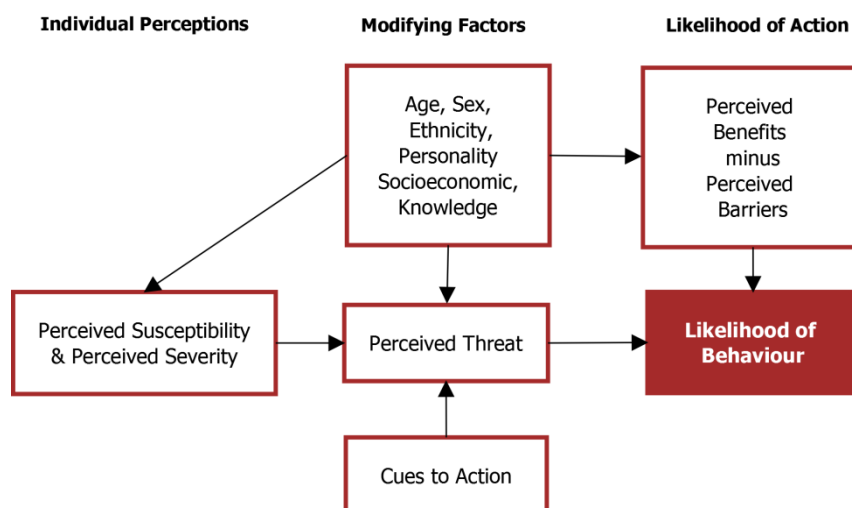
Figure 5. Health Belief Model

The Health Belief Model (HBM; see Figure 5) is another continuum theory based on risk perception that attempts to explain and predict health behaviours. The most recent version of the model identifies two considerations in an individual's intention to adopt behaviour in response to a threat: their perception of the threat (perceived susceptibility and perceived severity) and evaluation (perceived benefits and perceived barriers) of the required behaviour to resolve the threat. In addition, behaviour is modified by internal (e.g. symptoms) and external (e.g. the media) cues to action. The original model has been amended to include the additional factors of health motivation (Becker, 1974) and perceived control (Becker & Rosenstock, 1987).

A meta-analysis of 18 studies by Carpenter (2010) found that perceived barriers and perceived benefits to be the strongest predictors of behaviour but perceived severity was weak. However,

they cautioned against the continued use of the model to explore direct effects and suggested that future research should examine possible mediation and moderation between its core components.

Taylor et al. (2006) in a review of research adopting HBM found no evidence that HBM-based interventions have contributed positively to improved health outcomes in the UK. The HBM has also been found to be a less powerful predictor of intention and behaviour compared to TRA and was least powerful in predicting outcomes when compared to TRA and social cognitive theory in a meta-analytic review (Zimmerman & Vernberg, 1994). A recent meta-analysis by Jones, Smith, and Llewellyn (2014) of 18 studies investigated interventions based on HBM to improve health adherence and 83% of these made improvements and 39% of studies showed moderate to large effect sizes. While the meta-analysis indicated that HBM was effective in driving behaviour change, the authors were cautious about the utility of the model as only 6 of the studies explored the model in its entirety.

Davinson and Sillence (2010, 2014) have shown HBM to be useful for analysing qualitative data around security and financial transactions and has provided some support for driving anti-phishing security behaviour.

2.2.1.4 | Deterrence Theory

In the context of security, theoretical considerations of deterrence are important for discouraging computer abuse at work. Unlike erroneous or accidental behaviours that can lead to a security breach, misuses of information systems are knowingly performed and violate the organisational IS policy. These can be malicious (e.g. stealing confidential information) and non-malicious (e.g. circumventing a security process to save time and effort for productivity).

Deterrence theory is a prominent theory within criminology which posits that people make decisions about committing a crime (or breaking organisational rules and procedures) based on the benefits and costs. It focuses on formal sanctions such as the legality of acts and argues that the higher an individual's perceived certainty, severity and swiftness of the sanctions following the act, the more they are deterred from it (Gibbs, 1975).

Formal sanctions in the workplace will be described in the IS policy of the organisation which may include disciplinary action. Sanctions can also be informal and include shame and social disapproval (Piquero & Tibbetts, 1996). When sanctions are less certain and severe, employees may not fully comply with the IS policies because they do not expect to be punished by their organisation.

2.2.1.5 | Technology Acceptance Model
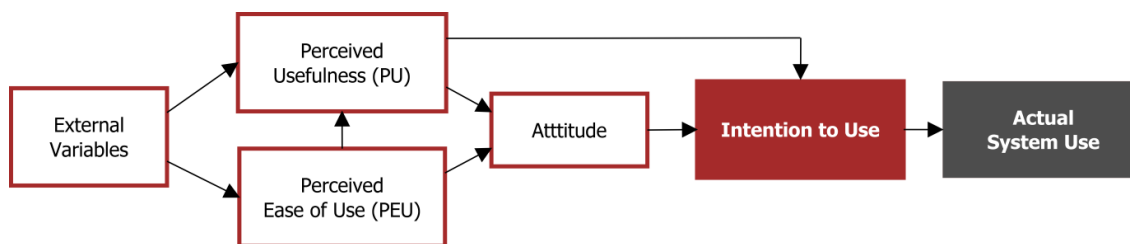
Figure 6. Technology Acceptance Model

An important consideration when disseminating a piece of security software across an organisation is the extent to which it will be accepted and used by employees. There has been a wealth of research and support of the Technology Acceptance Model (TAM) developed by Davis (1989). Based on the TRA, the model attempts to explain why a user will accept or reject technology. Initially developed to explain organisational users' behaviour, the model has been adopted to explain regular users' adoption intentions and behaviour. The model posits that the perceived usefulness of the system and perceived ease of use are two important beliefs that influence an individual's attitude towards the system. Perceived usefulness (PU) is defined as *"subjective probability that using a* specific application system will increase his or her job performance within an organisation*al context"* (Davis, Bagozzi, & Warshaw, 1989)(p.985). Perceived ease of use (PEU) is defined as *"the degree to which a person believes that using a* particular system would be fr*ee from effort"* (Davis et al., 1989) (p.985). Like TRA, TAM argues that usage is determined by intention which is in turn influenced by attitude and perceived usefulness. Studies adopting TAM either explore the effect of perceived usefulness and perceived ease of use directly on intention or look at the mediating role of attitude on intention with little variation in explanatory power between the two approaches (Dillon & Morris, 1996).

Meta-analyses have indicated that TAM is a valid and robust model (King & He, 2006), however, other reviews have warned against using the model outside of its validated setting as PEU and PU have weak relationships with actual usage (Turner, Kitchenham, Brereton, Charters, & Budgen, 2010).

2.2.2 | THEORY OVERVIEW

Lebek, Uffen, Breitner, Neumann, and Hohler (2013) conducted a literature review on employees' information security behaviour across 113 publications and found that four commonly used theories were the Theory of Planned Behaviour, General Deterrence Theory, Protection Motivation Theory and the Technology Acceptance Model. Table 2 shows the use of these theories in organisational and consumer research.

Table 2. The most commonly explored theories and their usage in organisational and consumer behavioural information security research

		Organisational Studies	Consumer Studies
Theory	**Protection Motivation Theory**	Crossler, Long, Loraas, & Trinkle, 2014; Herath & Rao, 2009b; Ifinedo, 2011; Pahnila, Siponen, & Mahmood, 2007; Siponen, Mahmood, & Pahnila, 2014; Vance et al., 2012	C. Anderson & Agarwal, 2010; Chenoweth, Minch, & Gattiker, 2009; Crossler et al., 2014; Crossler, 2010; Gurung et al., 2009; D. Lee et al., 2008; Mwagwabi, McGill, & Dixon, 2014; Woon, Tan, & Low, 2005; L. Zhang & McDowell, 2009
	Theory of planned behaviour / Theory of reasoned action	Bulgurcu, Cavusoglu, & Benbasat, 2010; Ifinedo, 2011, 2014; Pahnila et al., 2007; Siponen et al., 2014	Burns & Roberts, 2013; Y. Lee & Kozar, 2008; J. Zhang, Reithel, & Li, 2009
	General deterrence theory	Aurigemma & Mattson, 2014; Cheng, Li, Zhai, & Smyth, 2014; Cheng, Li, Li, Holm, & Zhai, 2013; D'Arcy & Devaraj, 2012; D'Arcy, Hovav, & Galletta, 2008; Herath & Rao, 2009b; Pahnila et al., 2007; Siponen, Pahnila, & Mahmood, 2010	
	Technology acceptance model		Dinev, Goo, Hu, & Nam, 2009; Dinev & Hu, 2007; Herath et al., 2014; Kumar, Mohan, & Holowczak, 2008; Y. Lee & Kozar, 2008; Shropshire, Warkentin, & Sharma, 2015

These psychological theories share overlapping constructs but with different conceptualizations (Michie et al., 2005). So whilst studies may adopt different theories, the underlying constructs under investigation may be the same.

Table 3 illustrates the similarities in the underlying concepts offered by these theories which is then used a basis to structure the rest of the literature review. Additional factors necessary for understanding behaviour in the workplace but not covered in the behavioural models are presented in the table and will be discussed in the literature review.

Table 3. The most commonly explored theories and overlapping constructs in behavioural information security research

Section	Categorisation for literature review																				
	Threat evaluation			Coping evaluation			Internal influencers					Environmental influencers									
	2.2.3			2.2.4			2.2.5					2.2.6									
Constructs	Perceived Susceptibility	Perceived Severity	Fear Appeals	Response efficacy/perceived benefits	Self-efficacy/ Perceived behavioural control	Response costs / perceived barriers	Attitude	Knowledge, awareness, and experience	Memory and cognition	Personality	Psychological Ownership	Cues to action	Subjective norm (social influences)	Organisational culture	Rewards/incentives	Punishment severity/sanctions	Detection certainty	Positive organisational behaviour	Design and usability of security	Persuasion and Deception	Intention/Motivation
Behavioural models — Protection Motivation Theory (2.2.1.2)	X	X	X	X	X	X															X
Health Belief Model (2.2.1.3)	X	X		X	X	X						X									X
Theory of planned behaviour (2.2.1.1) / Theory of reasoned action (2.2.1.1)					X (TPB)		X						X								X
General deterrence theory (2.2.1.4)																X	X				
Technology acceptance model (2.2.1.5)							X	X							X				X		X
Important factors not covered in behavioural models									X	X	X	X		X	X			X		X	

2.2.3 | THREAT EVALUATION

There are many threats to organisations' information resources such as insider threats, hackers and malware. When an employee perceives a threat to the organisation's information assets, they evaluate the threat based on the degree of severity of the threat and their perceived susceptibility to it.

2.2.3.1 | Threat Evaluation: Perceived Severity

Perceived severity is the assessment of the seriousness of a security threat and its associated consequences. Weinstein (2000) highlight the importance that it is independent of an individual's perception of the likelihood of a threat. Ifinedo (2011) defines it in the context of IS compliance and focusses on the severity towards one's organisation's information. Other definitions go beyond focussing purely on consequences towards data and systems. For example, Ng et al. (2009) argue that the consequences can have implications for the employees' job or organisation as the loss of availability, confidentiality and integrity of information can negatively affect the organisation and can also disrupt the employees' work. If it resulted as a consequence of an employee's behaviour, they might be held responsible for the cause of the security breach. Severity perceptions arising from security threats can, therefore, have consequences that directly affect the employee and their organisation. Not all research focuses on these differences in severity implications for employees and organisations.

The research investigating perceived severity in an organisational context has demonstrated mixed findings. Research has found a significant relationship between perceived severity and employees' intentions to comply with their organisations' information security policy. Herath and Rao (2009b) found an indirect role as severity significantly influenced security breach concern which in turn was found to influence employees' security policy attitude. Others have found significant positive relationships between severity and compliance intention (Siponen et al., 2014; Vance et al., 2012). Ifinedo (2011) however did not find a direct relationship and they attribute this to potential differences in how severity is explored within different models. They argue that it may have an indirect relationship with security compliance which may account for its supportive indirect role with other factors in studies by Herath & Rao (2009).

Studies have supported the direct role of severity in consumers' anti-spyware adoption (Chenoweth et al., 2009; Gurung et al., 2009; Liang & Xue, 2009) and securing home wireless networks (Woon et al., 2005). Research exploring other security behaviours in consumers has been more mixed as research by Lee, Larose, and Rifon (2008) found that severity did not affect anti-virus protection behaviours. Crossler (2010) found opposing effects as perceived severity influenced consumers' backing up data behaviours but this relationship was negative which they argue may be due to the behaviour and threat under investigation. Zhang and McDowell (2009)

found that severity did not relate to students' intentions to adopt password protection strategies (i.e. updating passwords frequently, using strong passwords and unique passwords for different accounts). The findings of these studies suggest that severity perceptions and their influence may differ by type of security behaviour which may explain the lack of support in some studies.

Other research has indicated an indirect relationship between severity and security behaviour, in line with the findings by Herath and Rao (2009b). Ng et al., (2009) explored severity in the context of being cautious with emails that have attachments with employees. They found that severity did not have a significant effect on security behaviour but had moderating effects on other variables which influence security behaviour. They found that it increased the effect of cues to action and general security orientation (their predisposition towards security) but reduced the effect of perceived benefits and self-efficacy. This suggested that when severity perceptions are high, perceived benefits and self-efficacy are not as important in driving one's decision to undertake security behaviours.

A limitation of the existing research in the workplace is that it generally does not focus on severity of specific security threats but rather uses items that refer to the broad term "security threats". Only a few studies of consumers focus on the specific security threats in their items such as viruses (Lee et al., 2008; Ng et al., 2009), wireless hacking (Woon et al., 2005) and spyware (Gurung et al., 2009; Liang & Xue, 2010).

In summary, severity appears to play a role in consumers' security behaviours and employees' compliance with information security policies. Some research suggests that it may play a direct role in security (Chenoweth et al., 2009; Gurung et al., 2009; Siponen et al., 2014; Vance et al., 2012) or play a more indirect role and moderate the effect of other factors on security (Herath & Rao, 2009b; Ng et al., 2009) such as combining with susceptibility to influence perceived threat and subsequently security behaviour (Liang & Xue, 2010; Mwagwabi et al., 2014). Despite the support of a role for severity in driving security behaviour, there appear to be inconsistencies in whether it plays a direct role or indirect role. Future research needs to explore specific threats in the context of work and further understand the direct or indirect role of severity on behaviour.

2.2.3.2 | Threat Evaluation: Perceived Susceptibility

Perceived susceptibility is the second component of an individual's threat evaluation as outlined in PMT and HBM. Aiken, Gerend, Jackson, and Ranby (2012) note that the terms perceived risk, susceptibility and vulnerability are often used interchangeably in literature but refer to the subjective likelihood of being a victim of a threat, independent from their perceptions of the severity of the threat. This thesis will use the term perceived susceptibility, as vulnerability has different connotations within computer security. Perceived susceptibility is *an individual's* assessment of the probability of threatening events (e.g. threats towards security). Employees

may have differing perceptions of the likelihood of different threats, for example, they may feel they are more likely to be a victim of a malware attack than having their account compromised.

There has been less research exploring the role of susceptibility on security behaviour. Research has supported the positive relationship between perceived susceptibility and compliance intention (Ifinedo, 2011; Siponen et al., 2014). Other research exploring an indirect relationship between susceptibility and security breach concern level has not found a significant relationship (Herath & Rao, 2009b). Recently, Crossler et al., (2014) found that susceptibility did not influence intention or actual compliance to BYOD policies.

Research on consumers' behaviour has also found a relationship with the use of virus protection behaviours (sum of using anti-virus software, installing OS updates, setting up email filters and installing a firewall) (Lee et al., 2008). However, other research found it did not play a role in password protection behaviours (Zhang & McDowell, 2009). There have also been mixed findings for its role in anti-spyware software usage. Some research has not found a relationship for use of anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009) whereas other research supported an indirect role of susceptibility when combined with severity as it influenced individuals' perceived threat for using anti-spyware software (Liang & Xue, 2010) and complying with password guidelines (Mwagwabi et al., 2014).

Other research suggests conflicting findings. Ng et al., (2009) also found that susceptibility influenced security behaviour in the context of being cautious with email attachments. Other research by Woon et al. (2005) found that perceived susceptibility was not significantly related to enabling security measures on home wireless networks. Other research, however, has found that susceptibility negatively affected consumers backing up data behaviours (Crossler, 2010).

Like severity, the body of research exploring security in the context of work do not focus on specific security threats within their items and use the broad term "security threats" (Herath & Rao, 2009b; Ifinedo, 2011; Siponen et al., 2014). Unlike severity, the research supporting a direct role or indirect role of susceptibility has been less consistent.

2.2.4 | COPING EVALUATION

Coping evaluation is how an individual responds to threatening situations considering their ability to enact recommended courses of action successfully (self-efficacy), expectations of the efficacy of the action in reducing the threat (response efficacy) and costs associated with taking the course of action (response costs).

2.2.4.1 | Coping Evaluation: Self-efficacy

Research has explored end-users' beliefs in their capabilities to undertake security actions. Self-efficacy is one such capability and can be defined as *an individual's beliefs about their*

competence to cope with a task and exercise influence over the events that affect their lives (Bandura, 1977). In a security context, employees who have high security-related capabilities and competence are presumed to be more likely to follow security practices as they are more effective in learning how to follow them and being able to perform the appropriate behaviour.

The importance of self-efficacy for behaviour can be demonstrated by its occurrence in many behaviour change theories including PMT, HBM and emphasised heavily in SCT. The TPB/TRA also explores a construct similar to self-efficacy which is Perceived Behavioural Control.

Bandura (1997) posits that there are four sources of an individual's self-efficacy which can account for differences in individuals' levels of self-efficacy (Bandura, 1997). The first is past accomplishments or past experience (enactive mastery); Bandura argues that employees who have succeeded in job tasks are likely to have more confidence in completing similar job tasks than those who have been unsuccessful in the past. Success raises an individual's mastery expectations of task performance, while failure lowers these expectations. Therefore, within security, prior experience of conducting security tasks at home or in the workplace should lead to higher levels of confidence in employees' ability to undertake security tasks. Bandura argues that our beliefs about self-efficacy are specific to particular situations so while employees may have high self-efficacy for one security behaviour, it may not necessarily transfer to other security behaviours.

Another source of self-efficacy is vicarious experience that suggests that individuals can build their levels of self-efficacy by observing others perform the behaviour. In the workplace, if managers and colleagues are behaving securely, employees can learn through observation, which will increase their security self-efficacy. Research suggests that this source of information is weaker than mastery experience in helping to build self-efficacy beliefs (Bandura, 1997). A third source of self-efficacy is verbal persuasion which is convincing people that they have the ability and can cope with specific tasks. Coaching is a form of verbal persuasion used in organisations to increase self-efficacy and is often used in training employees. Positive persuasion is likely to work in encouraging and empowering employees to behave more securely, whereas negative persuasion can weaken self-efficacy.

The final source of self-efficacy is emotional cues or physiological states in which the individuals' self-efficacy is influenced by their physiological (such as high heart rate) and emotional states (such as anxiety) in relation to the tasks. Negative states are heightened through people's expectations to fail and can lead to lower levels of self-efficacy. People are likely to expect success when they are experiencing positive arousal rather than negative.

Given the importance of self-efficacy for job performance and motivation, and computer use it is unsurprising that its role has been consistently supported in IS compliance research. (Bulgurcu et al., 2010; Crossler et al., 2014; Herath & Rao, 2009b; Ifinedo, 2011, 2014; Sommestad et al., 2015; Vance et al., 2012; Zhang et al., 2009).

Support has also been found for a relationship between self-efficacy/PBC and virus protection behaviours (Lee et al., 2008), using a personal firewall (Ng & Rahim, 2005), being cautious with email attachments (Ng et al., 2009), anti-spyware adoption (Gurung et al., 2009; Lee & Kozar, 2008; Liang & Xue, 2010; Sriramachandramurthy, Balasubramanian, & Hodis, 2009), enabling security measures on home wireless networks (Woon et al., 2005) and complying with password guidelines (Mwagwabi et al., 2014).

Rhee, Kim, and Ryu (2009) focussed solely on the role security self-efficacy plays on various security outcomes and to identify potential determinants of high or low self-efficacy. For experiences of security incidents, they found a negative relationship with self-efficacy suggesting that experience of a security threat may lower individuals' levels of self-efficacy for security. They found that self-efficacy was a significant determinant of students' use of security protection software, engagement in security conscious care behaviour and intention to strengthen their security efforts (e.g. learn more about security, add additional security measures).

Overall, the existing research suggests that self-efficacy is an important determinant of security behaviour by consumers and within the workplace.

2.2.4.2 | Coping Evaluation: Response Efficacy

Response efficacy is belief in the benefits of the behaviour (Rogers, 1983), and includes individuals' outcome expectancies with regards to security actions. It is a key component of an individual's coping appraisal within PMT. In the case of security, this is the belief that performing security behaviours is an effective way to reduce security breaches. On the other hand, if an individual has less belief in the effectiveness of the action, they are less likely to adopt it. Evaluation of outcome expectancies is a component of many different behaviour change theories but they offer different conceptualisations. The HBM refers to *"perceived benefits"* which is an individual's assessment of the efficacy of engaging in the behaviour in reducing threats (Janz & Becker, 1984). SCT refers to outcome expectancies which are the individual's belief that the behaviour will lead to a desirable outcome. People place different expectations or values on behavioural outcomes that can be either positive or negative (Bandura, 1986). Enacting behaviour is more likely to happen when individuals expect the behaviour to maximise positive outcomes and minimise negative outcomes.

Response efficacy has received less attention in information security research to date compared to other potentially influential factors. However, research has supported a positive relationship between attitude toward security policies (Herath & Rao, 2009b) and intention to adopt anti-spyware software (Johnston & Warkentin, 2010; Liang & Xue, 2010). Crossler (2010) found that response efficacy was significantly related to consumers backing up data behaviour and studies have shown it to relate to anti-spyware usage (Gurung et al., 2009; Liang & Xue, 2010), compliance with password guidelines (Mwagwabi et al., 2014), adopting password protective behaviours in students (Zhang & McDowell, 2009) and enabling security measures on home wireless networks (Woon et al., 2005).

The influence of response efficacy on IS policy compliance intention has been somewhat mixed. Some studies have supported a positive relationship between response efficacy and intention to comply with security policies (Ifinedo, 2011; Wall, Palvia, & Lowry, 2013), and to predict intentions in addition to actual compliance with BYOD policies (Crossler et al., 2014). Other research on IS compliance intention has been unsupportive (Siponen et al., 2010; Zhang et al., 2009) and two studies have indicated a negative relationship with compliance intention (Vance et al., 2012; Zhang et al., 2009).

Ng et al., (2009) found that perceived benefits significantly influenced individuals' email security behaviour. They also found that perceived benefits were moderated by perceived severity as it reduced the effect of perceived benefits and self-efficacy. When severity is high, benefits and self-efficacy are not as important in driving security behaviour.

Despite the lack of research exploring response efficacy in the workplace, research has been supportive of its relationship with security behaviours. However, recent literature reviews by Sommestad et al. (2014) on security compliance found that response efficacy was one of the worse predictors of compliance and IS misuse based on the effect sizes. However, they attribute this to variation in the findings of the four response efficacy studies in their review (Sommestad et al., 2014).

There appears to be some support for response efficacy on security behaviours in consumers. However, its relationship to employees' security behaviour is still unclear. This may be due to the abstraction problem of using overall policy compliance as a single behaviour, as users may feel it easier to provide an estimation of security effectiveness for specific security behaviours than an overall behaviour. Other research has also discussed participant difficulty in answering questions at this level (Sommestad et al., 2015). Overall, further research is needed to understand the role of response efficacy on driving specific security behaviours in the workplace.

2.2.4.3 | Coping Evaluation: Response Costs

Response costs refer to beliefs about how costly performing the recommended security behaviour will be. These costs may include monetary expense, time, and effort expended in behaving securely or other negative consequences, which result from performing the security behaviour. If an individual perceives that considerable resources will be required to carry out the action, they will be unlikely to follow through with the behaviour. Conversely, if few resources are required, the behaviour may be adopted. In other words, when an employee considers executing a behaviour, they conduct a cost-benefit analysis.

The HBM refers to response costs as "perceived barriers" which it views as the potential obstacles or negative aspects of engaging in behaviour (Janz & Becker, 1984).

Research findings are inconclusive on the role of response costs. Herath & Rao (2009b) found support for a negative relationship between response costs and compliance intention whereas Ifinedo (2011) and Crossler et al. (2014) did not find support for response costs. Mixed findings have also been reported between response costs and anti-spyware adoption (Chenoweth et al., 2009; Gurung et al., 2009; Liang & Xue, 2010). Ng et al., (2009) found no support for response costs in employees' email security behaviour. Additionally, Crossler (2010) found that response costs did not relate to the backing up behaviour of consumers. However, an older study by Woon et al. (2005) found response costs to be significantly related to determining if participants' enabled security measures on their home wireless network.

Response costs role in password behaviours is also inconclusive. Zhang and McDowell (2009) found that response costs had a significant negative relationship with intentions to engage in password protective behaviours but Mwagwabi et al. (2014) did not.

Despite the lack of support for response costs in quantitative research, the notion of the costly aspects of engaging in security behaviours within the workplace is well-documented in qualitative research. For example, the compliance budget proposed by Beautement, Sasse, and Wonham (2009) supports the role of response costs as they found that individuals and organisations place different values on the cost and benefits of behaviours with IS policies. They argue that an employee's choice to comply or not comply is determined by the perceived costs and benefits of compliance. Employees consider the potential cost towards the organisation and themselves.

Out of all the constructs within an individual's coping appraisal, response costs is the one which has the most disparity of findings despite the wealth of qualitative research suggesting the costly nature of security has a negative influence on security behaviour (Albrechtsen, 2007;

Beautement et al., 2009; Inglesant & Sasse, 2010). Further research is required to understand the role of response costs in preventing the uptake of security behaviour in the workplace.

2.2.5 | INTERNAL INFLUENCES

2.2.5.1 | Internal Influences: Attitude

Attitude is defined as *the individual's positive or negative feelings toward en*gaging in a specified behaviour. In the context of security, this is towards behaving securely or compliance to the IS policy.

The TPB posits that attitude is determined by individual's beliefs about the consequences arising from the behaviour and an assessment of the desirability of the outcome. Fishbein and Ajzen (1975) expectancy-value model explains how attitudes are formed. Attitudes develop from beliefs about a behaviour (e.g. changing passwords) which are attributes (e.g. cognitive load) associated with the behaviour. Individuals form an attitude by linking these beliefs to a certain outcome such as the cost incurred by doing the behaviour (e.g. mental effort). This attitude towards the behaviour is automatically acquired based on the positive or negative evaluation of the belief. Behaviours, which are associated with more desirable consequences are favoured more than those which are linked to undesirable consequences, and consequently, have a more favourable attitude. In understanding an individual's or populations attitude towards a behaviour, research explores the salient beliefs of the target group before attempting to change attitudes (Ajzen, 1991).

Individuals that have a positive attitude toward behaving securely are more likely to intend to behave securely. The influence of attitude on security compliance intention has been consistently supported in research (Bulgurcu et al., 2010; Herath & Rao, 2009b; Ifinedo, 2011; Pahnila et al., 2007; Sommestad et al., 2015; Zhang et al., 2009). Support has been found for a relationship between attitude and; anti-spyware adoption (Dinev & Hu, 2007; Lee & Kozar, 2008) and online privacy protective strategies (Yao & Linz, 2008; Burns & Roberts, 2013), updating anti-virus software (Ng & Rahim, 2005) and firewall adoption (Kumar et al., 2008; Ng & Rahim, 2005). Anderson and Agarwal (2010) found attitude to significantly relate to intentions to perform security-related behaviour to protect the internet (as a form of citizenship) and to perform security behaviours to protect their own computer. They also found that an individual's attitude was influenced by their concern regarding security threats, their perceived citizen effectiveness (a form of response efficacy towards helping to secure the Internet) and their self-efficacy.

Based on the wealth of research supporting the role of attitude, it appears to be an important determinant of security behaviour.

2.2.5.2 | Internal Influences: Knowledge, Awareness, and Experience

2.2.5.2.1 | Knowledge and Awareness

Employees cannot be vigilant against security threats or behave securely if they lack awareness of the risks or they lack knowledge and necessary skills to undertake effective security actions. Knowledge is a basic necessity for undertaking security behaviours and despite the wealth of practice that focuses on improving users' knowledge of security risks and behaviours, individuals remain unmotivated despite having the required knowledge and skills to protect themselves and their organisation (Kang, Dabbish, Fruchter, & Kiesler, 2015). Empowering users with required security knowledge is necessary for behaviour change but may not lead to an actual and sustained change in the long-term.

Aytes and Connolly (2004) assessed how much students knew about Cyber security and explored their awareness of risky security behaviours. They were interested in risky behaviour in three areas; password usage (such as sharing passwords), data backup and email-usage (such as not scanning email attachments for viruses). Despite the user group considering themselves to be highly knowledgeable and competent, they engaged in multiple risky behaviours indicating that knowledge is a poor predictor of students' actual levels of risky behaviour.

Furman, Theofanos, Choong, and Stanton (2012) explored knowledge, awareness and skills of end-users. By conducting in-depth interviews with 40 participants, they were able to identify myths and misconceptions around security. The majority of participants rated themselves as moderately knowledgeable to expert about computer security. Participants were familiar with security icons, trust marks and security terms but when further questioned were often unable to elaborate or provide clearer definitions. Overall, they found that while users were concerned about computer security and rated themselves to be knowledgeable they lacked the necessary skills to protect themselves.

Parsons, McCormac, Pattinson, Butavicius, and Jerram (2014) conducted a survey to explore the knowledge, attitudes and behaviours in relation to eight policy areas (importance, principles and rules of security, password management, email and internet usage, reporting security incidents, consequences of behaviour and training) across three government organisations. They found that employees had high and appropriate knowledge (measured by participants stating whether a statement was true or false) of information security rules and password security. However, their knowledge of wireless technology security was lacking.

Dinev and Hu (2007) looked at differences in IT experts and non-IT experts on intentions to engage in anti-spyware behaviours. They found that the influence of subjective norms on intention was significant for the IT group but not for the non-IT group. They argue that because

the IT group may have greater awareness surrounding spyware, they are more likely to discuss it within their social groups that may, therefore, lead to a greater influence from subjective norms. The findings of this study suggest that professional background and experience of individuals may play a role in influencing perceptions of subjective norms, and consequently engage in security behaviour.

Overall, the research suggests that knowledge may play a more indirect role in security behaviour. While it appears to be a necessary precursor, in isolation, it does not lead to secure behaviour.

2.2.5.2.2 | Experience

Experiences can be both negative and positive, and can potentially influence security behaviour in different ways. Negative experiences include breaches in security such as a virus infection or a personal account being hacked. These can result in many negative emotional states for the user such as frustration, annoyance and embarrassment. They can also have more severe consequences such as the potential for financial loss and identity theft. Experiencing such situations may heighten awareness of security threats and, therefore, led to adoption of security software or change in an individual's security behaviour. Experience is not just limited to threats but also the experience of protective security responses.

Within behaviour change, experience is studied as an individual's past behaviour. The well-known statement that "past behaviour is the best predictor of future behaviour" has been shown to have strong empirical support. Ouellette and Wood (1998) conducted a meta-analysis of existing research exploring past and future behaviour in different behavioural domains. They found that past behaviour was an important predictor of future behaviour and was comparable to that of other frequently studied behavioural influencers. Its impact on future behaviour was slightly weaker than intention's impact but it had a similar influence to that of attitude and had better predictive strength than behavioural control and subjective norms. They argue that past behaviour influences future behaviour through two processes. The first is in relation to habitual behaviour since the process of enacting the behaviour becomes automatic, requiring less decision making and conscious deliberation and secondly, the frequency of the past behaviour influences the habit strength of the future behaviour. They also argue that past behaviour may have a minimal direct effect on future behaviour when conscious decision making is required but rather will interact with attitudes and subjective norms to influence intention and subsequently, future behaviour.

Within PMT, experience is one source of intrapersonal information which influences individuals' threat and coping appraisal and can be defined as ''feedback from personal

experiences associated with the targeted maladaptive and adaptive responses" (Floyd et al., 2000), p. 409).

Few studies have explored security breach victimisation experiences and its influence on motivating individuals to undertake security actions. Lee et al. (2008) explored student's virus experiences and their intentions to adopt virus protection measures. They asked participants to rate the frequency of having been infected with a virus from downloading a file and from opening an email attachment. They found that there was a significant relationship between prior virus experience and intentions to engage in anti-virus protective behaviours. Individuals who had a computer virus are therefore more motivated to protect themselves. However, other research has found direct influence of experience on motivation. Anderson and Agarwal (2010) and Harrington, Anderson, and Agarwal (2006) found that personal experience of security violations and knowledge of people they know being affected by viruses did not influence attitude or intention measures for users protecting their own computer.

Undesirable experiences relating to proactive security behaviours are problematic as individuals may be less likely to engage in the security behaviour again to avoid experiencing a similar situation. Vaniea, Rader, and Wash (2014) found that negative experiences influenced users' future software update behaviour. When users have a bad experience with a piece of software, they will base future update decisions for this software on this experience and refrain from installing the update.

Experience of security threats and security behaviours, therefore, appears to influence current behaviour.

2.2.5.3 | Internal Influences: Memory and Cognition
All security behaviours will be influenced by the cognitive abilities of the user, however, none more so than those relating to passwords which research has shown to have high memory demands on people.

In the workplace, password-composition policies govern the complexity required by users' passwords. Inglesant and Sasse (2010) discuss the features of password policies that place pressure on users and those features that can help reduce cognitive burden. The demands placed on users include the password strength and character restrictions, frequency of password changes, and the number of passwords they are required to remember.

Inglesant and Sasse (2010) in their study on password use found organisational differences in employees' cognitive burden due to the restrictions set by their organisations. They found that difficulties arose when policies required unique, strong passwords, changed frequently and for them to differ significantly from previous passwords. Further restrictions which created a

burden on employees included being locked out of services for 2 hours during a password reset. Overly restrictive password policies, therefore, led to employees' maladaptive behaviour such as writing down passwords.

Given the average number of accounts individuals have passwords to manage for is around 8 (Grawemeyer & Johnson, 2011) and have on average 25 accounts protected (Florêncio & Herley, 2007), it is not surprising that motivation to rehearse and encode a password will be low due to the effortful process of transferring information from short term memory to long term memory (Hasher & Zacks, 1979).

Passwords are more easily remembered if the account is frequently used, as repetition and maintenance of rehearsal of the password will lead it to be stored in long-term memory. Forgetting passwords can cause problems for users; they will have to dedicate time to resetting the passwords which in the workplace setting can lead to users locked out of their work system for a period of time (Inglesant & Sasse, 2010), thus affecting their productivity.

Due to the many demands placed on users' memory, coping mechanisms are adopted to help overcome the cognitive issues including choosing passwords which have some personal characteristics (such as birth dates) (Brown, Bracken, Zoccoli, & Douglas, 2004), short in length (Brown et al., 2004), writing down passwords (Inglesant & Sasse, 2010), and more commonly, password re-use (Florêncio, Herley, & Oorschot, 2014; Grawemeyer & Johnson, 2011). All of these benefit the user's ability to authenticate themselves but lead to further security vulnerabilities as one compromised account can result in other accounts being comprised if the login credentials are the same.

To overcome the cognitive demands on users, alternatives to passwords have been developed with varying degrees of success such as graphical authentication systems - Passfaces (Valentine, 1998), Déjà vu (Dhamija & Perrig, 2000), VIP (De Angeli et al., 2002) and Passpoints (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005) to name a few. Those systems relying on recognition over recall are considered to be more effective, as they have fewer cognitive demands and take advantage of a user's ability to recall with or without a cue rather relying on pure recall (Nicholson, Coventry, & Briggs, 2013). Graphical authentication systems have been found to be more memorable than passwords but these advantages may not be sustainable (e.g. Chiasson, Forget, Stobert, Van Oorschot, & Biddle, 2009). Furthermore, these systems may be subject to observation attacks (Tari, Ozok, & Holden, 2006; Wiedenbeck, Waters, Sobrado, & Birget, 2006).

2.2.5.4 | Internal Influences: Personality

Recent research has started to explore personality and security behaviours. A wealth of research on personality has led to the development of many different theories and measurement of personality. One of the most commonly used is the five-factor model (McCrae & Costa, 1987) which represents a hierarchy of the personality traits; openness, extraversion, agreeableness, conscientiousness, and neuroticism. Despite the number of different conceptualisations and suggested factorial structures of personality, the big five structure has received consistent support (Barrick & Mount, 1991).

McBride, Carter, and Warkentin (2012) explored the big five personality traits in relation to participants' intentions to violate information security policy situations as depicted in scenarios such as disregarding the mandatory encryption procedure. Participants were asked to rate the degree to which they would act the same as the character. They found that open and neurotic individuals were less likely to intend to violate the policies than extroverted individuals.

Halevi, Memon, and Nov (2015) recently explored conscientiousness in relation to spear phishing. They used a targeted phishing message that appealed to conscientiousness and found that the conscientiousness level was significantly higher for those that fell for the phishing attack compared to those that did not. The phishing message appealed to efficiency and order by asking participants to review their time sheet by clicking on a link provided in the email. Wording within the email was intended to motivate conscientiousness individuals to act on the email. This study suggests that a person's personality may heighten their susceptibility to targeted phishing attacks.

Shropshire, Warkentin, and Sharma (2015) explored the role of conscientiousness and agreeableness on the intention-behaviour gap on individuals' adoption of security software. The software provides the user with recommendations for various activities to improve their safety level. They found that the personality types moderated the relationship between intention and actual use of the software. Conscientiousness had a medium sized moderating effect whereas agreeableness had a small/medium effect. The findings of the study suggest that personality may play a moderating role between intention and behaviour and may account for individual differences in why some motivated individuals go on to enact behaviours while others do not.

Jeske, Coventry, and Briggs (2013) looked at the role of impulse control in the context of nudging users into making better security decisions. By manipulating the presentation of wireless networks (such as the order and/or the colour (red, amber, green) of the Wi-Fi name), they explored if they could nudge users to click on secure WI-FI. They found that individuals who self-reported as IT novices and had diminished impulse control made poorer security decisions. They found that they were able to nudge individuals with poor impulse control. The

effect for individuals with high impulse control was relatively small as they make better security decisions without needing to be nudged.

2.2.5.5 | Internal Influences: Psychological Ownership

Psychological ownership is defined as a state in which individuals experience a possessive connection with targets they feel are "theirs" (Pierce, Kostova, & Dirks, 2003). These feelings of ownership can occur regardless of whether or not the individual legally owns the object, including objects used by employees that are the property of their organisation (Pierce et al., 2003). These targets can be physical items such as work computers and non-physical targets such as ideas and creative works. Higher levels of psychological ownership towards a target can lead to increased feelings of responsibility towards it, leading to enhanced protective strategies (Dipboye, 1977; Korman, 1970). In the context of work, if employees perceive that they own the data they create and/or their work computer they may engage in more security behaviours to protect it. Previously the notion of psychological ownership and computer security has only been studied in home users (Anderson & Agarwal, 2010). They found that psychological ownership of one's computer was significantly related to intention to perform security-related behaviour, indicating that individuals who feel that their devices belong to them are more protective of them. Research has also shown psychological ownership to be important for driving technology uptake behaviour in the workplace (Paré, Sicotte, & Jacques, 2006). Feelings of ownership towards devices and data in the workplace may increase the likelihood of protective strategies to maintain their integrity, availability and confidentiality. Further research is required to explore its potential role in employee security behaviour.

2.2.6 | ENVIRONMENTAL INFLUENCES

2.2.6.1 | Environmental Influences: Social Influences

Employees are influenced by their immediate work environment and the individuals within this environment. Employees' perceived social influences are *the extent to which an individual's* behaviour is influenced by what relevant others (e.g. colleagues, management, subordinates) expect him/her to do and the extent to which the employee believes others are performing the behaviour. If an individual believes that relevant others are following security actions or perceive that others expect them to follow the actions, they are more likely to undertake the security actions.

The role of social influences on behaviour is emphasised in some behaviour change theories. The TPB argues that beliefs in whether peers and people of importance to the person think they should engage in the desired behaviour influences the degree to which the individual will perform the behaviour. Social learning theory posits that normative beliefs increase intention to perform behaviour. As discussed earlier, the role of others is important for building self-efficacy

through vicarious experience and verbal persuasion of others. We learn through observation of others which is demonstrated in Bandura's well known BoBo Doll study (Bandura, Ross, & Ross, 1961). In security, if management and colleagues think security behaviours are necessary (normative beliefs) and perform them (descriptive norms); the employee is more likely to perform the desired behaviour. Employees may learn through vicarious experience by observing other employees or management engaging in security actions which also enhances their levels of self-efficacy and their perceptions of social pressure norms. The influence of social norms is also likely to be mediated by the extent to which the employee identifies with the company (e.g. Hogg & Terry, 2000). Social influence in the work environment is, therefore, an important determinant of encouraging security behaviours but may also provide an understanding of how norms may influence insecure practice.

Research has used a number of different constructs to explore the role of social pressures on security behaviour. Some research focusses on the role of normative beliefs (Bulgurcu et al., 2010; Herath & Rao, 2009a, 2009b; Pahnila et al., 2007; Siponen et al., 2010; Sommestad et al., 2015) or subjective norms (Ifinedo, 2011, 2014), both of which focus on the individuals perception of what they think important people (e.g. management) expect of them. Whilst other research focuses on descriptive norms/peer behaviour which is the perception of the actual behaviour of others such as fellow employees (Herath & Rao, 2009a, 2009b). The research base consistently supports the role of these different components of social influences on IS compliance intention in the workplace with the exception of a few studies. For example, subjective norms were not found to relate to policy compliance (Zhang et al., 2009) and intentions to engage in anti-spyware behaviours (Dinev & Hu, 2007). Research exploring consumer behaviour has also supported the role of subjective norms in intention to adopt anti-spyware software (Lee & Kozar, 2008) and updating anti-virus software, backing up data and using firewalls (Ng & Rahim, 2005).

Social influences, therefore, appear to be an important determinant of security behaviour.

2.2.6.2 | Environmental Influences: Organisational Culture

There are many different perspectives and definitions of organisational culture, however, it can be regarded as the shared beliefs, norms, values and learned ways that have developed through the organisation's history (Brown, 1998) and is often referred to as *"the way we do things around here"* (Schein, 1985). Organisational culture is an important determinant of the effectiveness of an organisation, influencing the practice and performance of the organisation and its employees.

There are many different theories and models of organisational culture; however the work of Schein (1985) has received lots of attention and provides a good basis for understanding the

complexity of organisational culture. Schein (1985) suggested that there are three levels of culture. The first is artefacts which are the visual representations of culture and include dress codes, rituals (e.g. meeting practices) and award ceremonies. These are observable to outsiders but not necessarily easily understood. Below these surface level artefacts are the espoused values of the organisation which include the goals, strategies and philosophies of the organisation. They are the values the organisations wish to be known for and are expressed in the mission statements of the organisation and advocated by the leaders of the organisation. Finally, there are the hidden basic assumptions about the organisation which reflect the shared values and are not necessarily visible to employees as they are so widely shared they are largely unaware of them. They are referred to as unwritten rules and exist largely at the unconscious level but they provide the best understanding of why things happen within an organisation. Schein used the iceberg metaphor to explain culture with artefacts and espoused values above the waterline, representing the observable values, behaviours, practices and discourse, and below the waterline are the influential unconscious values and behaviours.

Given the importance of an organisation's culture for influencing employees' behaviour, it is of particular significance to information security. An effective information security culture is one where security behaviours and security norms are embedded within the basic assumptions and values of the organisation. An organisation that values the integrity and confidentiality of information which is reflected in the philosophies of the organisation and advocated in the leadership and management will have a more effective security culture. Furthermore, if the basic assumptions within the organisation also reflect the values of information security, employees will be more likely to engage in security behaviours as they reflect the overall information security culture.

A number of research papers discuss the importance of developing an information security culture in organisations (such as Furnell & Thomson, 2009; Lacey, 2010; Thomson, von Solms, & Louw, 2006). In their review of literature exploring information security culture from 2000 to 2013, Karlsson, Astrom, and Karlsson (2015) found that the existing literature has largely focused on understanding what information security culture is, the roots/factors that contribute to information security culture and cultivating/changing security culture. They found no studies comparing security cultures and the potential differences on information security. They also found that a large body of the existing literature was descriptive or theoretical in nature and there were few papers on theory testing or studies looking at intervention. In particular, studies exploring the links between culture and information security relied heavily on survey methodology with a lack of other forms of research methods.

Despite the wealth of literature discussing information security culture, there are relatively few studies exploring the link between culture and end-users' security behaviour. These studies highlight a link between freedom to express opinions and try new ideas and security behaviour (Connolly, Lang, & Tygar, 2015). Other research has supported the role of top management support (D'Arcy & Greene, 2014; Knapp, Marshall, Rainer, & Ford, 2006), security-related communication (D'Arcy & Greene, 2014) and computer monitoring in the workplace (D'Arcy & Greene, 2014) for security culture.

Organisational climate is often explored in relation to organisational culture. Climate focusses on employee perceptions and evaluations of their work environment including policies, behaviour, practices and goal attainment in the workplace (James & James, 1989) and provides a context for understanding employees' attitudes and behaviour (Schneider, Bowen, Ehrhart, & Holcombe, 2000). It is often explored at the individual-level of psychological climate (Parker et al., 2003) and when aggregated or clustered to group-level is considered to be part of the organisational climate. Meta-analytic reviews such as Parker et al. (2003) have shown psychological climate to be associated with some organisational variables including work attitudes, motivation and performance in meta-analytic reviews. Climate differs from culture as it focuses on employees' perceptions of the work environment. Where culture is often referred to as *'the way things are done around here'*, climate is *'how it feels to work here'* and considers the experiences of working in the organisation.

Despite the lack of research exploring links between culture/climate and security behaviours in the workplace, the current literature indicates that support and commitment from top management (Chan, Woon, & Kankanhalli, 2005; D'Arcy & Greene, 2014; Goo, Yim, & Kim, 2013; Knapp et al., 2006), supervisor practices (Goo et al., 2013), security communication (D'Arcy & Greene, 2014; Goo et al., 2013), co-worker socialisation (Chan et al., 2005) and security enforcement/monitoring (D'Arcy & Greene, 2014; Goo et al., 2013) may be important at the individual-level for information security culture/climate within the workplace. However, this research is relatively in its infancy (Karlsson et al., 2015) and further research is required to explore its role in information security in more depth.

2.2.6.3 | Environmental Influences: Perceived Punishment and Detection

Within the workplace, employees' unacceptable behaviour can often be dealt via reprimands from management or other formal sanctioning procedures such as disciplinary action. Organisations' IS policies often dictate the consequences of non-compliance and as such, research has been dedicated to exploring whether fear of sanctions promotes policy compliance.

Research exploring whether the threat of sanctions deters misuse has mixed findings and has mainly been explored in the context of employees' intention to misuse computers or circumvent

security procedures. Some studies have focussed primarily on formal sanctions in the workplace. Formal sanctions refer to those which are outlined within the IS policy which may include disciplinary action or other official procedures for dealing with policy violations.

Some studies have supported formal sanction severity (Aurigemma & Mattson, 2014; Cheng et al., 2013; D'Arcy & Devaraj, 2012; Herath & Rao, 2009a, 2009b) whereas other research did not support its role in IS misuse or compliance intention (Johnston & Warkentin, 2015; Siponen & Vance, 2010).

Certainty of formal sanctions also has mixed findings. Herath and Rao (2009b) found it played a positive role in employees' IS policy compliance intention and Li et al., (2010) found the same for Internet policy compliance intention, however studies exploring its role in IS misuse have largely been unsupportive (Aurigemma & Mattson, 2014; Cheng et al., 2013; D'Arcy et al., 2008; Siponen & Vance, 2010). Recently, Cheng et al. (2014) did support its role in intentions to use the internet for personal usage.

Potential differences could be due to measurement of the IS misuse behaviour, the majority of those studies not supporting a relationship between perceived certainty have used scenarios and asked participants if they would intend to act in the same way as the character depicted (Cheng et al., 2013; D'Arcy et al., 2008; Siponen & Vance, 2010) and often create composite variables from multiple scenarios depicting different issues that may mask potential effects. Those studies supporting the role of perceived certainty on IS policy compliance intention (Herath & Rao, 2009a, 2009b) and intentions to use the internet for non-worked related purposes (Cheng et al., 2014) have used broad items to measure this motivation. Studies adopting scenarios depict specific IS misuse behaviours (e.g. modifying data without authorisation) whereas those using intention items focus on broad and less specific security/misuse behaviours. This may, therefore, account for the disparate findings as detection certainty may differ depending on the specific insecure behaviour. For example, people may have a higher detection certainty if they modified data on a system (as the modification may get recorded) than if they shared their password with a colleague. Subtle differences in detection certainty in relation to specific IS misuses have not been explored in literature to date but rather those studies using broad measures may suffer from abstraction difficulties. Further highlighting the need for specifcity in IS behavioural research.

In their review of GDT, D'Arcy and Herath (2011) argue that compliance and IS misuse may not be two sides of the same coin and that there may be different antecedents for both types of behaviour as one is positive and desirable while the other is negative and undesirable. This may be particularly important for perceived certainty as literature using a compliance approach (e.g.

(e.g. Herath & Rao, 2009a, 2009b) has supported its role whereas those studies looking at IS misuse have not supported its role.

Other research has explored the role of informal sanctions which refer to sanctions that are not covered explicitly in the IS policy such as disapproval of colleagues/peers but may occur as a result of an employee's insecure behaviour. Siponen and Vance (2010) found that certainty and severity perceptions of informal sanctions (e.g. loss of respect, jeopardised promotion prospects) did not significantly predict intentions to perform information security policy violations. D'Arcy and Devaraj (2012) also found informal (social desirability pressure and moral beliefs) sanctions to directly and indirectly influence individuals' intentions to misuse technology. However, Li et al. (2010) explored informal sanctions in the context of subjective norms and found that it did not significantly relate to compliance intention to internet use policy.

Johnston and Warkentin (2015) argue that existing research does not distinguish between formal and informal sanctions. When exploring these separately, they found that informal sanction severity and certainty were found to be significant determinants of compliance intention with protective strategies whereas formal sanction severity and certainty were non-significant. The authors suggest that the potential to lose the regard of colleagues (informal sanction) is a more significant motivator to engage in security behaviours as informal sanctions are less discrete compared to formal sanctions.

As little research has explored the role of informal sanctions, there is less support for its potential role in deterring IS misuse. For formal sanctions, there is a wealth of research exploring sanction severity and detection certainty, with literature suggesting that employee' perceptions of sanction severity are more effective in deterring misuse than their perceptions of the likelihood of getting caught. This suggests that detection mechanisms such as computer monitoring only work if backed with severe sanctions.

A major assumption of studies adopting the deterrence approach is that employees are aware of formal sanctioning procedures outlined within IS policies or that they are aware that their behaviour is illicit in the eyes of the policy compliance approach. There appears to be a lack of studies addressing whether employees are aware of the sanctions of insecure behaviour.

2.2.6.4 | Environmental Influences: Rewards/Incentives

The role of rewards and incentives for influencing behaviour stems from early work on behaviourism. Skinner's work on operant conditioning showed that people's behaviour could be shaped through positive reinforcement, where a desirable stimulus is presented as a consequence of an individual enacting a behaviour (Skinner, 1938). The importance of rewards

for behaviour and motivation is part of other well-known theories including social cognitive theory (Bandura, 1997), and self-determination theory (Deci & Ryan, 1985).

Organisational reward systems are often in place within organisations; such as performance-related pay and bonuses. Rewards can be tangible and include money or material goods such as prizes whereas intangible rewards include praise, recognition and achievements. They are largely explored in relation to employees' intrinsic motivation and job performance. Meta-analyses on incentives in the workplace have found them to have moderate effects on employee job performance (Condly, Clark, & Stolovitch, 2003). However, their influence on motivation is less clear (Pierce & Cameron, 2003) particularly those relating to performance-contingent rewards.

Deci, Koestner, and Ryan's (1999) meta-analytic review found performance-contingent tangible rewards led to decreases in individuals' intrinsic motivation but positive feedback or intangible rewards resulted in enhanced motivation. Other research has found that tangible rewards can be useful for intrinsic motivation when the rewards meet progressively demanding (but attainable) standards rather than a constant required task performance (Pierce & Cameron, 2003). A recent meta-analysis by Cerasoli, Nicklin, and Ford (2014) indicated that rewards are a better predictor of the quantity of performance whereas intrinsic motivation is a better predictor of quality of job performance. They conclude that they are not necessarily antagonistic and that motivation and incentives are best considered simultaneously.

The role of incentives or rewards for security-related performance is understudied. Security is often seen as a secondary task in job performance (Beautement et al., 2009) so behaviours are unlikely to be covered within an employee's performance-contingent rewards. The limited research has been unsupportive of their role. Posey, Roberts, and Lowry (2011) found that tangible rewards such as financial incentives were a weak source of employees' motivation to protect information security but intangible rewards such as management support were a strong source. Siponen et al. (2014) also found rewards of compliance did not significantly relate to compliance intention. Bulgurcu, Cavusoglu, and Benbasat (2009) found that rewards (combination of tangible and intangible) were only important for compliance in employees with a longer organisational tenure. The literature suggests that intangible rewards may be important for driving security behaviour. However, the influence of tangible or intangible rewards on employees' performance needs further investigation.

Rewards have mainly been studied in relation to perceived maladaptive rewards, i.e. the benefits of engaging in risk-taking behaviour such as the rewards of writing down passwords are a reduction in cognitive demand and saving time. PMT posits that rewards decrease the likelihood of an adaptive response but increase maladaptive coping. Rewards are often understudied in

PMT research as there is a lack of conceptual difference between rewards for maladaptive behaviour and the response costs for the adaptive behaviour (Abraham & Sheeran, 1994). Research exploring the rewards of maladaptive behaviour has found that intangible rewards (e.g. saving work time) significantly negatively affected compliance intention (Vance et al., 2012). Posey, Roberts, and Lowry (2011) looked at both tangible and intangible maladaptive rewards and found that intangible (e.g. personal gratification and satisfaction) rewards negatively affected motivation to protect information assets. They found that tangible maladaptive rewards had no relationship to motivation. The research suggests that intrinsic rewards from engaging in maladaptive risk-taking behaviour negatively influence engagement in security behaviour.

2.2.6.5 | Environmental influences: Positive Organisational Behaviour

2.2.6.5.1 | Organisational Commitment

Organisational commitment is an *employee's identification with and/or loyalty towards an* organisation (Morrow, 1993). It can be considered to be the degree to which they have a positive relationship with their organisation and is a stable indicator of employees' intentions to remain in a job (Mowday, Porter, & Steers, 1982). Organisational commitment has been differentiated into three forms that reflect different psychological states (Meyer & Allen, 1991). Affective commitment refers to the emotional attachment employees feels towards their organisation; continuance commitment when employees evaluate the costs and gains associated with leaving the organisation and normative commitment which refers to moral obligations employees may have towards their organisation. Of the three forms, affective commitment has been shown to significantly relate to performance, attendance and organisational citizenship behaviour (Meyer, Stanley, Herscovitch, & Topolnytsky, 2002). As organisational commitment is a positive form of organisational behaviour and has positive links towards occupational performance, individuals with greater commitment may be more likely to engage in security actions.

The relationship between commitment and security has been relatively understudied. High organisational commitment has been found to relate to greater security behaviour and less engagement in counterproductive behaviours (Stanton, Stam, Guzman, & Caledra, 2003), abiding to acceptable use policies and discussing these policies with colleagues (Stanton & Mastrangelo, 2004) and intending to comply with IS policies (Herath & Rao, 2009b). These studies suggest that commitment may play some role in security, particularly for appropriate and acceptable use of IS systems. However, the research is relatively in its infancy and its links to security behaviours merit further investigation.

2.2.6.5.2 | Organisational Citizenship Behaviour

Organisational citizenship behaviours (OCB) are positive organisational behaviours defined as *'discretionary contributions that go beyond the* strict job description and that do not lay claim to contractual *recompense from the formal reward system'* (Organ, 1988). They go beyond an individual's job performance and relate to behaviours that contribute to the optimal functioning of the organisation. These individuals "go above and beyond" the minimum requirements of their job role and as such, organisations benefit from increased productivity, efficiency and customer satisfaction when employees engage in OCB (Podsakoff, Whiting, Podsakoff, & Blume, 2009).

Williams and Anderson (1991) distinguish between two forms of OCB. The first is organisational citizenship behaviour towards individuals (OCB-I) which are behaviours targeted at fellow employees within the workplace. The second is organisational citizenship behaviours towards the organisation (OCB-O), those which directly benefit the organisation. The importance of OCB has been demonstrated in occupational psychology literature and has been found to have many positive consequences for organisations such as higher unit sales (Podsakoff & MacKenzie, 1997) and increased job performance (MacKenzie, Podsakoff, & Ahearne, 1998). The role of OCB in the security context has remained unexplored. However, it would be expected that individuals who engage in discretionary behaviours may contribute to, and engage in more security-related actions. Further research on the role of OCB in information security is required.

2.2.6.6 | Environmental Influences: Design and usability of security

 "When security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security" (Norman, 2009)

The design and usability of security systems is a necessary pre-exquisite for ensuring that users can perform security tasks. When systems are unusable, users will circumvent the process or find workarounds to the system to perform their job (Adams & Sasse, 1999), or adopt less secure practices that are more usable.

Whitten and Tygar (1999) define usable security as a set of priorities in which the expected user is; *"(1) reliably made aware of the security tasks they need to perform; (2) are able to figure out how to successfully perform those tasks; (3) don't make dangerous errors; and (4) are* sufficiently comfortable with the interface to continue using i*t."* (p. 2).

Early work by Whitten and Tygar (1999) on the issues surrounding usability and security mechanisms are still of importance today. Their paper *"Why Johnny Can't Encrypt"* highlighted important issues on the state of play of security software design and usability for consumers.

They argued that design standards for consumer software are not sufficient for security which they demonstrated through a user study of email encryption. Since their early work, there has been increased interest in usable security from researchers and practitioners, and a body of work has been dedicated to designing solutions so that they are more usable, particularly in authentication research.

Therefore, the design of security is important in driving appropriate and correct security behaviour in users. However, in isolation, usable security is not enough to fully understand the complexities surrounding poor security behaviour as despite usable security, users still behave insecurely. Initially, studies of usability and anti-spyware found a link between usability and perceived behavioural control but not of their intention to use it (Dinev & Hu, 2007; Lee & Kozar, 2008), and at best it may play an indirect role via attitude (Kumar et al., 2008).

More recently, support has been found for role of perceived ease of use and perceived usefulness on intentions to adopt an email authentication service (Herath et al., 2014) and security software (Shropshire et al., 2015).

Perceived usefulness and perceived ease of use appear to be important for protective actions that involve software usage. However, contradictory evidence is found in the small amount of research exploring their role on attitudinal and motivational components of security software usage.

2.2.6.7 | Environmental Influences: Persuasion and Deception

The role of persuasion in influencing individuals into engaging in insecure behaviour is best understood in connection with the success of social engineering. Social engineering is particularly problematic for organisations and is considered a major security threat (Mitnick & Simon, 2003). Social engineering techniques rely on human interaction and involve non-technical methods of intrusion from attackers. They adopt social persuasion techniques to target the human element in security (Applegate, 2009).

There are many social engineering methods used to try and trick individuals. These include tailgating, baiting, pretexting and phishing to name a few. Phishing emails are one of the most common forms of cyber social engineering as attackers can cheaply and easily distribute millions of emails but require a very small return to achieve substantial benefits. To understand the success of social engineering tactics, it is necessary to explore how people are persuaded and deceived into behaving insecurely.

One of the most prominent theories of persuasion is the elaboration likelihood model (ELM; Petty & Cacioppo, 1986) that posits that individuals' attitudes can be changed through persuasive communication, and is of particular relevance to phishing emails. When presented

with persuasive information, individuals engage in some level of elaboration. According to ELM, there are two routes to persuasion: the central route and the peripheral route which are moderated by the ability and motivation of the individual (Petty & Cacioppo, 1986). The central route involves greater elaboration and cognitive effort than the peripheral route and often involves extensive thinking and diligence. When receiving a phishing email, those who process it using the central route may carefully examine the information in the message (e.g. the perceived legitimacy of message content), scrutinise the email (e.g. examine the authenticity of links and the sender email) and consider other heuristics that could indicate a phishing email. When individuals do not elaborate on information, they will go down a peripheral route in which they rely on simple heuristics such as the communicator credibility or message content. As such, individuals' peripheral route may be fooled by the email content (e.g. a false urgency or a promise of reward) and the false representation of legitimate companies (e.g. logos of mimicked companies). The peripheral route relies on mental shortcuts, not requiring actively thinking about the information and as such, relies on superficial factors. The two routes are not mutually exclusive and are often used in combination. However, individuals who largely use a peripheral route when using email are more likely to be phished as they do not engage in necessary relevant thinking (e.g. phishing detection). On the opposite side of this, an extremely persuasive phishing email could engage central route processing but still lead individuals to act on the email.

Message credibility plays an important role in the peripheral route to impact persuasion (Petty & Cacioppo, 1986). Attackers impersonate large organisations that users will know; through impersonation they are relying on the credibility and reputation of the company to persuade the user. Furthermore, the use of a business logo, signatory and copyright may enhance the credibility of the message (Wang, Chen, Herath, & Rao, 2009). As research has found that personalization/spear-phishing emails also leads users to click on links (Halevi et al., 2015; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Rocha Flores, Holm, Svensson, & Ericsson, 2014) and more so than emails which are not personalized (Rocha Flores et al., 2014), the presence of personalisation, therefore, enhances the perceived credibility of the message. Other research has found that the sender's email address influences trust in the email (Dhamija, Tygar, & Hearst, 2006; Karakasiliotis, Furnell, & Papadaki, 2006; Kumaraguru, Acquisti, & Cranor, 2006; Vishwanath, Herath, Chen, Wang, & Rao, 2011), which is problematic as they can be easily spoofed. Wang et al. (2009) argue that an authentic looking sender email address is one of the features of assessing information credibility in emails. Perceived credibility will, therefore, determine the persuasiveness of a phishing email.

A second important contribution to research on social engineering is theories of deception. One of the prominent theories is the interpersonal deception theory (Buller & Burgoon, 1996),

however Wang, Herath, Chen, Vishwanath, and Rao (2012) argue that it focuses on face-to-face communications so its applicability to phishing is limited and relies on many channels of communications (including body language and speech patterns). They use the Theory of Deception (Johnson, Grazioli, Jamal, & Zualkernan, 1992) as it is more appropriate for less-interactive and non-face-to-face communications such as email phishing, and focuses less on the interplay between deceivers and targets, but provides more consideration on the level of the individual in the cognitive processing of deceptive information (Grazioli, 2004).

The theory focuses on the information processing involved in deceiving and detecting deception. When receiving an email, individuals first compare assurance and trust cues (e.g. email phishing heuristics) with their expectations about these cues and when there is an inconsistency between the observed cues and what is expected, activation raises suspicion and directs attention to the cues. Individuals then use their domain-specific knowledge (e.g. evaluating multiple phishing heuristics) to assess the genuineness of the cues. Individuals then form an overall deception assessment resulting from one strong assessment (e.g. the link in the email is clearly illegitimate) or the result of several weaker ones combined (e.g. the sender email does not match the address, the attachment is a zip archive and the content is creating a sense of urgency). An individual's competence at identifying deception cues is indicative of better detection performance (Grazioli, 2004) so individuals with greater knowledge of what to look for in phishing emails are better at detection.

Vishwanath, Herath, Chen, Wang, and Rao (2011) found that when individuals receive a relevant email (e.g. from a service provider they use), they will focus disproportionality on emotional triggers (e.g. urgency cues) and will ignore deception indicators (e.g. the source, and grammar and spelling elements within emails), which will increase susceptibility. Focusing on these latter elements will not lead to elaboration whereas focusing on urgency cues does influence elaboration as it garners greater information processing resources from the user, triggering elaboration and reducing susceptibility. Individuals who do not enter elaboration may, therefore, be more likely respond to the email. Further research by Wang et al. (2012) found that those with greater scam knowledge paid more attention to deception indicators and consequently have a lower chance of getting phished. Individuals with greater knowledge pay less attention to emotional triggers and rely more on deception indicators, suggesting that knowledge and ability play an important role in determining how individuals react to persuasion and deceptive messages. This is supported by other research that has found that individuals with greater knowledge and experience with social engineering threats are less likely to fall for phishing emails (Downs, Holbrook, & Cranor, 2007; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

2.2.7 | SUMMARY OF FACTORS INFLUENCING SECURITY BEHAVIOUR

Overall, research suggests that users' security behaviour is influenced by a range of factors that are both internal and external to the individual.

The literature included research from consumers' behaviour to understand further what may motive security behaviour. However, employees' behaviour is more complex within the workplace setting as it is influenced by their organisation and working environment. Despite the wealth of studies that explore the factors that influence employees' intentions to comply with their organisation's IS policy, there are only a few studies in which the determinants of the individual security behaviours within the policy are explored (Ng et al., 2009; Workman et al., 2008). There is, therefore, a need to explore the research gap to identify determinants of specific security behaviours in an employment sample rather than continued use of globalised indicators of employees' security behaviour.

Additionally, while the existing research has provided a promising baseline for understanding security behaviour in the workplace it is unclear which factors (e.g. internal and environmental) are most important for security at work and whether the organisational context plays a role in determining these factors. The existing literature has largely focussed on the factors for the prediction of attitudes, intentions or behaviours. However, more understanding is needed for what may influence these factors within the workplace and how they may interplay in determining levels of different security behaviours.

2.3 | BEHAVIOUR CHANGE

Section 2.1 explored literature addressing the influencers of secure and insecure behaviour. As discussed, many of these studies have adopted behavioural models that focus on behaviour at the individual level such as PMT, TPB, HBM and SCT. There has, however, been less use of these theories for driving security behaviour change. The question is, what predictors to target in an intervention? (Conner, 2014). For instance, if self-efficacy consistently predicts security behaviour, interventions and systems can be designed to best maximise users levels of self-efficacy.

Despite investigating factors that influence behaviour, research has been limited in using the findings in behaviour change interventions. They have been primarily dedicated to understanding the causes of security behaviour, which is important, but leaves a gap of where this knowledge has been used to actually change security behaviour. There are many approaches to behaviour change which include focussing on the behaviour as an agent of change (e.g. Diffusion of innovations; Rogers, 2010), integrated research-driven frameworks (e.g. behaviour change wheel; Michie, van Stralen, & West, 2011) or combining knowledge from behavioural economics and psychology (e.g. MINDSPACE; Dolan, Hallsworth, Halpern, King, & Vlaev, 2010). However, as this thesis is interested in intervening at the individual level, it is important to consider the body of work on behaviour change processes for intervening at this level. Consequently, other behaviour change approaches will not be discussed in-depth.

2.3.1 | MOTIVATIONAL AND VOLITIONAL APPROACHES

PMT, TPB, and HBM as discussed in section 2.2.1 are examples of motivational theories that place behaviour change on a continuum and view intention as the best predictor of subsequent behaviour and that levels of the determinants of intention give rise to high or low engagement in the desired behaviour. However, research exploring the link between intention and behaviour indicates that intentions are insufficient in predicting actual behaviour, accounting for 1/3 of the variance in actual behaviour – an issue referred to as the "intention-behaviour gap" (Sheeran, 2002).

Motivational theories may only explain the first part of behaviour change (motivating people to intend to change), with more attention needed on the second part (aiding intenders into behaviour change). Motivational approaches do not explain how intentions are translated into action and are not sufficient in creating large changes in behaviour (Webb & Sheeran, 2006). The lack of translation into actual behaviour is because while many people may intend to act; they may fail to follow through with their intentions. Therefore, in isolation, a motivational intervention may not lead to desired and sustained behaviour change (Hagger et al., 2002). Attention has therefore been drawn to understanding the volitional processes involved in

enacting and maintaining behaviour and bridging the intention-behaviour gap. For example, one of the reasons people fail to enact behaviour is due to poor self-regulation strategies, and one such strategy is planning (Abraham, Sheeran, & Johnston, 1998).

Theories which consider the volitional processes in translating intentions into actions are "stage-based" in which movement through a stage is influenced by different variables (Weinstein, 1988). These models have moved away from the limitations of other social cognition models as they do not focus solely on intentions as the most proximate predictor of behaviour but consider the transition from motivation to actual behaviour engagement.

One of the most commonly used is the transtheoretical model (TTM; Prochaska & DiClemnte, 1983). The model is distinguished by six mutually exclusive stages that posit change as a process that unfolds rather than as a discrete event. Individuals progress through each stage, although relapse and multiple attempts are recognised. Individuals are categorised into one of six stages:

1. Pre-contemplation is where people do not intend to take action in the near term and may be unaware that their current behaviour is problematic.
2. Contemplation is where people intend to change their behaviours in the short term and are beginning to assess the costs and benefits of their continued behaviour.
3. Preparation is where people intend to take action soon, have a plan of action and are beginning to take small steps towards behaviour change.
4. Action is where people have made modifications to their behaviour but as action is often equated with behaviour change, individuals must maintain the behaviour.
5. Maintenance is where the person has been able to sustain the behaviour and is working towards preventing relapse.
6. Termination is where the individual has zero temptation to revert to the old behaviour.

The TTM also identifies ten processes of change and strategies which individuals use when progressing through stages (Prochaska, Velicer, DiClemnte, & Fava, 1988). The TTM is a dominant model in health psychology and has received significant empirical support (Sutton, 2001). However, its use in understanding security behaviour alongside other stage theories has remained relatively underexplored. The TTM will be used within the final intervention to assess participants' readiness to change their security behaviour.

The Health Action Process Approach (HAPA; Schwarzer, 1992), Rubicon Model of Action Phases (Heckhausen & Gollwitzer, 1987) and the Precaution Adoption Process Model (Weinstein & Sandman, 1992) are other examples of stage theories. They all differ in the number of stages proposed and what strategies help individuals transition through stages.

However, a central component of all these stage theories is that there are two main stages to behaviour change: a motivational stage and a volitional stage. The motivational stage contains the motivational elements of models such as the Theory of Planned Behaviour and Protection Motivation Theory, focussing on the determinants that led individuals to intend to enact the desired behaviour (such as enhancing threat and coping appraisal). Following the formation of an intention, individuals must then form a goal and consequently, a commitment to follow through with behaviour change. This is called the volitional stage and focusses on the initiation and maintenance of behaviour change through the use of self-regulatory processes such goal setting and planning.

2.3.2 | IMPLEMENTATION INTENTIONS

Implementation intentions are a volitional technique that has been used in behaviour change to help translate intentions into action. They are a planning technique to identify behaviours that will be performed in specific critical situations (Gollwitzer & Sheeran, 2006) and take the form of "if-*then"* statements; a type of action plan. The "IF" component is where the individual specifies the situational cues or critical situations that will prompt the behaviour (e.g. IF I leave my workstation…). The "THEN" component is the goal-directed response which is in line with the overall desired behavioural change (…THEN I will lock the work computer) and is to be cognitively associated with the situational cue. If-then statements allow a strong association between the situational cue and the specified response and are quite stable over time (Gollwitzer & Oettingen, 2011). Unlike goal intentions that specify desired future behaviour, the strength of implementation intentions lies in the specificity of the plan by detailing when, where and how the individual will perform the behaviour (Gollwitzer & Sheeran, 2006). The critical situation then becomes highly salient to the individual, reducing the likelihood of missed opportunities to enact the desired behaviour (Webb & Sheeran, 2004). Implementation intentions are a useful self-regulatory strategy for managing the critical situations that lead to undesired habitual responses. They can break down unwanted habits and promote new, wanted behaviours. When a person attempts to alter their existing behaviour, implementation intentions are useful to link the new behaviour with the situation that previously led to the habitual behaviour (Adriaanse, de Ridder, & de Wit, 2009; Gollwitzer & Sheeran, 2006). For example, an employee who knows they are unlikely to lock their computer when they leave their desk may use the following plan to help counteract that habitual response: "If I am tempted not to lock my computer, then I will remind myself it does not take long to log back in".

Implementation intentions have been shown to be effective in bridging the intention-behaviour gap for a variety of health-related behaviours (Hagger & Luszczynska, 2014). Meta-analyses of 94 studies have shown them to have a medium to large effect size (d=.65) for goal attainment (Gollwitzer & Sheeran, 2006). Whilst there is a plethora of research exploring and

demonstrating the impact of implementation intentions on behaviour change, they have largely been comprised of populations drawn from non-occupational groups, mainly students (e.g. Arden and Armitage; 2012; Milne et al., 2002) or the general public (e.g. Brewster, Elliott, & Kelly, 2015; De Vet, Oenema, Sheeran, & Brug, 2009), with less research exploring their applicability within the workplace setting. There is no research which has explored implementation intentions in the context of security behaviour in the workplace, however research has shown them to be effective for pro-environmental behaviour (Holland, Aarts, & Langendam, 2006), health and safety training attendance (Sheeran & Silverman, 2003) and anti-smoking behaviour in the workplace (Armitage, 2007).

As discussed, an intervention combining motivational components accompanied by volitional strategies will lead to greater behaviour change than the sole use of one of the behaviour change techniques. Combined interventions have shown to be effective in driving behaviour change (Chatzisarantis, Hagger, & Wang, 2010; Hagger, Lonsdale, & Chatzisarantis, 2012; Milne et al., 2002; Prestwich, Ayres, & Lawton, 2008)

A central aim of this thesis is to develop and evaluate an intervention to improve the security behaviour of employees based on behaviour change principles. The thesis seeks to adopt a stage-based approach to designing an intervention that combines motivational (using continuum theories) and volitional approaches (implementation intentions).

2.4 | RESEARCH EXPLORING BEHAVIOUR CHANGE FOR SECURITY

Changing users' security behaviour and decisions has been largely understudied. The majority of attempts have focussed on designing better systems and software so that they are more usable. While usable systems are essential for reducing the burden to users, the previous section has shown that there are a number of influencers of secure and insecure behaviours that are independent of software/system design. This section of the literature review focuses on research that has attempted to influence users' security behaviour - both in consumers and within the workplace rather than literature focussing solely on usable security. In particular, it will concentrate on the growing body of literature utilising psychological knowledge to motivate users to behave more securely and those that target the processes underlying and regulating security behaviour.

Despite efforts to understand the security behaviour of employees, there has been little attention dedicated to improving this behaviour. The security domain is inundated with papers and reports highlighting the importance of awareness campaigns and information security training in the workplace and survey literature has positioned this approach to improve motivation but not actual behaviour. There is a large research gap between experimental studies that address the effectiveness of interventions and approaches to improving actual security behaviour.

Taking a policy-compliance approach, methods in the workplace have largely focussed on training, education, and awareness campaigns to improve compliance with the companies' IS policy. These approaches have taken a number of different forms including presentations, newsletters, video games, and posters. Topics covered in training and awareness programs can include social engineering, password security, security on the internet, phishing emails and clear screen policy (Bauer, Bernroider, & Chudzikowski, 2013) along with other topics and behaviours that may be covered in the companies' IS policies.

Information security training has been considered to be different from other forms of training as it relies on persuasion (Karjalainen & Siponen, 2011) and not merely education; it is designed to influence behaviours and persuade employees to take a particular course of action rather than purely focusing on awareness building and skill acquisition. For effective behaviour change in the workplace, training and awareness campaigns need to be theoretically-grounded to be effective. Unfortunately, reviews have indicated that this is largely not the case in existing approaches for IS security training. For example, Puhakainen and Siponen (2010) reviewed the existing literature on IS security training and concluded that previous approaches have been largely non-theoretical and anecdotal, with the majority of approaches lacking empirical evidence and a theoretical grounding. For interventions to be effective and of high quality, they must be based on theory so that they can provide an explanation of how and why they work.

Similarly, approaches also need to provide empirical evidence of their efficiency so that they can demonstrate whether their approach works in practice. Puhakainen and Siponen (2010) argue that training approaches within the IS domain often take a pedagogical approach to improving employee compliance and of the 23 studies reviewed in their study, only 4 were found to have a theoretical underpinning and only 2 of these provided empirical evidence.

To overcome the previous issues in IS training approaches, Puhakainen and Siponen (2010) developed a training program using persuasive communication to increase e-mail encryption. They found that persuasive communication can successfully improve policy compliance behaviour of employees. Furthermore, they suggest that IS training should use methods that enable learners' systematic cognitive processing of information and should adopt learning tasks that are of personal relevance to the learners. This study is one of the few that have a theory-based grounding and provides empirical evidence demonstrating the utility of adopting theory-based IS training.

Training approaches to behaviour change may be more appropriate for security behaviours that require a level of skill such as detecting phishing emails. The training aims to equip individuals with necessary skills to undertake security actions. However, not all security behaviours are skill-based so the appropriateness of training for specific security behaviours needs consideration.

Reducing susceptibility to phishing emails is an area of research where training has been shown to be effective. Kumaraguru et al. (2009) conducted a real-world evaluation of "PhishGuru", an email embedded training system that trains users with strategies to avoid falling for phishing emails. The system works by sending simulated spear-phishing emails to users. Those who fall for phishing emails are then presented training in the form of comics. By being embedded in the phishing email, it provides a highly salient training system that is linked to the individual's current insecure behaviour. They found that the training led to retained knowledge after 28 days and additional training messages resulted in decreases in disclosing information to phishing attempts. However, participants could be more cautious simply because they feel they are being monitored by their organisations as research has shown that perceived monitoring influences security behaviour (D'Arcy & Greene, 2014). Other approaches adopting embedded training in simulated phishing emails have been found to be somewhat effective but only a small percentage of victims (12.65%) go on to take part in the training (Jansson & von Solms, 2011).

Training and awareness promotion in isolation is not sufficient for behaviour change. A wealth of research indicates that users and employees do not behave securely despite having the necessary knowledge and skills. Recent research has shown that there is no difference in the security behaviour of experts and non-experts despite experts having better mental models of

the internet (Kang et al., 2015). This suggests that knowledge in isolation cannot explain secure/insecure behaviour. Other research has shown that despite taking part in training, users still behave insecurely. Kearney and Kruger (2013) found 69% of those users who disclosed their passwords in their phishing study had completed the security training in the past. Approaches that combine training alongside behaviour change principles may lead to actual and sustained behaviour change for security.

The following sections of this literature review have been broken down into recurring approaches that have been investigated to promote security behaviour. These are self-efficacy manipulations, fear appeals, serious games, message framing and persuasive communication.

2.4.1 | SELF-EFFICACY MANIPULATIONS

Within the existing research that has utilised training or educational approaches to improve end-user security behaviour by using principles of enactive mastery through directly training the user and then requiring them to practice the behaviour. However, there are few studies which discuss the theoretical underpinnings in relation to self-efficacy.

Wirth, Rifon, LaRose, and Lewis (2007) designed an intervention based on PMT to increase self-efficacy and protective online safety behaviours with 547 high school students through enactive mastery. The interactive programme covered safety issues focusing on potentially dangerous encounters through emails, social networks, surfing and financial transactions. They were provided with the option of "show me how" to train them how to protect themselves against a particular issue. They found that those exposed to the enactive mastery intervention had higher levels of self-efficacy compared to those who were not exposed. However, there was no main effect of the self-efficacy intervention on intentions to engage in protective behaviour except for intentions to use privacy settings in browsers. Overall, the intervention increased levels of self-efficacy and had some influence on students' motivation to adopt protective behaviours.

Shillair et al. (2015) used PMT to enhance security behaviours of internet users. They were interested in the role of personal responsibility for security. They believed that people who have a higher sense of personal responsibility for security are more likely to undertake security behaviours. Individuals with high self-efficacy view security as their responsibility whereas those with low self-efficacy may diffuse responsibility onto other sources (such as their IS policy). They were interested in whether manipulating responsibility perception alongside enactive mastery training would lead to greater intentions to engage in the security behaviours compared to using persuasive threat messages (providing simple suggestions that they could cope with the security threat). They found that those exposed to the vicarious experience treatment had significantly higher coping self-efficacy than those within the persuasion

57

condition. It had no direct effect on intentions in isolation but when combined with the responsibility manipulation it improved intentions.

Boehmer, LaRose, Rifon, Alhabash, & Cotten (2015) also looked at experimentally manipulating personal responsibility to increase protective behaviours (reading privacy policies, changing passwords, changing browser privacy settings, reading licencing agreements for software, changing IM settings, backing up files and verifying the identity of websites). They did not manipulate self-efficacy but looked at the influence of existing levels on the effects of the responsibility manipulation. Like the Shillair et al. (2015) study, participants were exposed to a responsibility manipulation; in which they were either persuaded that online security is their personal responsibility or is shared responsibility. They were interested in the effects of this manipulation on intentions and also the potential role that existing levels of self-efficacy and safety involvement may play.

They found that framing the message towards personal responsibility led to increases in intentions to engage in security behaviours. The effect was greatest for individuals with high existing levels of online safety involvement and high self-efficacy, and that high involvement users exhibited greater protective behaviours. The manipulation did not work for individuals with low self-efficacy and low involvement: the authors position these as potentially the most vulnerable group. They found that they had lower security intentions when presented with a personal responsibility manipulation suggesting that they were discouraged from behaving securely. The findings suggest that this novice group may be easily discouraged when presented with security information that informs them to take responsibility for security online as they also lack self-efficacy to undertake the behaviours. The findings indicate the need to tailor interventions to participants existing self-efficacy perceptions as there is potential for negative effects.

2.4.2 | FEAR APPEALS

"Fear appeals are persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" (Witte, 1992, p. 329). Fear appeals traditionally target aspects of individuals' threat appraisals by using statements of the severity of threats and their potential susceptibility to the threat. The appeals may also target coping appraisal with statements of response efficacy and self-efficacy. Witte and Allen's (2000) meta-analysis of fear appeal literature found that fear appeals produce moderate effects for fear arousal and large effects for perceived severity and susceptibility. They also found that the stronger the fear appeal, the greater effect it had on attitude, intentions and behaviour change.

Johnston and Warkentin (2010) looked at fear appeals and adoption of anti-spyware. The fear appeal sought to target the severity (e.g. potential to affect computer performance) and susceptibility (e.g. providing likelihood statistics) of the security threat and statements about coping with threat and the efficacious of such coping approaches. They found that following exposure to the fear appeal, there was a significant increase in severity, susceptibility, self-efficacy and response efficacy for those exposed to the fear appeal.

Recent work by Johnston and Warkentin (2015) compared three fear appeals covering password theft, data theft from not logging out and USB theft within multiple government organisations and their effect on changing passwords, logging out and USB protective behaviour. They argue that existing fear appeals focus on threats to information, data and systems and these lack relevance to the individual and this is often the conventional approach in IS fear appeals. They add sanctioning rhetoric to account for the threats to the human asset as they posit that threats to non-human assets (e.g. data) lack robustness to the user since they lack descriptions of threats of a personal nature. They explore this personal relevance in the context of sanctions, which they argue directly affects the individual and thus can enhance the personal relevance of threat appeals ("enhanced fear appeals elements"). They found that there was a significant difference for all PMT constructs (severity, susceptibility, self-efficacy, response efficacy) and additional constructs for sanction rhetoric (formal/informal sanction severity, formal/informal sanction severity and sanction celerity) between those exposed to the fear appeal and a control group who experienced no fear appeal. They also found that there was a significant difference in compliance intention with those in the fear appeals groups, which significantly indicated greater intention to engage in protective security behaviour. The study does not report any inferential statistics comparing the three types of fear appeal to ascertain any potential differences in PMT constructs and intention.

Jenkins, Grimes, Proudfoot, and Lowry (2013) used just-in-time fear appeals to reduce password re-use. Their system detected when users were reusing an existing password (using keystroke dynamics when a user generates the passwords – e.g. a re-used password is routinely processed information so will have a faster typing flow than when creating a new password) and then presented them with the fear appeal. The fear appeal emphasised that re-using a password puts the user at risk of being hacked (perceived susceptibility). The mention of being hacked is to influence perceived severity of re-using a password. The fear appeal concluded by saying that to protect themselves, they must choose a unique password – influencing the response efficacy of the user. For the behaviour change manipulation, 88.41% of those who received the fear appeal created unique passwords compared to 4.45% of users in the control. The findings suggest that a just-in-time fear appeal was a useful approach to reduce insecure behaviour.

Vance, Eargle, Ouimet, and Straub (2013) explored static and interactive (visual password meter) fear appeals on selecting strong passwords which they compared to a control and a non-fear appeal password meter. They found that those exposed to an interactive fear appeal selected stronger passwords than those in the static fear appeal treatment, control and those who received a password meter. There were no differences between those receiving the static fear appeal or an interactive password meter compared to the control group. Their findings provide strong support for the addition of interactivity in fear appeals on enhancing their effectiveness.

Overall, the evidence for the use of fear appeals to influence security behaviours appears to be promising with studies demonstrating changes in PMT constructs (severity, susceptibility, self-efficacy, response efficacy; Johnston & Warkentin, 2010, 2015), changes in intentions and actual behaviour (Boss, Galletta, Lowry, Moody, & Polak, 2015; Jenkins et al., 2013; Vance et al., 2013) and recent findings showing that the addition of interactivity and just-in-time fear appeals can lead to better password behaviour (Jenkins et al., 2013; Vance et al., 2013).

2.4.3 | SERIOUS GAMES
Serious games may be useful for behaviour change as they provide entertainment to the user with the potential for changing user behaviour through learning and skill development.

A systematic literature review by Connolly, Boyle, MacArthur, Hainey, and Boyle (2012) exploring the empirical evidence of serious games in other domains have found mixed results. Some reoccurring outcomes were improved knowledge acquisition and affective and motivational outcomes. A few studies have looked at the effects of serious games behaviour change, which were varied in their methodologies and focus, but suggested that they may be useful to change behaviour.

Games have been used in the context of security with varying levels of success. Anti-phishing training has received much attention in research in an attempt to help users identify phishing heuristics at the email level. Anti-phishing Phil teaches users how to identify illegitimate URLs through four rounds that become increasingly difficult. Sheng and Magnien (2007) found that participants trained with anti-phishing Phil were better at identifying fraudulent websites than individuals who read an anti-phishing tutorial or read existing online training.

Game designs based on behaviour change are in their infancy, however, Davinson and Sillence (2010) used risk manipulations (targeted via heightening perceived susceptibility) based on the HBM alongside anti-phishing Phil to promote secure behaviour. Participants were randomly allocated to one of four conditions in which they were given training or no training and a low threat or high threat message. Those in the low threat condition were presented with an "at low" risk message, which stated they were 20% at risk of being a victim of fraud. Those in the high

threat condition were told they were at an 80% at risk of victimisation. Participants were led to believe that the risk message reflected their baseline scores, however, in reality they were randomly allocated to low or high-risk message regardless of their actual baseline security behaviour. They found that the use of anti-phishing Phil had no effect on secure behaviour at 1-week follow-up which could be due to the lack of tailored messages relating to their baseline behaviour as giving high threat messages to people who already behave securely may lead them to dismiss the threat and subsequently reduce their behaviour. Their measure of security behaviour was also quite broad and they did not discuss the effect on specific security behaviours that were measured (including the behaviour that was directly trained within the anti-phishing Phil paradigm i.e. identifying suspicious URLs). They also found no main effect of risk warning score between the two types. However, they found that it increased intentions to behave more securely regardless of the level risk of presented and that follow-up security behaviour was significantly higher than baseline. This suggested that users only need information generically regarding their susceptibility rather than seemingly tailored.

Other games have largely been training-based such as cyber-CIEGE (Irvine, Thompson, & Allen, 2005) in which the game player takes the role of a decision maker for a fictional organisation and they are required to make choices regarding procedural, technical and physical security.

Research has argued that serious games could be improved by utilising best practice from behaviour change literature (Blythe & Coventry, 2012). Furthermore, caution has been suggested for the potentially intrusive nature of these games and the logs of user behaviour that they collate and store (Blythe & Coventry, 2012).

2.4.4 | MESSAGE FRAMING AND PERSUASIVE COMMUNICATION

Research has also been dedicated to looking at the effects of message framing and persuasive communication on improving security behaviour.

Anderson and Agarwal (2010) looked at influencing undergraduate students' attitudes and descriptive norms towards performing security behaviour (a broad non-specific measure) through manipulation of goal-framing and self-view. They manipulated the message framing by presenting participants with either a positively focussed message that discussed the benefits of performing security behaviours or a negatively-focussed message that discussed the severity and probability of security threats.

They also manipulated a participant's self-view, which aimed to focus an individual's attention on themselves or others. This involved priming an individual towards an independent or interdependent view. For the independent view, they were primed to think of themselves as

distinct and separate from others (e.g. a conscientious cybercitizen). The inter-dependent view was that they were told to think of themselves as part of a larger group (e.g. a community of cybercitizens). By manipulating self-view, the aim was to influence levels of subjective and descriptive norms as the closer a referent group is perceived to be, the more salient norms are. Those primed with an inter-dependent should have reported higher subjective and descriptive norms than those primed with an independent self-view. They further posit that those given an interdependent view respond more to prevention-focused messages.

They found that there was no significant interaction of self-view and goal framing on attitudes towards protecting one's own computer or the Internet. However, its effects were approaching significance for their influence on subjective norms. Further analyses found that those primed with the independent self-view with a promotion focused message had significantly higher levels of subjective norms compared to those with the same self-view but a prevention-focused goal. There were no differences in subjective norm for those within the interdependent self-view for either goal frame.

The authors conclude that positively framed messages may be more persuasive in the context of security as existing approaches typically focus on loss aversion and prevention such as fear appeals. Furthermore, they posit that these positively-framed messages may have greater effectiveness in combination with an independent self-view manipulation. Additionally, they argue that attitudes may be harder to influence than an individual's subjective norms in the context of security.

Shropshire, Warkentin, and Johnston (2010) also explored message framing for technology uptake and found that negative message framing is more powerful in encouraging users to adopt detective technologies (e.g. biometric keyboard) than preventive technologies (e.g. adaptive email filter) in undergraduate students.

Unlike Anderson and Agarwal (2010) and Shropshire et al. (2010) who focus on influencing positive security behaviour, Barlow, Warkentin, Ormond, and Dennis (2013a) were interested in reducing employees' password sharing by discouraging neutralizations. These are employees' rationalisations of their insecure behaviour, for example, they may share their password with a colleague because they rationalise that it will allow them to get the job done quicker and no one is being harmed as a result of their actions. They found that the deterrence-focused and neutralization-focused communications both resulted in significantly lower violation intentions compared to scenarios where no focus was given. There was no significant difference between the two forms of communication suggesting they were equally effective. There was also no significant effect of the negative or positive framing of the scenarios on intentions compared to the no framing scenario suggesting that neither was more effective in reducing violation

intentions. The authors conclude that organisations should focus on neutralisation mitigation in their information security efforts in addition to communications focussing on deterrent sanctions as they are both equally effective in reducing neutralizations.

Shepherd, Mejias, and Klein (2014) conducted a longitudinal study in the workplace to investigate the effectiveness of persuasiveness communication on reducing internet abuse. Participants were presented with messages reminding them of the acceptable use policies (AUP) in their organisation. Based on deterrence theory, they were interested in comparing the effects of a mild AUP (reminding users that the systems are for business use only) and a severe AUP (emphasising sanctions for non-compliance). They used employees' data by logging their website usage. They found that when using a mild AUP message that non-work internet traffic decreased from 55% to 43% whereas the severe AUP message decreased from 72% to 39%. At 2-week follow-up, non-work traffic had increased but was still lower than pre-treatment levels for the severe AUP but for the mild message, it had increased to levels of that at pre-treatment. The findings suggested that the more severe AUP was better at reducing internet abuse and had better longevity than the mild AUP message.

Overall, there is little research on the influence of message framing on security behaviour. The existing research has indicated mixed findings. Anderson and Agarwal (2010) suggested that positively framed messages may be more effective for influencing attitudes and subjective norms in the behaviours of home users. However, they use a very broad term of "security measures" and additional research has found that negative message framing does have an effect on different types of security behaviours more than others, with a greater influence on adopting detective technologies than preventive technologies (Shropshire et al., 2010). Recent research by Barlow et al. (2013) within the workplace has found that neither negative nor positive message framing had a greater effect on deterring employee violation intentions but other recent research by Shepherd et al. (2014) found that negative framing based on deterrence led to decreases in internet abuse. The role of message (positive or negative) framing for motivating security behaviour requires further research to understand its potential role in driving behaviour change.

2.4.5 | SECTION OVERVIEW

The existing experimental research for security behaviour change is a start. There is a lack of research exploring the effectiveness of theory-based studies with experimental evaluation within the workplace. Studies with occupational samples have been supportive of the influence of theory-based training, fear appeals and message framing. More research is needed on the design of interventions that are theory-based with a contextual understanding of the occupational setting and their efficacy validated through experimental studies which will be taken up in

chapter 6. More attention is also needed looking at the role of volitional strategies in security behaviour change.

There are some limitations with the current literature base. Firstly, only a few studies are conducted in a workplace setting (Barlow et al., 2013; Jansson & von Solms, 2011; Johnston & Warkentin, 2015; Kumaraguru et al., 2009; Shepherd et al., 2014). The majority of research has explored behaviour change in the context of end-users but, has largely relied on student samples (Anderson & Agarwal, 2010; Boehmer et al., 2015; Boss et al., 2015; Davinson & Sillence, 2010; Sheng & Magnien, 2007; Waddell, McLaughlin, LaRose, Rifon, & Wirth-Hawkins, 2014; Wirth et al., 2007). Research has shown the bias of using student samples in research and the lack of generalizability to the general population (Henrich, Heine, & Norenzayan, 2010).

There is also a need for more stringent evaluation of behaviour change interventions. The ACMA (2011) in their review of Cyber-security educational campaigns found that was a lack of evaluation and absence of measures put in place before, during and after the initiatives they identified to help assess impacts.

Randomised Control Trials (RCT) are considered to be the gold standard way to evaluate a behaviour change intervention as they provide valid and reliable evidence regarding the effectiveness of the intervention. An RCT design allocates participants to an experimental condition and control condition (which is not exposed to any form of treatment), reducing confounding variables as participants experience all the same factors of the intervention (except differing treatments/control). Randomization is also an important component of an RCT as it reduces selection bias. The importance of RCT and evaluation of interventions are recommended by the Behavioural Insights Team (Haynes, Service, Goldacre, & Torgerson, 2012) and the Medical Research Council (Craig et al., 2009). RCTs will be used in the evaluation of the intervention developed in this thesis.

CHAPTER 3: EXPLORING THE DETERMINANTS OF INFORMATION SECURITY BEHAVIOURS: AN ELICITATION STUDY OF BEHAVIOUR CHANGE FACTORS WITHIN THE WORKPLACE

Work from this chapter has contributed to the following publications:

Blythe, J.M. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In Proceedings of CHItaly 2013 Doctoral Consortium (pp. 92–101).

Blythe, J.M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 103–122). USENIX Association.

3.1 | INTRODUCTION

The literature review demonstrated that there are a number of factors that may influence the degree to which an employee may undertake protective action. An over-reliance on a policy compliance paradigm for exploring security behaviour in existing organisational research means that we do not yet fully understand individual behaviours and their influencers. The question of whether all security behaviours are equal and influenced by the same or different influencers remains unanswered. This has resulted in the first step of this thesis to explore and understand what motivates individual security behaviours that contribute to information security policy compliance. Protection Motivation Theory and the Theory of Planned Behaviour are two important behavioural theories that have been used to explain compliance behaviour but little is known about their potential utility in understanding specific security behaviours in the workplace. Of particular importance to PMT is employees' perceptions of security threats and appraisal of protective actions to mitigate these threats. TPB is concerned with appraisal of their attitude, perceived behavioural control and influence of subjective norms on these protective behaviours. Eliciting these perceptions for individual behaviours will help understand how they may differ by behaviour; identify areas for further exploration and ultimately, interventions to promote behaviour change. To this end, the current study adopted a qualitative method to explore the two theories using semi-structured interviews to address the following research questions:

RQ₁. What are the causes of employees' secure and insecure behaviour across different security behaviours?

RQ₂. What are the potential barriers to security actions?

RQ₃. What differences exist in employees' psychological ownership and organisational citizenship behaviour?

This rest of this chapter will present justification for the approach before presenting details of the study.

3.1.1 | QUALITATIVE METHODS FOR SECURITY

Qualitative methods are a useful approach for understanding security from the perspective of the participant. They are used less often in behavioural organisational IS research and this lack of adoption could be due to the potentially intrusive nature of information security research and concerns for the reputation of recruited organisations (Kotulic & Clark, 2004). These methods afford an in-depth understanding of the reasons for specific behaviours and warrant more use within organisational research.

Existing qualitative studies have been exploratory and inductive in nature, aiming to generate data pertinent to a research question that is not necessarily attached to a particular theory or paradigm (Albrechtsen & Hovden, 2010; Albrechtsen, 2007; Beautement et al., 2009). This approach has often taken the form of semi-structured interviews which allow exploration of key issues and themes in relation to the research question under study. However, there has been little research using a deductive approach. Elicitation studies are one form of a deductive approach used within behaviour change literature and are a proposed stage in some behaviour change models. For example, in the context of the TPB, the purpose of an elicitation study is to determine the beliefs (behavioural, normative, and control) of a target population (Ajzen & Fishbein, 1980). They are considered a valuable part of understanding behaviour (Downs & Hausenblas, 2005) as interviews with the target population ensure that beliefs and attitudes are data driven rather than pre-determined by previous research and the research team's preconceptions of the target group. Other behaviour change models recommend elicitation stages for questionnaire development, for instance, Protection Motivation Theory (PMT; Rogers, 1975) and the Integrated Behavioural Model (IBM; Montaño & Kasprzyk, 2008). The current study is interested in the interplay of factors that are part of these behaviour change models for security behaviours. A deductive approach was, therefore, considered more appropriate as it will allow an understanding of how these factors may differ for individual security behaviours but also allow additional factors to emerge from the interviews that may not have been covered by these models.

Such an approach has proved useful to others. For example Searle, Vedhara, Norman, Frost, and Harrad (2000) utilised components of protection motivation theory in a qualitative application to investigate parents' perspective of children's compliance to wearing eye patches. It has also been used to analyse existing qualitative data, a recent study by Davinson and Sillence (2014) explored financial-related security behaviour in an interview setting using the HBM to analyse

the data. They found the application of a behaviour change model in a qualitative setting to be useful in guiding understanding of factors influencing security behaviour in financial settings.

Elicitation of behavioural determinants using theoretical models as a basis is an important approach in behaviour change as it ensures that underlying attitudes and beliefs are identified from the population under investigation. However, this approach has remained relatively untapped in the information security domain. A deductive approach for understanding components of PMT and TPB is therefore more suitable approach to address the research questions.

3.1.2 | SECURITY AS A SENSITIVE TOPIC

A qualitative approach may be a useful for understanding the behavioural context of information security; however it relies on honest and open discussions with participants. Within the workplace, employees have designated roles and responsibilities for undertaking their primary work tasks. Security, however, can be considered a secondary task (West, 2008). With primary tasks, employees have a clear understanding of how to perform and complete their job duties. However, secondary security tasks can be considered to be much more nebulous. These task differences are further elaborated in the work of Gross and Rosson (2007) who argue that employees' security management lacks the affordances of normal work tasks such as boundaries, constraints, specific goals and resources. Security is not multifaceted, time-bound or goal-oriented, and employees lack feedback on their efforts for performing security actions. Employees may have general awareness of security and practices but lack detailed knowledge (Gross & Rosson, 2007). Employees may therefore find it difficult to discuss security as they may view it secondary to their primary job tasks. Furthermore, security can be considered to be subject to social desirability bias as it is directly linked to an individual's job performance and failure to comply with security practices can have disciplinary consequences towards employees. Researchers may find it difficult to elicit honest responses about compliance. For these reasons, security can be considered a sensitive issue and alternatives for approaches to engage employees are required to aid discussion of security practices and behaviours.

Vignettes may be a suitable tool to help engage participants with sensitive cyber security discussion in interviews. Vignettes are versatile and can be used for a number of purposes including icebreakers to build rapport, elicit attitudes and beliefs about a topic, compare group differences and investigate topics that are sensitive to respondents (Barter & Renold, 1999). They have been used for a variety of sensitive issues including health and wellbeing-related concerns, such as suicide, relationship violence and drug taking (Hughes, 1998). Vignettes can be presented in many forms such as videos but are typically in written format and often take the format of short stories presenting a fictional scenario in which the story places the behaviour of

the character in a concrete context and allows the researcher to explore participants' views on the issues arising from the scenario. Vignettes are useful for exploring attitudes and beliefs towards behaviours and can be used to compensate for lack of personal experience of the behaviour under question. They can generate data untapped by other methods such as interviews and questionnaires allowing them to be used in isolation or in conjunction with other data collection techniques (Renold, 2002).

3.1.3 | BEHAVIOUR CHANGE FACTORS IN THE WORKPLACE

Security behaviours are protective actions that secure information and systems and can be best understood using theories that explain why individuals are motivated to protect themselves. PMT and TPB are two of the most commonly used theories in behavioural information security research (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014). However, they have been widely studied quantitatively for understanding IS policy compliance and protective security behaviours in consumers. There has been little qualitative research exploring their utility for specific security behaviours in the workplace and how they may be moderated at the individual-level within an organisational context. The current study, therefore, seeks to explore factors from these models qualitatively for a set of behaviours that comprise information security compliance to identify how they may be optimised to maximise security behaviour. These factors are shown in Figure 7:
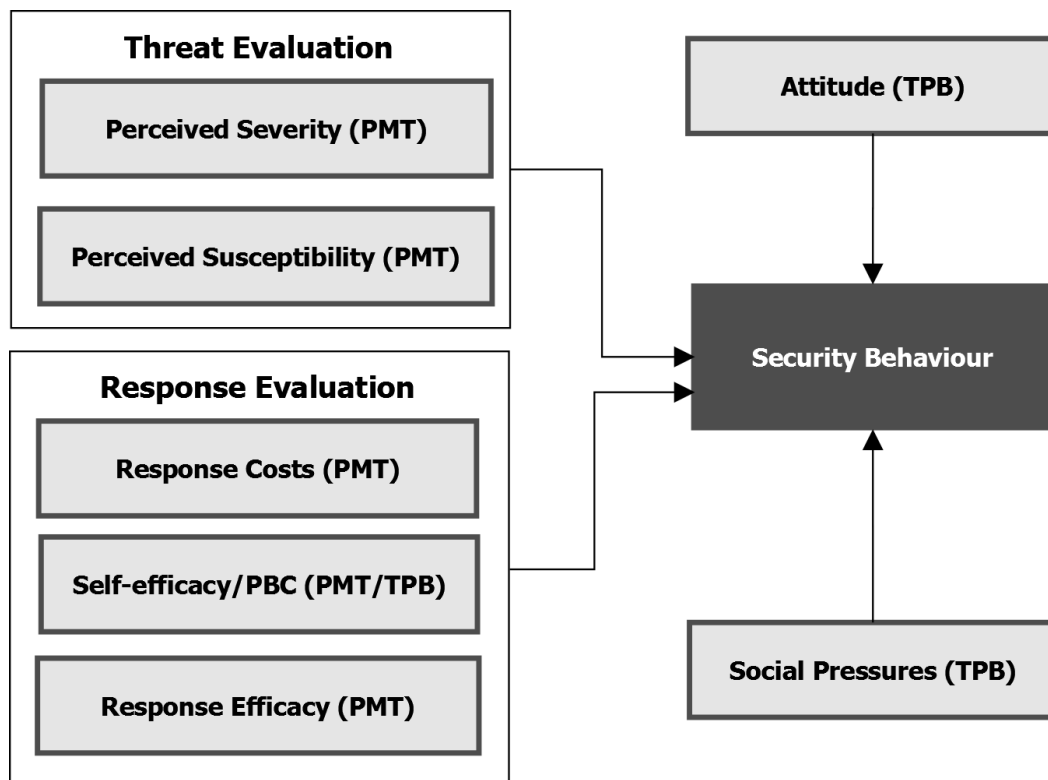
Figure 7. A combined model of behaviour change factors to be explored qualitatively

3.1.4 | ORGANISATIONAL INFLUENCERS ON BEHAVIOUR

Information security research presently gives little attention to the antecedents of behaviour in organisations. Research principally uses general behaviour change theories (such as the TPB and PMT) to explain behaviour but these are not workplace-specific. Using existing behaviour theories will help to provide a clearer picture of the complexities surrounding what causes secure and insecure behaviour in the workplace. However, there may be organisational factors that are not covered by these models which may be important. Behaviour becomes more complex under the constraints of different environments so greater consideration is needed on potential organisaitonal factors that may influence employees' behaviour. The study of organisational behaviour explores how employees behave within the workplace and may provide insight into other potential factors. There are many definitions of organisational behaviour that focus on the interplay of situated social behaviour that is shaped by the communities, beliefs, values and employment systems and practices of the organisation (Clegg & Hardy, 1999).

Two unexplored factors that may be important for security behaviour in the workplace and are of interest to this thesis are organisational citizenship behaviour and psychological ownership discussed in section 2.2.6.5.2 and 2.2.5.5 respectively. The current study seeks to explore if there are differences between the two recruited organisations in these constructs. As discussed in the literature review, both are organisational constructs that influence employees job performance and may play a role in their security behaviour. Intellectual property is of particular interest as employees may experience a connection with this information and perceive it as "theirs" (Pierce et al., 2003) and higher levels of psychological ownership towards a target leads to enhanced protective strategies (Dipboye, 1977; Korman, 1970). Academic and research institutions both work with information that can be considered intellectual property, but may have differing organisational procedures pertaining to intellectual property and ownership. The two organisations for the current study were chosen as a "close match" in terms of types of job and research outputs. Similarly, citizenship differences between the organisations may explain potential differences in the qualitative findings.

3.2 | METHOD

3.2.1 | APPROACH

This study used a semi-structured qualitative approach of vignette based one-to-one interviews and employed framework analysis to elicit factors that influence security behaviours. Interviews were chosen over focus groups as the topic of security was considered sensitive as it is linked to an employees' job performance.

3.2.2 | PARTICIPANTS

A purposeful sample of 20 participants were recruited from two organisations (a university & industry research institution) from the North of England and South of Scotland. All recruited participants were (1) currently in full-time employment, (2) used a computer for work tasks on a daily basis and (3) dealt with sensitive information classified under the Data Protection Act (1998) or information considered sensitive to their company's intellectual property.

3.2.2.1 | Organisation 1

Organisation 1 was a university based in the North of England. 5 males and 5 females took part from this institution, aged between 25-49 years (mean =33.5, SD=9.07). The tenure ranged from 9 months to 15 years with an average tenure of 3.78 (SD=4.25) years. Of the 10 that took part, 4 were on permanent contracts while 6 were on temporary contracts. All participants used a computer for more than 4 hours daily. Only 1 participant had read the information security policy which was in the last 1-6 months. All participants used personally-owned devices in the workplace and 9/10 conducted work tasks on their personally-owned devices. 7 of these participants also stored personal data on their work devices.

3.2.2.2 | Organisation 2

Organisation 2 was an industry research institution based in the East of Scotland. 4 males and 6 females took part, aged between 26-57 years (mean age of 39.10, SD=10.61), tenure ranged from 5 months to 27 years with an average tenure of 11.12 (SD=10.89) years. 8 of those participants were on permanent contracts while 2 were on temporary contracts. 9/10 participants used the computer for more than 4 hours daily while one used the computer for three to four hours. 9/10 participants had read the information policy, of which 2 had read the policy in the last 1-6 months, 2 had read the policy 6-12 months ago and 5 had read the policy more than 12 months ago.

All participants used personally-owned devices in the workplace, 6 participants conducted work tasks on their personally-owned devices and 7 participants also stored personal data on their work devices.

3.2.3 | MATERIALS

3.2.3.1 | Questionnaire

Participants were required to complete a short questionnaire to gather demographic and background information about their gender, age, employment sector, tenure, usage of work computers and personal devices. Questions were included that assessed determinants that were deemed difficult to explore within the interview context. These were organisational citizenship behaviour and psychological ownership.

Organisational citizenship behaviour was measured using the OCB-O questionnaire developed by Lee and Allen (2002). The scale consists of 8 items (e.g. Defend the organisation when other employees criticise it). All items were measured on a 7 point scale that ranged from 1 (never) to 7 (always) in which participants indicated the extent to which they perform the citizenship behaviours. See

Appendix A for full scale.

Psychological ownership was measured using 4 items based on the scale from Anderson and Agarwal (2010) in which the target was changed to reflect the work computer and work data. 2 items measured the subscale of psychological ownership of work data (e.g. I feel a high degree of personal ownership for the data stored on the device I use at work). A further 2 items measured the subscale of psychological ownership of the work computer (e.g. I sense that the device I use at work is MINE). All items were scored on a 5-point scale ranging from strongly disagree to strongly agree. Participants were required to indicate the extent to which they agreed with the statements. See Appendix B for full scale.

3.2.3.2 | Information Security Policies Review

Due to the vast array of behaviours depicted within security policies, a review was conducted of 25 information security policies available online and revealed 11 behavioural categories with expected security behaviours. These behavioural categories are displayed in Table 4. The categories represent shared consistency across the policies, while the actual behaviours within each sub-category varied depending on the company. This current study will explore what influences and prevents security behaviours within these categories, these categories are therefore used as a basis for the interview guide.

Table 4. Behavioural security categories

Category	Description	Example behaviours from policy
Remote working	Actions for working on mobile devices and in external locations	Avoid accessing sensitive information when connected to public Wi-Fi
Removable media	Portable storage devices that can be connected to and removed from a computer (e.g. USB sticks)	USB keys and other removable media must be encrypted
User access management	How access controls are allocated and managed	Strong passwords should be used e.g. have at least seven characters, include one or more numerical digits
Prevention of malicious software	Actions to prevent malicious software	Users must not alter, bypass, disable or remove the anti-virus software from computers
Breaches of security	Steps for recovering and reporting security incidences	Employees must report suspected breaches to a nominated point of contact i.e. IT services
Physical security	Strategies to physically protect infrastructures, information and information resources	All personal and sensitive business information held in any form (e.g. on paper, memory sticks etc.), should be locked away when unattended and not left on desks.
Information control	Responsibility in protection, storage and processing of information	Employees must store company information on the designated drive and not on the computer's C: Drive
Software & Systems	Software and system acquisition, installation and maintenance	Software must be authorised prior to installation
Acceptable usage	Appropriate usage of information systems, email and the internet	Employees must not use their email to violate any laws, interfere with network users, services, or equipment, or harass other users
Continuity planning	Outlines prevention and recovery from internal and external threats	All users of portable devices for example laptops, PDA's, smart phones and USB memory sticks must ensure the information is also stored on the network drives.
Compliance to legislation	Compliance to legislation acts such as the data protection act (1998)	Employees must conform to freedom of information requests

3.2.3.3 | Interview guide

The interview was semi-structured to allow exploration of key issues and themes pertinent to the research question while also allowing flexibility to probe the unexpected issues that are important to the participant (Hutchinson & Wilson, 1992). As such, an interview guide was developed to lead the course of the interview and elicit the behavioural determinants that have been investigated in security research. The guide covered the behavioural categories identified from a review of information security policies to ensure that the scope of information security was covered by the interviews. The behavioural categories (see Table 4) were explored via the vignettes and further discussion with participants. For the behaviours discussed, the questions within the interview guide were targeted to elicit their potential determinants. See Table 5 for explored behavioural determinants and example questions. It was also of interest to explore

potential factors that were not covered by the previous research, so further discussion on security behaviour not covered by the interview guide was encouraged.

Table 5. Example questions from interview guide

Determinant	Example elicitation questions
Self-efficacy	If you want to perform these behaviours, how certain are you that you can?
Experiential Attitude	What do you like/dislike about these behaviours?
Instrumental Attitude	What are the advantages and disadvantages of performing these behaviours?
Social pressures	Who would encourage/ discourage you to perform these behaviours?
Response efficacy	How effective do you think these behaviours are in reducing threats and why?
Response cost	What are the costs in terms of monetary, time and effort in performing these behaviours?
Perceived Susceptibility	How vulnerable to a threat are you by not performing these behaviours?
Perceived severity	What are the potential consequences of not performing these behaviours?

3.2.3.4 | Vignettes

Sixteen vignettes were developed for the current study covering issues related to the security behavioural categories identified from the review of information security policies. The vignettes were used to provide a safe way to open discussion on security for each behavioural category and to encourage honest disclosure from participants.

These scenarios were designed based on recommendations in previous research. As a result, the vignettes remained relatively mundane and avoided unusual events and characters, while also appearing realistic to the respondent (Barter & Renold, 1999; Finch, 1987). The vignettes also had to provide enough contextual information so that respondents had a clear understanding of the situation but be ambiguous enough to ensure that multiple solutions exist (Wason, Polonsky, & Hyman, 2002). As such, the scenarios were designed based on common security incidences related to the eleven categories identified from the information security policies.

Additional vignettes were provided for categories that had many sub-categories. Common security incidences were identified through security provider's reports, news reports, and the research teams' knowledge and experience. The vignettes focused on basic security hygiene behaviours required by all users (Stanton et al., 2005). The wording of vignettes was particularly important to ensure that they did not influence the respondent (Wason et al., 2002) and were designed to avoid stating the consequences of the characters action (as the study was assessing perceived severity). The vignettes remained ambiguous in whether the behaviour and situation portrayed was secure or insecure. Avoiding the consequences of the characters' action,

enabled assessment by the participant of the implications of the characters actions. This approach is outlined by Seguin and Ambrosio (2002) who argue that vignettes should have unresolved issues and finish at the height of tension in the story. The vignettes were neutral and covered behaviours people may not perceive as insecure but are known to be risky from a security perspective. See Figure 8 for an example vignette and Appendix C for all vignettes used.

Removable media

Joe is a 24 year old administrative assistant working for a large telecommunications company. As Joe likes to avoid the rush hour traffic he normally arrives at work half an hour before he is due to start. After parking in a public car park, Joe walks towards his office building and finds a USB stick lying on the ground. Due to his curious nature, Joe pockets the USB stick and decides that he will check the contents of the device when he arrives at work, on his work computer. Upon arriving at work, Joe inserts the USB stick into his computer and opens a number of files.

Figure 8. Example cyber security vignette

3.2.3.5 | Pilot study

The study was piloted with 8 employees to assess the appropriateness of the methodology and the use of vignettes. To evaluate the suitability of the vignettes, 4 participants took part in an interview with vignettes while another 4 participated in an interview without the vignettes. The pilot found that while the vignettes did not lead to more insecure behaviours disclosed by employees; they were useful for exploring participants underlying beliefs and attitudes towards security in the workplace. Furthermore, they proved beneficial in understanding employee's awareness and knowledge of particular insecurities and addressing whether participants would engage in the behaviour. Based on the pilot, the vignettes and interview guide were taken forward to the main study.

3.2.4 | PROCEDURE

The full interview guide and procedure can be found in Appendix D.

Participants who met the criteria for participation were recruited using internal emails in the participating organisations. Participants were interviewed individually, in a private room at their organisation and on arrival were asked to read an information sheet covering all aspects of the investigation, including the purpose of the study and what they were required to do. They then provided written informed consent. Participants then completed a demographic questionnaire that was followed by a semi-structured interview lasting 45-60 minutes.

Participants were first introduced to a topic area (see Table 4) in which the researcher provided a short description of the topic. Participants were then presented with a vignette related to individual behaviours from the topic area and asked to imagine how they would react in that

74

scenario. Following this, discussion centred on how participants currently behave in the workplace for each IS policy area. At this point, the interview guide was used to elicit behavioural influencers for the behaviours discussed. Participants were then given the opportunity to provide any other factors or reasons for their behaviour not covered by the interview guide.

On completion of the study, participants were presented with a debrief sheet that fully explained the purpose of the investigation and re-emphasized participants right to withdraw their data. Participants were all entered into a prize draw to win a £50 Amazon voucher. Following interview completion, the interviews were transcribed verbatim.

3.2.5 | ANALYSIS PROCEDURE

The data was analysed in NVivo 9 using the principles of thematic (Braun & Clarke, 2006) and framework analysis (Ritchie & Spencer, 2002) and verified by conducting a mini-audit by two members of research staff at Northumbria University, who agreed with the theme constructs. The current study used the five-step (see Figure 9) procedure set out by Srivastava and Thomson (2009).

Familiarisation:
Become immersed in data by transcribing and re-reading transcripts

Identifying a thematic framework:
Utilise existing framework and identify any themes not anticipated by the framework

Indexing and charting:
Index and use charts to map data and classify under headings

Mapping and Interpretation:
Development of schematic diagram to guide data interpretation

Figure 9. Framework analysis procedure

3.3 | RESULTS AND DISCUSSION

3.3.1 | PSYCHOLOGICAL OWNERSHIP AND ORGANISATIONAL CITIZENSHIP BEHAVIOUR

Data was scored and entered into SPSS where independent sample t-tests were conducted to investigate differences between the organisations.

Table 6. Means (and standard deviations) of psychological ownership of data and technology and organisational citizenship of employees from the research and education companies

	Psychological ownership of data	Psychological ownership of technology	OCB-O
Research institution	4.75 (1.01)	4.60 (1.17)	4.85 (.66)
Education institution	4.35 (.88)	4.35 (.82)	4.28 (.65)

The findings suggest no significant differences were found between the two organisations for perceived data ownership (t(18)=-.944, p=.358), perceived technology ownership (t(18)=-.533, p=.587) or organisational citizenship behaviours (t(18)=-1.96, p=.066).

3.3.2 | THEMES

Seven themes emerged from the framework analysis of the data. Table 7 provides an overview of these themes and Figure 10 provides an overview of how these themes may link together and influence security behaviour. Response evaluation stems from PMT but with the addition of perceived benefits. Threat evaluation also stems from PMT but also gives attention to employees' information sensitivity appraisal and their individual threat models. Knowledge, experience, security responsibility and personal and work boundaries emerged from the data and did not necessarily confound to PMT or TPB. Security behaviour also emerged as a final theme and consisted of three levels of security hygiene. The following sections will be dedicated to discussing these themes individually.

Table 7. Summary of emergent themes

Theme	Brief description
Response Evaluation	Assessment of security behaviours as characterised by response efficacy, perceived benefits and response costs.
Threat Evaluation	Appraisal of the threats to information security as influenced by individual threat models, susceptibility, severity and information sensitivity appraisal.
Knowledge	Knowledge of security risks and protective actions and the sources that contribute to this knowledge
Experience	Previous experience of security including security breaches and work experience
Security Responsibility	Whom employees perceive is responsible for security in their workplace
Personal and Work Boundaries	Boundaries individuals have between personal and work
Security Behaviour	The actions employees take to ensure information security which is categorised as either high, medium or low-security hygiene
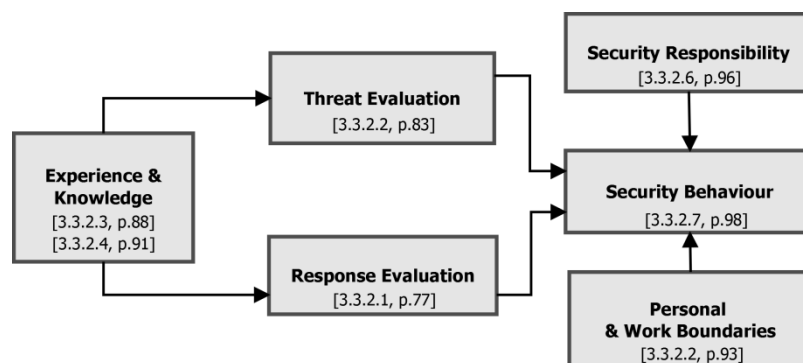
Figure 10. Thematic framework of security behaviour

3.3.2.1 | Response evaluation

Prior to undertaking a security action, employees evaluate the response and its associated outcomes. This is referred to as response evaluation which is characterised by; response efficacy, perceived benefits and response costs. See Figure 11 for visualisation of the response evaluation theme.
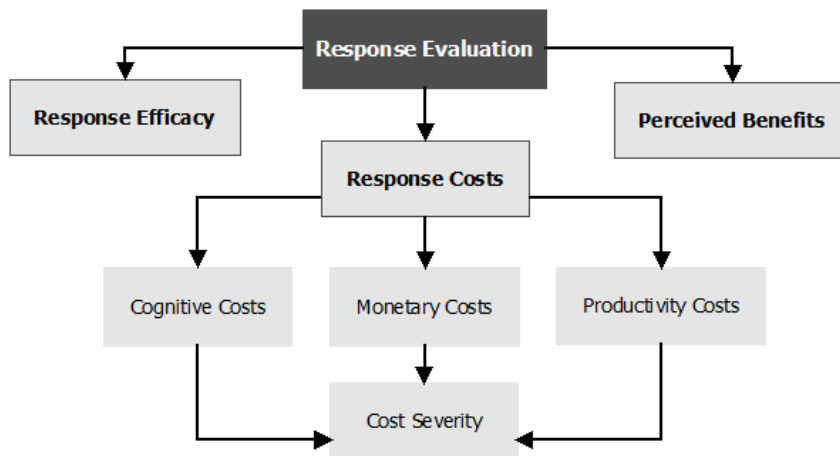
Figure 11. Thematic map of Response Evaluation

3.3.2.1.1 | Response costs

Security behaviours require different levels of input and effort on behalf of the user. The findings from this study indicate that employees appear to make a decision about whether to execute a security action, which is based on an appraisal of the costs associated with it. The major cost concerning employees is the degree to which security impacts on their job as there appears to be a "productivity threshold" regarding security actions. This can lead to a number of behavioural outcomes, for instance, the employee circumventing the security process or disregarding the security behaviour. This security vs. productivity imbalance was apparent for behaviours relating to information access such as password restrictions. Furthermore, tasks such as restarting the work computer for security updates were also seen as impacting on productivity. Employees recognise the disturbance these restarts cause to their workflow and will subsequently postpone the task until a period of low inactivity or until the end of the working day.

> *"I will postpone it (the compute*r), postponing security updates happens a lot because they usually time them at really inconvenient times.. *it's* like well do you want me to do my job?...."* [P14, Company 2]

This security vs. productivity imbalance is also evident in software acquisition procedures. Organisations often place restrictions on the software employees can install on their work machines, requiring administration rights and authorisation for the installation of new software. There were organisational differences in the current study with regards to how the companies mandate software acquisition. The university has a very restrictive system where users have no administration rights, employees can only install pre-authorised software or seek IT services to deploy a computer administrator to install additional software. The research institution, on the other hand, had a less restrictive system allowing employees to freely install software. Both organisations had the option of allowing employees to install authorised licenced from the

company network. The lack of installation restriction meant that employees did not consider the licencing agreements of software and would download software without consultation from IT including pirated and open access versions.

There are also monetary and time costs associated with acquiring legitimate software. Official procedures for software acquisition are considered "time-consuming" due to the organisational process for procuring new software. Furthermore, new software requires allocated budget to be able to purchase the product. However, employees recognise that there is not often budget available, in which employees express a "don't bother" attitude that leads to risky software acquisition such as the downloading of freeware obtainable online.

> *"bu*t because I know it is going to end up as a no anyway *I just don't bother with* that.. just save yourself the grief and go and get the free thing, that does the job equally well without the hassle.." [P14, Company 2]

Security vs. productivity is the largest response cost that employees are faced with as it directly affects "doing their job". However, there are other response costs employees associate with security behaviours. Monetary costs were mentioned less and typically referred to the acquisition of software for personal devices such as purchasing anti-virus on their own laptop. Cognitive demands were another major cost which occurred as a result of using passwords. Passwords are a form of knowledge-based authentication which relies on the user to remember a password to validate them as the user. Many online services require passwords with their own strength requirements. In addition to this, employees also have their workplace passwords to remember which they may be forced to change regularly by their organisation. The result of this is that employees have many passwords that they are required to remember, with different password requirements resulting in high cognitive demand on the user.

> *"Well passwords.. you know actually after many years using computers the passwords just get longer and more complicated to remember, most of them are just randomly generated letters and numbers which can make them hard to remember especially if you.. well especially if you have to change them"* [P6, Company 1]

Not all security behaviours have response costs as some actions require minimal time and effort on behalf of the users. Specifically, the security behaviours of locking the computer, keeping a clear screen and desk policy, and checking physical environments when working in public locations were seen as having minimal costs. Employees recognise that these less costly behaviours become more of a "habit" to ensure they follow through with the action.

".. there is no real effort on my part and I mean ultimately it is CTRL ALT DEL and you have locked your computer and that's all it is.. so it's not exactly an effort from my perspective.. that's probably it.. it doesn't delay me or put a burden on what I am doing generally.. I imagine it would be effort.. I would be a little bit more resistant if there was a lot more effort.. for me to do stuff..." [P4, Company 2]

Perceived response costs are part of PMT (Rogers, 1983) and previous research has mixed findings with regards to response costs and security behaviours with a number of studies not supporting a relationship (Crossler et al., 2014; Crossler, 2010; Gurung et al., 2009; Ifinedo, 2011; Ng et al., 2009). However, this study supports the negative relationship between response cost and compliance intention (Herath & Rao, 2009b), anti-malware software (Chenoweth et al., 2009) and intentions to engage in password protective behaviours (Zhang & McDowell, 2009).

The current study suggests that different security behaviours have a different set of response costs that are not equally as costly as suggested by the IS policy compliance paradigm. These differences in response costs by security behaviour may account for the mixed results in the security literature. The findings also support the "compliance budget" that suggests that individuals' choice to comply or not comply is determined by the perceived costs and benefits (Beautement et al., 2009).

3.3.2.1.2 | Perceived benefits

Another aspect of an individual's response evaluation refers to their perceived benefits of performing security actions. Overall, it emerged that employees understood the benefits of security behaviours regarding protection of information and technology from malicious others, and maintaining the confidentiality of data.

"Again advantages are that you can keep your information secure.. you can be confident that.. you're taking responsibility" [P2, company 1]

There was also an overall perception of "layers of security" in which the individual security actions help contribute to the overall picture of information security.

"It's like having a burglary, if you leave your door open it's like inviting someone in but if you put extra locks on, it's deterring them so I think the stronger your password is, the more of a deterrent it is to people.." [P8, Company 1]

Reassurance in security was another perceived benefit within an individual's response evaluation. Employees gain reassurance that their actions are aiding information security and they feel safer in what they are doing.

"I like it (anti-virus) because I think it's important, it gives you an element of security that what you are using is safe… so you don't have to worry as much.."
[P8, Company 1]

".. well I think having it there, whether it's effective or not just makes me feel just a little bit safer.." [P1, Company 1]

3.3.2.1.3 | Response efficacy

This sub-theme is an individual's assessment of the effectiveness of security behaviours. The findings from the current study indicated that employees struggle to evaluate the effectiveness of security actions as they lack awareness and feedback on security behaviour.

"I don't know. Again I'm not a techie so I am not really sure but.. I mean I don't know, if you password protected it whether somebody could still access it, I don't know. I guess they probably could" [P4, Company 1]

Feedback appears to play an important role when employees evaluate security behaviour. Gaining information regarding their security performance allows them to assess how effective it is. A lack of feedback about security behaviour indicates that employees cannot develop an awareness of the utility of the security action. This indicates that there is an "action-feedback" gap in employees' information security efforts.

"The one time that I did get a virus on an email.. the computer picked up on it straight away and I just rang IT and they came and got rid of it so obviously that is protecting the computer.. erm. so yeah.. effective.." [P5, Company 1]

"They say things that if you don't notice something has gone wrong that that is a sign of effectiveness, that's what they say so I am gonna go with I think it is working (antivirus).." [P14, Company 2]

Furthermore, individuals' estimates of security response efficacy directly relates to their perceived susceptibility. As discussed in the "Susceptibility" sub-theme of threat evaluation, individuals perceive different levels of susceptibility depending on a physical or cyber security threat. Employees' response efficacy is capped as there is an overall "sense of insecurity" in their actions in which hackers or the IT savvy can still get access, undermining the effectiveness of their security efforts. However, they do perceive their efforts as effective against the average end user or criminal.

"I think it's (encryption) effective.. if someone really wants to find out what is on there.. they will find out.. if they are a hacker.. but it's enough to stop.. like if Joe picked it and put it into his computer and it said you can't read this file because it

is password protected or encrypted in some way.. it may be enough to stop him and just hand it and say I have found this.. so again I think it is a good enough deterrent and as I say if someone for whatever reason really wanted what was on that stick.. I am sure they could find ways of cracking the encryption but it is a good enough deterrent for 90% of the population.." [P19, Company 2]

Regarding behaviours that were perceived to be most effective for security, the current study also asked participants to pick three security behaviours that they perceived to be most important for information security (the findings of which are presented in Table 8).

Table 8. The perceived effective security behaviours and their frequency, ranked from most prevalent to least prevalent

Category	Behaviour	Frequency
Access controls		(n=19)
	Don't write passwords down	1
	Use strong passwords	11
	Use access controls (physical and online)	3
	Change passwords regularly	4
Physical security		(n=9)
	Protect physical documents	2
	Physical storage of information	1
	Use ID badges	2
	Use lockable cabinets for physical data	2
	Locking computers	2
Awareness and responsibility		(n=7)
	Treat information confidentially	1
	An awareness of security implications	1
	Personal responsibility for security	1
	Awareness of contemporary practice	1
	Don't share information unnecessarily	1
	Awareness of location of company-issued hardware	1
	Careful of opening files on your computer	1
Use security software		(n=6)
	Use anti-virus software	2
	Use firewalls	4
Removable media		(n=4)
	Use encryption with removable media	1
	Not storing information on removable media	2
	Don't use removable media	1
Internet Security		(n=3)
	More cautious and careful online	2
	Don't download stuff you shouldn't	1
Email security		(n=2)
	Non-disclosure of personal details over email	2
Company Procedures		(n=2)
	More regular security training	1
	Use IT resources	1
Business continuity		(n=1)
	Back up data	1
Personal Usage		(n=1)
	Don't store personal information on work computer	1

The findings show that access control behaviours were perceived to be most important for security, followed by physical security behaviours and an awareness and responsibility of security. Using security software and security with removable media were also seen as important. The findings indicate that while employees struggle to evaluate security actions, they do place more importance on some security behaviours over others.

A large number of models within the behaviour change domain means that these models share overlapping constructs however it has been argued that they are more similar than dissimilar (Maddux, 1999) in their theoretical underpinnings. One particular overlapping construct is outcome expectancy that refers to an individual's expectations of the outcomes that will follow a given behaviour (Williams, Anderson, & Winett, 2005) including the positive and negative consequences of acting and not acting. Perceived benefits and response efficacy form part of an individual's outcome expectancies. Perceived benefits in the current study, however, refers to individuals' estimation of the advantages of engaging in security behaviours that may be distinct from an individual's efficacious perceptions. These factors have received little research in security.

The role of response efficacy in email security behaviour (Ng et al., 2009), intention to comply with security policies (Ifinedo, 2011), attitude toward security policies (Herath & Rao, 2009b), and intention to adopt anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009; Johnston & Warkentin, 2010) has been supported. However, recent research has not supported this relationship (Siponen et al., 2014; Vance et al., 2012) and recent literature reviews (Sommestad et al., 2014) on security compliance have found that response efficacy to be one of the worse predictors of compliance and IS misuse. This study highlights a potential barrier to high response efficacy that may account for the disparity in existing research. Currently, employees cannot evaluate their security efforts as they lack feedback on their performance. However, they did indicate which behaviours they think are most effective for security with those relating to access controls having most perceived utility. PMT argues that response efficacy is part of coping appraisal and that higher levels of response efficacy will increase the likelihood of engaging in the behaviour. This study suggests that employees do not receive feedback or information regarding security actions and the effectiveness of these actions. Lack of/low response efficacy may, therefore, be a potential barrier to security behaviour within the workplace.

3.3.2.2 | Threat Evaluation

Employees undergo an evaluation of the security threats to information and systems. This is related to their individual threat models, their information sensitivity appraisal, their perceived susceptibility and perceived severity. See Figure 12 for a visualisation of the theme.
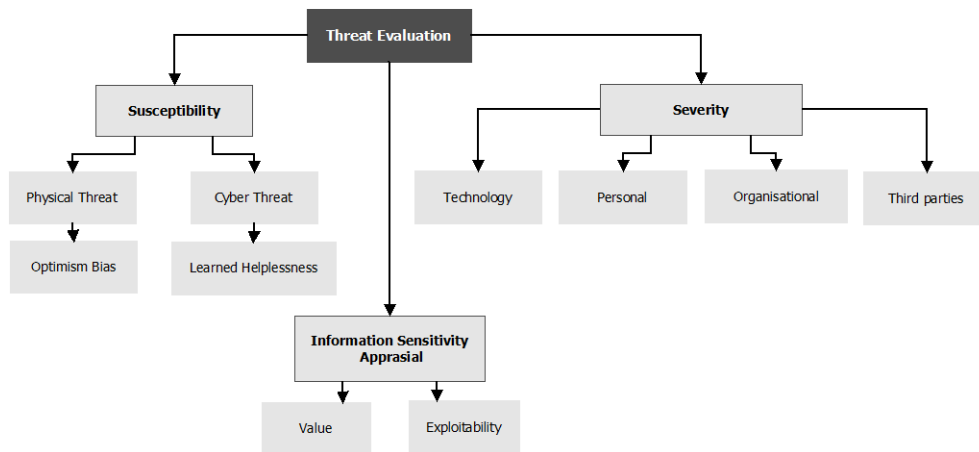
Figure 12. Thematic map of Threat Evaluation

3.3.2.2.1 | Information sensitivity appraisal

It emerged that the information employees work with holds high or low information sensitivity. However, the latter was more prevalent in this sample. This appraisal was often based on an assessment of the "value" of the information that they deal with which entailed a comparison to data with a perceived higher sensitivity such as health-related and financial-related information.

> *"Again, vulnerable in the respect that I could probably do more but at the same time, I am not sure what other people could do with the stuff that I leave lying around, it's not highly confidential or anything like that.. its.. I guess there are levels of data that need to be kept secure.. I haven't got peoples' bank details or anything like that.."* [P9, Company 1]

> *"yeah not a clever one.. having your password written down, in your bag.. again I can relate to having to remember passwords all the time can be difficult.. I think you have got to think of a better way of giving yourself a reminder than having that exposed especially if it has got patient.. at that level healthcare that's.. you couldn't take any chances with that sort of thing so.."* [P12, Company 2]

Furthermore, employees' appraisal also involved consideration of the "audience" for the information and their preconceptions of who can use the data that they store.

> *"It's not an equally weighted.. it's not an objective.. there is no objective value to this information that somebody has given us.. because to the vast majority of people it means absolutely nothing.. it's pointless and they would not bothered even if they were found out"* [P2, Company 1]

This supports research by Adams & Sasse (1999) who found that employees' perceptions of information sensitivity interacted with their perceptions of organisational security. They found

84

that employees rated information about individuals as more sensitive than commercially sensitive company information and placed security as a higher priority on some systems than others. The current study further demonstrates this appraisal through employees' evaluation of the value and audience of the information they work with in their job.

3.3.2.2.2 | Susceptibility

Perceptions of susceptibility to security threats appeared to be an important factor in employees' behaviour. Perceived levels of susceptibility differ across participants and vary depending on environmental or online threats.

Environmental threats to information and systems involve a physical attempt (i.e. offline) to infiltrate the information security of organisations which can include the attempts of criminals and malicious employees. Susceptibility to these kinds of threats appears to be low amongst most employees as they perceive low threat likelihood. Individuals perceive that environmental threats will be malicious others acting in a more opportunistic manner rather than pre-meditated. Individuals appear to hold an optimism bias with environmental threats, comparing the likelihood of a physical threat to other employees or other organisations.

> *"Yeah the physical security I feel fairly protected.. anti-virus, hopefully protected by the IT department.. I would say also because of the likelihood of people who surround me to come and search through my files is just next to zero so yeah I feel very secure"* [P3, Company 1]

> *"it's perfectly safe until somebody wants to get in comes along so you know… so in that respect it's probably absolutely safe 99.99% of the time to leave completely* personal information all over your computer and leave it unlocked because the majority of people that come into contact with it will not be interested and not *want access to it and not want to do anything with it.. so it's only to protect for* that minority of times.. for that possibility that somebody might want it and want access to *it.."* [P2, Company 1]

With regards to cyber threats, employees perceive themselves to be highly susceptible to this type of threat. There appears to be an overall sense of insecurity or learned helplessness in behaviour online. This is particularly related to employees' response efficacy of security behaviours. Individuals have an estimation of the effectiveness of different types of security behaviours and practices. However they feel that "hackers can still get access" and the "IT savvy can still bypass security". Employees understand the importance of implementing security behaviours however they feel that their efforts can still be circumvented regardless of the level of security that they implement.

"I have no idea.. probably they are (passwords) effective if you are going to protect yourself against somebody.. if you want to kind of see security from the person next to you however in terms of people whose job it is to break passwords.. probably not very effective and do realise that there are people out there whose vocation is to break people's passwords and virus people's computers so probably not.. I *have no idea…"* [P3, Company 1]

*"*For somebody like me I think your password would be enough to bar me from accessing your information, logging into your computer but I think somebody who had good sound IT knowledge could probably bypass them and get into other *people's* information*"* [P7, Company 1]

The relationship between levels of susceptibility and engagement in security behaviours has mixed support in the literature. Its relationship with IS policy compliance intention has consistently been supported (Ifinedo, 2011; Siponen et al., 2014) as has its role in anti-virus software usage (Lee et al., 2008). A potential reason for the lack of support in previous studies is that their conceptualization of threats is often non-specific and they do not refer to types of threat (e.g. Vance et al., 2012). This study demonstrates that an individual's threat assessment differs depending on an online or offline threat, with online having higher perceived susceptibility amongst employees. Previous studies do not make this distinction when assessing perceptions of susceptibility. Perceived susceptibility to online threats is closely linked with response efficacy, i.e. they do not believe they are protected even if they behave securely.

3.3.2.2.3 | Threat models

Employees appear to have different security threat models. This is related to their knowledge of security risks, their perceptions of appropriate security actions and perceived likelihood of threats. For example, there appears to be a large difference in attitudes towards writing down passwords. Some employees perceive this as being highly insecure and wouldn't engage in this behaviour, suggesting that they have more of a concern for physical threats than online threats in password security.

*"*I am quite conscious that someone can find a scrap of paper that I have written with a scrap of paper with important company stuff on so I *don't* do that.. even for my personal stuff I *don't* do it*"* [P14, Company 2]

Some employees, on the other hand, may perceive this as being insecure but balance the likelihood of an online threat vs. an environmental threat, in which they perceive the latter as being less likely so engage in this potentially risky physical behaviour.

"I just have like a note.. well.. I have a note with all passwords for all the different places where I need stuff, like online because there is too many passwords to remember so I need to have them written down somewhere.. "[P1, Company 10]

Other differences in threat perceptions were noted for working remotely and allowing unauthorised users to use work devices, locking work computers, and using encryption on removable media.

3.3.2.2.4 | Perceived severity

There was disparity in perceived severity of security breaches and the severity of security non-compliance consequences. Employees were highly aware of the consequences to their organisation's reputation and the potential implications of this. For example, competitors getting hold of their company's intellectual property and breaching legislation such as the DPA (1998).

"again other than the competitive threat that we are developing something that we don't want the competition to know about and they get access to that information.... you know something like that I guess would be of value to the competition so that they would then have time to put a counter strategy together"
[P16, Company 2]

"I guess anybody can get access to any sort of information, even if they shouldn't and that can lead to all kinds of issues and data protection laws and even just the sort of stuff that we have here like student files.. that a student should give you their information in the knowledge that only the people who should have access to it, have access to it.. so I guess, I mean the issues.. the.. the massive aren't they.. the potential for press, the press could get hold of the fact that the information isn't kept secure so that is all sorts of stuff blown out of all proportion typically.."
[P9, Company 1]

The impact towards technology, following a security breach, was also a consequence that employees had a high awareness of. This was primarily the consequences of downloading a virus or other malicious software to the work machine and the effect this can have on the organisation's network.

"if it's a really bad virus it can like infect your computer and I can assume it kind... like.. if somewhere like here, I'm not sure how realistic it is but I suppose technically it could affect the whole university system which would cause massive outrage and whatever, so I think you would get into a lot of trouble for doing stuff like that and I think it would have large consequences" [P8, Company 1]

Employees' perceptions of consequences to themselves were relatively mixed as employees were not aware of company action if they cause a breach in security. However, employees held assumptions about potential consequences that were often disciplinary actions or reduction in their own and companies' productivity. Consequences to others were considered less and included dissatisfied service users and distressed service users.

> *"I am not aware of the consequences for it.. I mean I am aware of the kind of potential problems that you could cause, and the stress you could cause people if any information was disclosed about a particular person but I don't know if I did something that caused a problem within the university systems I don't know what action would be taken"* [P7, Company 1]

Previous research has focused on the role of perceived severity in IS policy compliance (Herath & Rao, 2009b; Siponen et al., 2014), and anti-spyware adoption (Chenoweth et al., 2009; Gurung et al., 2009). The role of perceived severity on anti-virus adoption (Lee et al., 2008), being cautious with emails that have attachments (Ng et al., 2009) and other IS policy literature (Ifinedo, 2011) is unclear. The findings suggest that individuals perceive consequences and severity differently. These are consequences towards the organisation, technology, 3rd parties and themselves. Within these levels, knowledge of the consequences also differs with less awareness of consequences towards others and oneself. This suggests that an individual's perceived severity is not one overall construct but may comprise of different types of severity implications. This may account for the differences in existing research.

3.3.2.3 | Experience

Experience was an emergent theme from the current study and related to individuals experiences of security beaches and previous work experience. See Figure 13 for a visualisation.
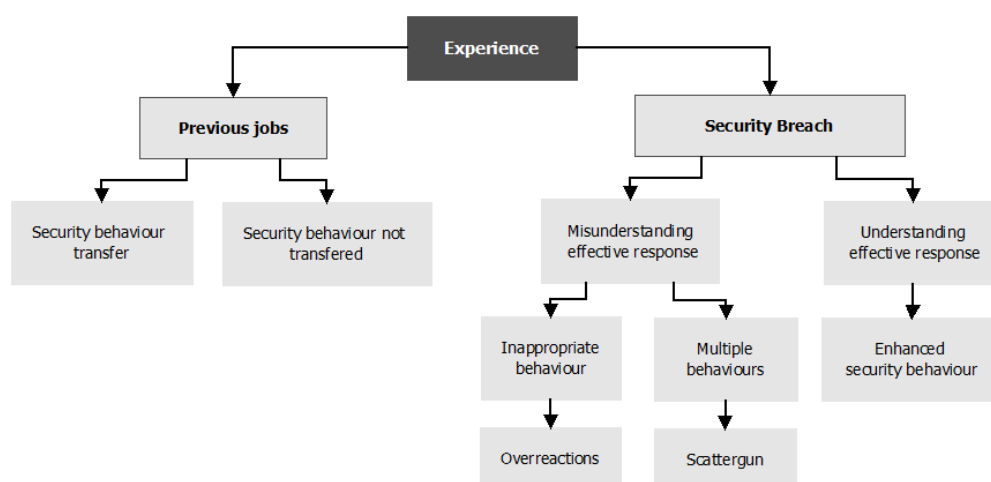
Figure 13. Thematic map of Experience

3.3.2.3.1 | Security breach experience

The current study suggests that previous experience is important for current behaviour. Previous job roles and experiences of security threats (including viruses and phishing emails) appear to promote awareness and secure behaviour. An employee's experience of security breaches can lead to different courses of action depending on their evaluation of an effective response to the breach. If an employee misunderstands an effective response, this can lead to "security overreactions" in which they make take a scattergun approach to dealing with the breach to ensure recovery and continuity (e.g. deleting contacts and changing passwords following an account breach).

> *"I mean I wouldn't do anything.. I mean once.. something must have happened to my email address, my yahoo email address because people were just getting emails just saying "try this money making scheme" so as soon as I got that.. I deleted everyone off my contact lists because I had them somewhere else and change my passwords and things like that.. but other than that, nothing.."* [P2, Company 1]

Inappropriate behaviours are another form of "security overreactions" and can lead to non-use of accounts and concluding that devices are unusable following a virus and a new machine needs to be acquired.

> *"Hotmail. Microsoft.. whoever owns it and yeah just couldn't get back onto it and they wouldn't allow it.. even though I gave them all the information that I could to say it was me.. they just said that it wasn't enough information so gone... I don't use it anymore.."* [P1, Company 1]

> *"I could see that it is not a right file and he should I have no idea why I clicked on it and the computer is now very slow and unusable so we are going to be binning it or selling it for parts.. no reason for that and it shouldn't be happening.. and we know that we should never disable the anti-virus."* [P3, Company 1]

These experiences typically refer to personal experiences; however work-related experience also appears to be important for secure behaviour especially when it impacts on an employee's productivity. For example, when an employee's organisation experienced a virus breach it led to implications that affected the whole business operation.

> *"it made me realise actually there is.. this is not some pen pusher saying don't use pen drives.. it's actually really serious and that was a good lesson for me and I think a lot of people don't understand the importance of things like that but*

because I have got experience of what happens.. of what could go wrong.. when it goes bad.. when it goes wrong it goes wrong really badly.." [P14, Company 2]

3.3.2.3.2 | Work experience

Previous job experience also appears to be important for current security behaviour. Organisations differ in their approaches to information security and subsequently their methods to promote security awareness and practices amongst employees. This is known as the security culture of an organisation which is their shared values and assumptions regarding information security. An organisation's culture is idiosyncratic so there will be differences in the levels of security culture across companies. Employees transfer their behaviour from previous organisations; this appears to be more evident in employees who come from organisations with a higher security culture than their current employer.

> "Again from my previous job there was, the company had a very very high.. it was very secretive company and there was a lot of examples where competitor espionage and things like that was.. it was a very regular occurrence and a very serious thing so security was.. it was like fort Knox over there most of the time so it just got drilled into you to lock your computer work station so that is just something that I brought with me to this job.. I notice that a lot of people *don't* lock their work stations" [P14, Company 2]

> "I kind of have a habit of doing that anyway.. like I say I used to work in a bank and we used to always lock our computers.. but I think *it's* just a habit really". [P2, Company 1]

However, not all behaviours are transferred as there appears to be a security threshold where employees will not transfer the behaviour if it requires too much effort on their part. For example, strong password enforcements in previous companies do not lead employees to adopt a strong password management practice in their current job if it is not enforced.

> "I have had the same password for the last 6 and a half years on my computer. I know I should change that, in my previous employer we got sent a reminder to change the password, I think it was every three months we had to change our password ... I know I should change it but I *just don't have the memory space to* do that.. I would forget what I had changed it to." [P9, Company 1].

Experience has received little investigation in previous research but has been supported for anti-spyware usage (Sriramachandramurthy et al., 2009), adoption of online privacy protections (Yao & Linz, 2008), and adoption of virus protection behaviour (Lee et al., 2008). Experience is also a source of information within PMT, influencing threat and coping appraisal. These

findings suggest that previous breach experience is important for current behaviour. Furthermore, employees' experiences of security in previous jobs are also important and potential transferability of behaviour has not been formally explored in employee security behaviour.

3.3.2.4 | Security-related knowledge

The theme is illustrated in Figure 14 and comprises of sources of knowledge and knowledge of specific domains (i.e. security risks and security actions).
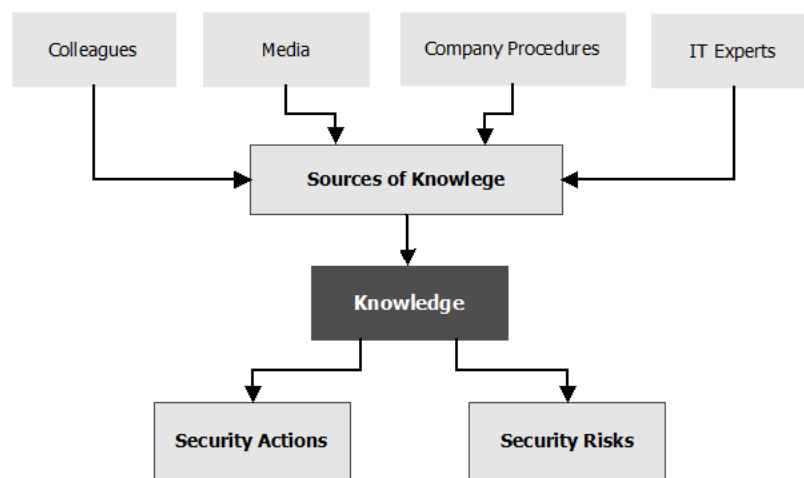
Figure 14. Thematic map of Security Knowledge

3.3.2.4.1 | Security risks

Knowledge of security risks is diverse and varies depending on security behaviours and security threats. Awareness of risks specific to poor password management is most prevalent and indicates that employees can identify the risks associated with: using poor passwords, not changing passwords, the disclosure of passwords, recycling passwords and writing passwords down. Furthermore, knowledge of risks associated with employees having administrative rights, risks when working remotely, viruses and social engineering tactics such as phishing emails were also high. Knowledge of risks related to mobile devices, removable media and physical security were however quite mixed, with mobile devices in particular an area where employees lack awareness of the risks of using mobile devices and the potential susceptibility of these devices.

3.3.2.4.2 | Security actions

Knowledge of security actions was also mixed, particularly with regards to those which are formally set in their organisations information security policy. There were differences in employees' knowledge of the security policy and its associated procedures between the two recruited companies. Information from the demographic questionnaire indicated that in the

academic institution only 1 employee out of the 10 recruited had read the policy compared to the other organisation in which 9 of the 10 employees had read their companies policy. While reading the policy does not indicate compliance with it or awareness of the entire content; it does appear to be a source of reference for some employees when determining appropriate security actions. Those who are unaware of their IS policy rely on their awareness of appropriate security actions when behaving with information and technology and may depend more on other sources of knowledge to inform appropriate security actions (such as recommendations from fellow employees).

Regarding security actions, encryption for removable media and work devices was the security action in which employees lacked most awareness of and sometimes there was clear confusion between the differences between encryption and password protection. Other security actions employees appeared to be knowledgeable about were those associated with; authenticating users, physical security of information and technology, and the prevention of malicious software. Two-factor verification for cloud storage and email accounts were security actions that were mentioned less and could be behaviours that requires further awareness.

3.3.2.4.3 | Sources of Knowledge

Employees relied mainly on individuals within their workplace or social circle whom they regard as having "IT expertise" as a source of security information. In the workplace, this was employees from the IT department but can also be fellow colleagues or friends with IT expertise.

> *".. I think it's* pretty good.. I have got windows laptops and I have got a mac and.. I have done research on the different virus software that you can use which is freely available.. I only use the freeware stuff.. and I have asked my friends as well who are quite up on computers and what not and I make sure that I use kind of the same ones that they do.."* [P1, Company 1].

Fellow colleagues and line management were noted to a lesser extent as sources of knowledge and this most commonly related to the receiving of suspicious emails or files, in which case they would seek information from their immediate peers before contacting "IT expertise" sources.

Other sources of knowledge were company procedures such as the IS policy or professional codes of conducts that cover aspects relating to the integrity of information and its security. For example, one employee has to sign non-disclosure agreements with service users and this influences their behaviour.

> *"I probably used to leave my computer unlocked more.. but in the job that I do* now we have to sign non-disclosure agreements so if you are working with a

university on certain things or different companies you have to sign NDAs and there have been some projects which have been deemed as pretty secret I guess so *you have to sign them and say that you won't talk to anybody about them.. you won't.. and as part of signing them it says when you leave your desk* you must lock *your PC.. you will adhere to this and stuff so I am very aware of doing that.."* [P19, Company 2]

The media was another source of information such as reports about hacking to consumers and organisations and their associated consequences such as identity theft and fraud-related experience (individual) and network disruption and reputation (organisation). Media reports relating to security risks and their implications were also noted such as government bodies losing unencrypted USB sticks with sensitive information on it.

"Well.. so far it's not too bad right other than there has been a few cases where we have seen.. Facebook.. or LinkedIn passwords being cracked so the information that I have got on Facebook *isn't* particularly of interest but of course then when you *go into online banking and everything that's when it starts to get a bit scary.."* [P17, Company 2]

3.3.2.5 | Personal and work boundaries

The theme is illustrated in Figure 15 and refers to the boundaries employees have between work and personal life.
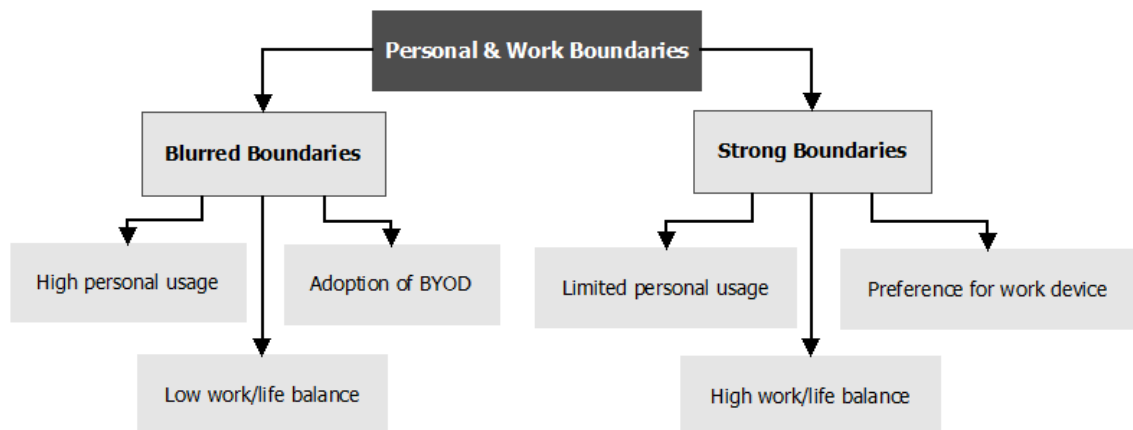
Figure 15. Thematic map of Personal and Work Boundaries

An important factor influencing secure and insecure behaviours is the degree to which individuals engage in personal activities on their work devices and the boundaries they have between home and the workplace. Those who have strong boundaries between home and work limit the personal usage they conduct, for example using the work email for work use only and limiting personal browsing on the internet.

"Well I try not to use it for anything personal so I don't really email anybody outside of work with my work email, just try to use my home one so in that respect trying to limit that.." [P12, Company 2]

"Well actually when I am at work I just do work to be honest and usually the sites and places that I visit on the web are educational resources or whatever.. I tend to.. I don't think I don't really surf the web and stuff and don't just click on random links and stuff.... I just stick to work related things and like I assume those kind of resources are pretty clear.. IT also have a web filtering thing so that might help as well" [P6, Company 1]

These strong boundaries also extend to outside of the physical workplace and relate to the use of work devices for personal usage when working remotely. Employees with strong personal boundaries use work devices solely for work purposes and don't allow unauthorised users (e.g. family, friends) to use the devices.

"I would suggest no, I mean personally I wouldn't let somebody use it a work PC.. even to log them on as different user or something" [P13, Company 2]

"Don't let anyone else use the computer. No one would want to use the computer anyway but erm.. I don't anyone else use it.... I don't like leave it in anyone else's care.. it's always kind of, under my own care because it's not my computer to pass around" [P8, Company 1]

These individuals also demonstrate a preference for using work-issued devices over their personal devices for work tasks. They may, therefore, be less likely to engage in BYOD activities.

"try not use personal devices.. that is as close as it gets.. I just view it as a work one, it's just that I am using it with two different works.. I don't use..

So what about that distinction of work and personal?

I think *it's* important in my mind having that line for a couple of reasons.. the information that is coming out of work, I *don't* want it stored on my home stuff for any trace of it and there was another reason.."* [P4, Company 1]

"Only to transfer files.. I don't get my work email on my phone.. but that's not actually to do with security but that's to do with the fact that I don't want to get my email on my phone.. my phone is my phone and I don't work stuff coming through

on it.. *It's* not the security aspect of it so I *haven't* really considered the security aspects of it because *it's* not something that I plan to do*"* [P17, Company 2]

The role of technology in employees' work/life balance is well documented in organisational psychology literature, ubiquitous access to the workplace can enhance individual productivity however can also inflate individual's stress levels leading to job burnout (Peeters, Montgomery, Bakker, & Schaufeli, 2005). However, a strong work-life balance may also be important for security. Working remotely is a necessity in some job roles, however, optional in others. Limiting working remotely is important for security as it can reduce security risks associated with working outside of the workplace. Individuals with a high work/life balance limit or prohibit doing work tasks outside of the workplace.

> *"I just generally don't once I leave work that is me done but for serious* work.. I know for example my boss and other people they have work laptops and they can work from home.. they get special equipment where they can do that.. it*'s not* really applicable to me..*"* [P14, Company 2]

They also have high psychology ownership of their personal devices and, therefore, limit work-related information on their own devices.

> *"Yeah I *don't* even know if it is a security conscious thing.. I think it is more just.. work/life balance of this is my phone.. I *don't* want to contaminate it with work stuff... yeah its mine, it's not the company's"* [P19, Company 2]

> *".. my phone is my phone and I don't work stuff coming through on it.."* [P17, Company 2]

Individuals with blurred boundaries between personal and work usage are less restrictive in their boundaries and engage in personal tasks on work devices. For example, they may have blurred boundaries in email usage for work and personal.

> *"In terms of the first one.. *It's quite tricky coz whilst I don't really receive emails* from my like.. I kind of do receive emails from my friends at work coz they also work here but *I don't receive emails from my friends who don't work here on that* account but at the same time but I also have it set up so that I do receive my Gmail *stuff to that computer as well so it sort of kind of blurs the boundaries a little bit"* [P6, Company 1]

When working remotely these boundaries are also blurred; they may use work-issued devices for personal usage and allow others to use the work devices.

> *"I have done it myself if my nieces have been up and there is only one laptop.. like my own personal one and someone wants to do something else then I would give them the work laptop to do it.."* [P19, Company 20]

They have less distinctive boundaries between home and the workplace and consequently have a lower work/life balance, they prefer ubiquitous access to work information so may use their own personal devices to stay connected to work and subsequently engage in more BYOD activities.

These employees also engage in more personal risky tasks on their work machines and disclose highly sensitive information such as bank details as they rely on the security of their organisation and assume that it is more secure than their own devices.

> *"Bec*ause everything on mine is what I have put onto it or set up to work on it or *adjusted the settings and I don't really understand what I am doing with stuff like* that so you assume that because you get an email from IT services periodically that goes to all users that says that we have identified a machine which is running malware on the network and they will give you the work station name of it and you *eventually track it down, you assume that because it's a corporate computer* system that there is some money and some resource and expertise at keeping it *safe.."* [P13, Company 2]

The use of personal devices in the workplace or BYOD (Bring Your Own Device) can bring many advantages for businesses including enhanced employee productivity, satisfaction and mobility (PwC, 2012). Despite this, BYOD also leaves organisations open to information breaches. Despite calls for organisations to implement more stringent BYOD security strategies (PwC, 2012), there is little research exploring employee attitudes towards BYOD, the factors that influence this form of behaviour and the role of personal device ownership on information security. This study sheds some light on security behaviours and BYOD activities relating to work/life boundaries.

3.3.2.6 | Security responsibility

The theme is illustrated in Figure 16 and refers to employees perceptions of who is responsible for security.
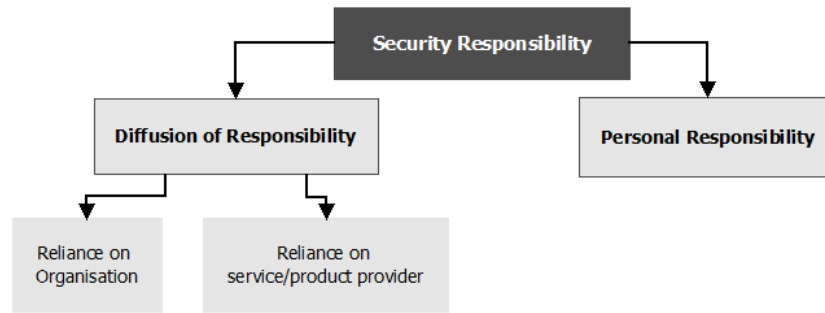
Figure 16. Thematic map of Security Responsibility

Employees rely heavily on their organisation or "security experts" in their company for the security of their systems. This appears to relate to specific types of security mechanisms such as anti-virus, encryption on machines, and system procedures such as installing updates rather than behaviours such as passwords and handling data, in which participants recognise they have responsibility.

> *"To be honest I assume that if that's* what the company tell us to use then somebody in the technology area has decided that it is secure enough and that our firewalls are there and whatever "* (P16, Company 2)

To prevent viruses and other malicious software, employees appear to rely heavily on their organisation with assumptions that "somebody else is taking care of it" and relying on the expertise of those in IT to ensure that they are protected from viruses.

> *"I don't understand bugger all about anti-virus software and all that kind of stuff and you assume that somebody else takes care of it and if you need it, it's sort* of automatically deposited onto your computer and you assume that its therefore as good as it needs to be or as good as it can be.. there are people who work in IT services and *that's* their job so you assume *that's* good enough.. "* [P13, Company 2]

> *"Yeah actually I haven't* checked what it is and how it works and whether I should do something about myself or if *it's* something that just works in the background.. I*'m hoping that it's just something that's in the background and then* its updated automatically and things like that.. maybe I should.. I *haven't* checked so far, I always just assume *that's* updated centrally from the IT services "* [P10, Company 1]

In the adoption of new security practise, diffusion of responsibility was also apparent, employees would adopt a new security behaviour but only if the company enforced it, therefore relying on the company to introduce new security practices rather than an employee taking responsibility and implementing a new behaviour.

"Yeah I would be quite happy to do it if the company came out and said every USB stick that you put in has to be encrypted and yeah I would do it.. again it becomes that another hurdle to get through in ya productivity of work but I can *understand that reasoning for it.."* [P19, Company 2]

This diffusion of responsibility was not just limited to the organisations that the employees work for but to also service and product providers of the technology they use for work tasks. For example, there was a general perception that Apple products are secure so you do not need any additional security and that you can rely on Apple for the security.

*"*I have got a mac at home so as far as I know I *don't* need any security on it.. it has got its own inbuilt.*"* [P12, Company 2]

*"*My understanding is that.. it*'s very basic first of all but understanding is* that its.. the operation system of the.. of apple products... is designed in such a way that you *can't* download.. not download things but I *can't* quite explain what I mean and what I know because I *don't* even know it properly but yeah *it's* kind of protected.. it *doesn't* require anti-virus..*"* [P3, Company 1]

The current study supports the findings of existing research (Dourish, Grinter, De La Flor, & Joseph, 2004) which found that individuals delegate responsibility to one of four modalities: technology, individuals, organisations and institutions. However, delegation of responsibility for specific security behaviours has remained relatively unexplored in existing quantitative studies.

3.3.2.7 | Security behaviour

The final theme is illustrated in Figure 17 and refers to the actions employees undertake to maintain information security in the workplace.
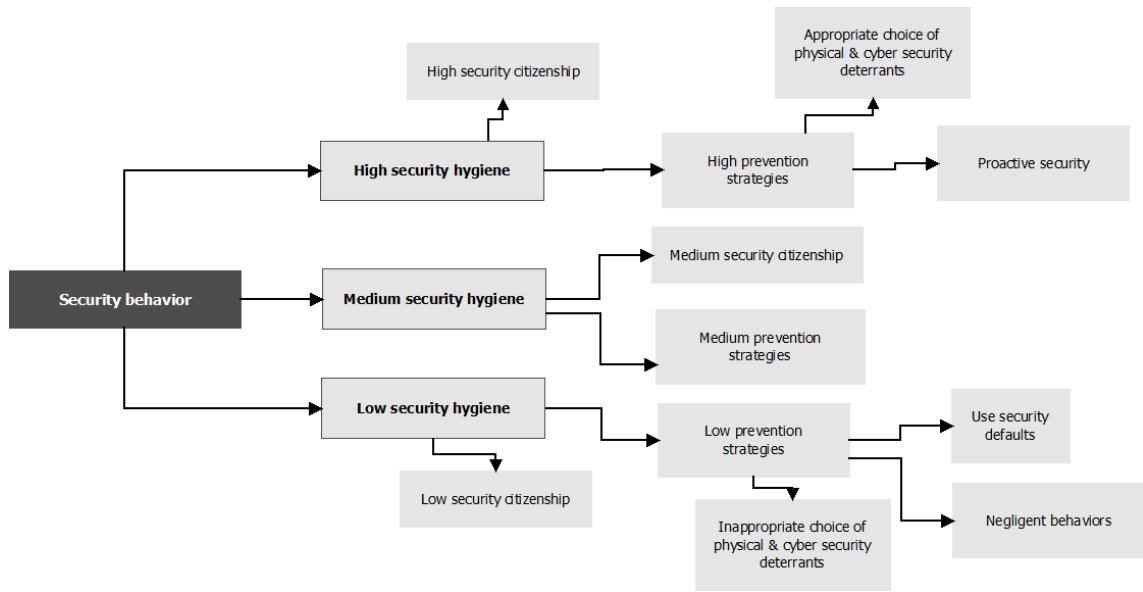
Figure 17. Thematic map of Security Behaviour

Security behaviour is an important overall theme as it indicates an employee's ability to engage in appropriate and effective security actions. There is three forms of security behaviour, here referred to as "security hygiene", which indicates the effectiveness of the security actions employees undertake. The previous themes of threat evaluation, response evaluation, knowledge, experience, security responsibility and personal and work boundaries affect the degree to which an individual engages in high, medium or low-security hygiene.

High-security hygiene, refers to the most effective security behaviours and is defined as employees engaging in proactive security, using high prevention strategies, security citizenship and being able to identify appropriate deterrents. Medium security hygiene are somewhat effective security behaviours and is defined as medium prevention strategies. Low-security hygiene are the least effective security behaviours and are defined as low prevention strategies, little to no security citizenship and lack the ability to identify appropriate deterrents.

3.3.2.7.1 | Prevention strategies

"prevention is better than cure as they say.." [P14, Company 2]

Prevention strategies are behaviours employees engage in which contribute towards information security in the workplace and aim to prevent security breaches. For example, not downloading suspicious attachments, not clicking on suspicious links online, adopting strong passwords, locking computers, encrypting removable media and non-disclosure of sensitive information to name a few.

Employees who practice high-security hygiene take appropriate action and have a strong ability to engage in the correct security action and take fewer risks with their security behaviour. They

rely less on their organisation for security and have a more proactive stance towards information security. They can also correctly identify whether a physical or cyber security deterrent is most suitable for the security threat. For example, they will adopt encryption on removable media rather than rely on keeping it on oneself as a form of protection.

> *"Yeah I use a USB stick with encryption and it's just a bit of a reassurance because having in the past, I haven't lost a USB stick but I have not been able to* find it for a few hours, dunno where I have put and so feel a lot more comfortable now where there is using a USB stick with actually encryption on and knowing *that if it did disappear then, you know, there wouldn't be staff information going into the wrong hands.."* [P4, Company 1]

Those with medium security hygiene may take appropriate action and know which security actions are most suitable but engage in more risks with their behaviour such as creating a strong password and then writing it down or locking the desk cabinet but leaving the key located within the vicinity. They are less proactive in their stance towards information security and rely more on their organisation for security.

> *"*I put them in the filing cabinet but I *didn't* actually lock it but they were out of sight so I suppose that is as far as I went.. *I didn't lock but I do remember going I shouldn't just.. because they are so easy.. it's not like a computer or a laptop that* you would be seeing walking out with, the mobile phones were just too easy to pick *up so yeah I put them out of sight but I don't think I actually locked them"* [P10, Company 2]

Employees with low security hygiene, on the other hand, lack awareness of appropriate security actions and engage in inappropriate security behaviours. They rely heavily on "security defaults" such as using the default security password and relying on the computer to lock itself when leaving their desk. They are more reactive towards security needs as they rely on security enforcement by their organisation for their security behaviour. They lack awareness of appropriate security actions for physical or cyber security threats, as such, they may engage in non-technical deterrents when a cyber-security deterrent would be more beneficial.

> *"however the advantages are that I am much more consciously aware because 15-* 20 times a day I need to pick my keys up and I would notice if the USB.. because the USB stick is attached to a.. like a lanyard thing that goes around your neck so *if that was missing I would be really consciously aware of it.."* [P2, Company 1]

Their behaviours are considered more negligent as they may be aware of security actions but fail to engage or perform the behaviour.

"I have kind of blurred the lines a bit by having a laptop.. it mostly stays at home but when I do take it to work, it probably is sensible to have a password on but I just don't.. for ease of access.." [P6, Company 1]

3.3.2.7.2 | Security citizenship

This refers to actions individuals engage in which aid the organisation in business continuity and recovery. Individuals with high-security hygiene may engage in these practices such as backing up data, informing colleagues and IT of security issues.

"Well.. the phishing thing.. they are all set up.. I don't mess around with them, I just leave it as it is.. erm.. if I see anything dodgy I have emailed like IT before and made them aware of it and sent them the email" [P1, Company 1]

"Usually every day or night, I back up the files that I have updated.. the new files..

Is that useful?

I think s*o yeah.. better safe than sorry"* [P11, Company 2]

Individuals with low security hygiene, on the other hand, rely more on their organisation for business continuity practices and take less responsibility and action to aid the organisation.

"No.. that's the one thing that I am really a bit confused about, I don't know if there are like official procedures for backing up or if I should do it myself.." [P10, Company 2]

3.4 | CONCLUSIONS

Overall seven themes emerged through the use of this deductive approach that explains why employees engage and do not engage in security actions. The results of this study suggest that employees undergo a threat and response evaluation before undertaking behaviour. Knowledge and prior experience also influence an employees' security behaviour, as well as, their perceptions of responsibility and boundaries between personal and work. All these factors influence the degree to which employees engage in security behaviours; this study indicates that there are different levels of security behaviour characterised by prevention strategies and security citizenship.

There are key findings from each theme that are important for understanding the research question. Firstly from response evaluation, the study found that different behaviours have different associated costs that can be either cognitive, monetary expenses or affect productivity. Response evaluation also suggested that low response efficacy is a potential barrier to security behaviour. Secondly from threat evaluation, information sensitivity may influence whether

employees engage in protective actions. Employees' susceptibility perceptions depend on whether it is an online or offline threat and their threat severity concerns correspond to four domains (technology, personal, organisational and third party). Thirdly, security breach experience can lead to effective and ineffective responses and previous work experience can lead to security behaviour transfer between jobs. Fourthly, knowledge of security actions and risks is important for driving behaviour. Fifthly, personal and work boundaries play a role in risky behavioural engagement and provide an understanding of personal usage of company resources in the workplace. Sixthly, perceived responsibility for security appears to empower employees to engage in protective security behaviours. Finally, security behaviours were found to relate to hygiene levels comprising of protective actions and citizenships behaviours.

The current study has provided a number of contributions to the security research area and organisational practice. Firstly, the findings demonstrate that IS policy compliance is complicated as different security behaviours are motivated by different factors and to varying degrees. Where possible, future research should move away from using an IS policy compliance paradigm and focus on individual security behaviours. Likewise, organisational campaigns would benefit more from targeting specific security behaviours.

Secondly, response efficacy was shown to be a potential barrier to some security behaviours; response efficacy is low because employees lack feedback on how effective their security behaviour is at reducing threats. Systems rarely provide enough feedback or positive reinforcement to users on their proactive security behaviour although they sometimes provide information on their reactive behaviour (e.g. weak password or non-updated system). Systems need to provide more feedback on their efforts and provide information on the effectiveness of these for prevention of security threats. Furthermore, employees perceive that their security efforts may be in vain as they do not receive reinforcement from their organisation/management to keep up their behaviour. Research shows the importance of management feedback on employee performance (Hackman & Oldham, 1976) and the importance of positive reinforcement in shaping behaviour (Skinner & Ferster, 1997). One approach may be for organisations to include security behaviour as part of the performance appraisal of employees. As security is part of an employee's job role, it should be given more focus and feedback from the attention of management during day-to-day business operation and more specifically, as part of their employees' performance appraisal.

Thirdly, the current study showed that employees undergo an information sensitivity assessment, evaluating the sensitivity based on their perceptions of the value of the information and the audience for it. The study highlights differences in individuals' threat evaluation; employees' perceived susceptibility differs depending on off- and online threats. Within

information security research, off- and online threats are often given equal weighting or not specified. However, this study suggests that research needs to consider these as two separate information security issues (on- vs. offline) and campaigns need to focus on communicating susceptibility to these threats differently to employees and being specific when framing susceptibility questions. More work is required to provide concrete definitions of sensitivity levels, rather than it being determined in relation to other types of information. The following study will seek to explore this issue in more depth.

Fourthly, security responsibility was an emergent theme that suggested that employees perceived different responsibilities for security tasks, some of which they accept responsibility for and others they diffuse the responsibility onto their organisation. Organisations need to be more transparent to employees with regards to what they are expected to do and what is within their remit. Organisational policies dictate these responsibilities however they need to be embedded within the culture of the organisation. Finally, employees' personal/work boundaries may help explain risky behaviour in the workplace and adoption of BYOD has implications for these boundaries. These boundaries need to be explored further.

The initial deductive framework included the factors social pressures, attitude and self-efficacy however these did not emerge within the final framework. These three factors have consistently been found to relate to security behaviour as identified by the literature review. The current study found that attitude emerged more broadly across the other constructs rather than as a separate construct. For example, security responsibility and personal/work boundaries have attitudinal components within them. For social pressures, existing literature suggests that what people important to the user expect them to do influences their security behaviour (see section 2.2.6.1). However, the current study found that when discussing security behaviour, employees did not appear to be concerned about the behaviour of others and their line management, with regards to their motivations for behaving securely. However, this factor may play more of a larger component within the security culture of both of the organisations. Previous research has explored the role of security culture, which is the shared beliefs, norms, values and learned ways that have developed through the organisation's history (Brown, 1998) and are captured in the mission statements and the vision of the organisation as they represent the values they wish to be known for. A poor security culture is one where security is not built into these shared assumptions and is not part of "*the way things are done around here*". In the absence of a security culture, individual-level motivational factors may play more of an important role as information security is at the level of the employee rather than driven top-down and across the organisation. This may account for the lack of discussion about social pressures in the two participating companies. The study did find that employees use social influencers as a source of

information regarding security, so while they may not be influenced by normative security behaviour of others, they may seek guidance for their security concerns.

Another factor that has received attention within information security behaviour is the role of sanctions. The findings suggested that employees were not influenced by the fear and certainty of sanctions in the workplace. This is somewhat supportive of the existing literature as sanction severity is consistently related to security behaviour but sanction certainty is not. The lack of discussion and consideration of sanctions could be due to low sanction certainty in employees supporting the literature base that while employees perceive sanctions to be severe, the likelihood of being sanctioned may be low.

The lack of discussion of environmental influencers – social pressures and sanctions and no other emerging environmental factors indicates that internal influences may play a larger role in determining security behaviour. Environmental influencers may play a more implicit role in security but internal influencers (threat and coping appraisal) may be best able to explain security behaviours as indicated by the current study. The role of these internal factors will further explored in the following chapters.

The current study also aimed to address differences in psychological ownership and organisational citizenship behaviour between the two recruited companies. The analysis indicated that there was no significant difference between the two for psychological ownership of technology and data and organisational citizenship behaviours towards the organisation i.e. those behaviours that help aid the functioning of the organisation. The lack of significant difference for psychological ownership could be due to the type of companies recruited. Most employees from both organisations worked in a research capacity involving the development of their own ideas or research. Although the research institution, compared to the academic institution, has a more explicit intellectual property ownership policy, it could be that the level of input and effort on behalf of the employee accounts for more of their perceived ownership of their performance outputs rather than explicit policy. Furthermore, organisational citizenship refers to discretionary behaviours that go beyond the job role. The current study found that "security citizenship" was part of the security behaviour performed by employees and may be a form of OCB. Security citizenship refers to behaviours that go beyond the job role of the employees but help serve the organisational information security goal.

Despite the benefits of this approach for the furthering understanding of the causes of secure and insecure practice, the approach has its limitations. Self-efficacy proved difficult to assess within an interview context and this could be due to the construct itself and tapping into an individual's perceived capabilities of engaging in security tasks. Certain constructs may, therefore, prove difficult to tap into with an interview context, it may be more suitable to assess

these constructs within a questionnaire format to give an indication of the levels of these constructs within the target population.

The use of the deductive approach incorporated factors from many behaviour change theories which allowed the comparison of the final framework with existing theory. The final thematic framework of security behaviour is primarily PMT based with other security-contextual factors that may be able to explain additional variance in behaviour if it was to be explored quantitatively and with regression analysis. By exploring these constructs qualitatively, the study was able to explore what leads to high or low levels in these constructs and the individual, system and organisational components that may influence different perceptions. In doing this, it has provided better clarity of the use of PMT in security and may explain the disparate findings for PMT constructs (severity and response costs) in research. Future research will investigate components of the thematic framework to explore what influences security behaviours using structural equation modelling. This will give an estimation over which factors explain the most variance in intention and actual behaviour, this information will help provide the basis for future intervention efforts to influence the determinants of behaviour to bring about change. An iterative approach will be adopted to ensure full scope within the study; this will involve investigating the themes from the current study, supported factors in previous security research and other potential factors from behaviour change models.

The use of a deductive elicitation approach proved a useful application for exploring the factors that influence security behaviour. Refinement of the initial thematic framework through the qualitative data allowed the emergent factors to be driven fully from the data set and also allowed comparison to the behavioural determinants that were identified a priori from the existing literature. Furthermore using this approach allows exploration of theoretical constructs with target populations ensuring that beliefs and attitudes are data-driven rather than pre-determined by the research. This is important for behaviour change as it allows the data from the qualitative interviews to be used to develop a questionnaire to quantitatively determine the degree to which the constructs influence intention and actual behaviour.

Overall, the current study provided further understanding of the causes and barriers to secure behaviour. The use of a deductive approach proved useful to assess previously researched constructs and understand how these differ for different security behaviours. The findings will prove valuable for future intervention efforts.

3.5 | NEXT STEPS

Components of the thematic framework will be taken forward in future studies. In particular, an extended PMT model (see Figure 18) will be explored throughout the rest of the thesis comprising of the original PMT components: threat appraisal (severity and susceptibility) and

coping appraisal (response costs, response efficacy and self-efficacy). The model is extended to include additional factors of information sensitivity (WISA), security responsibility, and experience derived from this qualitative study and psychological ownership and organisational citizenship from the literature review.
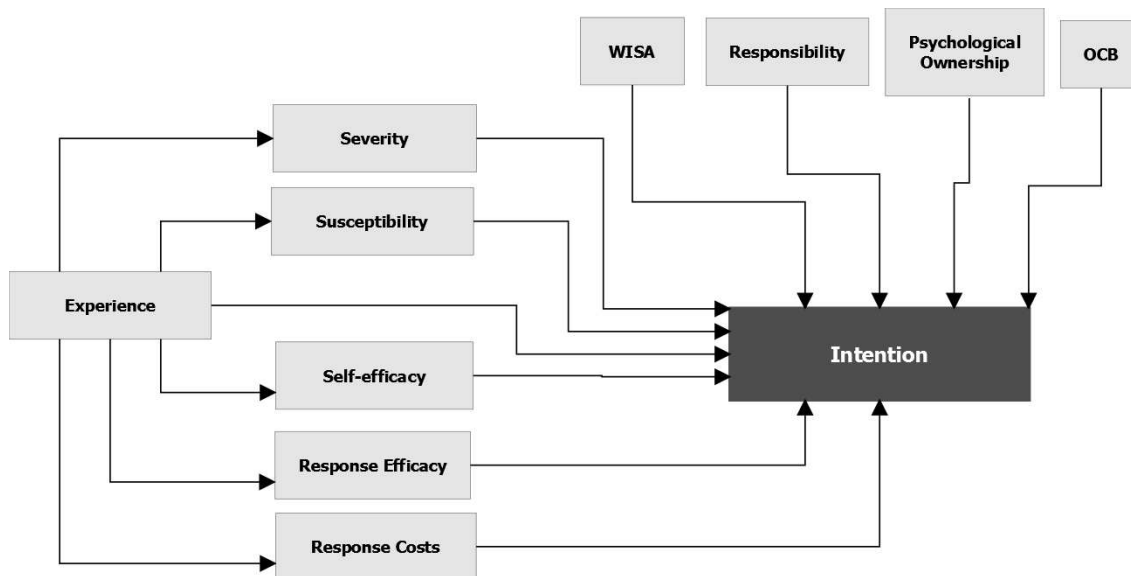
Figure 18. Extended-PMT model to be explored in thesis

Attention will be given to these factors as they are consistently under-researched and while appearing over-researched more work will also be given to understand the role of the PMT constructs; threat and coping evaluation with specific security threats and behaviours. The themes of knowledge and personal and work boundaries will not be taken forward in future studies. Knowledge will not be explored as it often an implicit part of many behaviour change models and not directly measured. Personal and work boundaries will also not be explored as this factor played more of a role in risk-taking behaviours, whereas future studies will focus on protective behaviours.

Prior to validating the extended-PMT model, a scale must be developed to assess information sensitivity and further explore its influence on security behaviours (Chapter 4). Following this, the model will be explored for its ability to predict engagement with three specific security behaviours (Chapter 5). Resulting from the findings of Chapter 3-5, the final study will assess whether the knowledge of the supported influencers from the model can be applied to an intervention (Chapter 6).

CHAPTER 4: DEVELOPMENT OF THE WORKPLACE INFORMATION SENSITIVITY APPRAISAL (WISA) SCALE

This chapter builds on the findings from Chapter 3 by developing a Workplace Information Sensitivity Appraisal (WISA) scale. There is currently a lack of empirical studies investigating information sensitivity and its role in employee security behaviour. There is also an absence of scales measuring how employees appraise information sensitivity. This chapter outlines the design, development and validation of the scale with an employment sample. To determine the validity of the scale, the factorial, content, discriminant and criterion-related validity were assessed. The scale was found to comprise of five subscales: Privacy, Worth, Consequences, Low proximity interest by others and High proximity interest by others.

The final 17-item WISA scale, alongside its five subscales, was found to have strong factorial validity which was confirmed across eight target information types. The scale was also found to have strong content validity, good criterion-related validity and adequate discriminant validity. Furthermore, the scale was found to have high internal reliability and represents a comprehensive measure of information sensitivity appraisal in the workplace.

The study also sought to explore sensitivity differences for company information pertaining directly to living individuals (personal, health, financial & lifestyle) compared to information that is organisationally-focused (intellectual property, day to day, commercial & HR). Financial information was found to have the highest ratings for sensitivity followed by health and HR. These information types were also found to be the highest for three of the five sensitivity subscales, in particular, Privacy, Worth and Consequences. Information about individuals (e.g. personal, health and lifestyle) was considered to be of significantly higher interest to employees' high proximity interest groups (i.e. family and friends) in comparison to organisational-focussed information. For low proximity interest, the opposite effect is apparent with organisational-focussed information perceived to be of interest (e.g. intellectual property (IP), day to day, commercial) to low proximity groups (i.e. criminals, fellow employees & business competitors). Finally, the findings indicated that the more an employee works with an information type did not influence their sensitivity ratings. There were, however, some differences in security behaviour dependent on data usage grouping.

This chapter starts by providing evidence of why an information sensitivity scale should be developed and then outlines the research questions explored in the study.

4.1 | INTRODUCTION

An under-investigated area is the role of information sensitivity appraisal in employees' protection efforts. Chapter 3 identified that employees appraise the sensitivity of the information that they work with and use this as a pre-cursor as to whether it needs protection. To explore this further, it is necessary to understand how individuals evaluate information sensitivity and how this may be linked to their security behaviours.

4.1.1 | WHAT IS INFORMATION SENSITIVITY?

There is no clear global definition of information sensitivity. In the UK, the protection of citizen's information is regulated by the Information Commissioner's Office and governed more specifically by the Data Protection Act (DPA; 1998). The act seeks to control how individuals' personal data is used in businesses by specifying different levels of protection required for personal data and sensitive personal data. Personal data refers to identifiable information such as name and sensitive personal data refers to information such as ethnicity, political opinions, religious beliefs, health, trade union membership, sexual health and criminal records. The DPA stipulates that these be considered sensitive due to:

> *"The presumption is that, because information about these matters could be used in **a discriminatory way**, and is likely to be **of a private nature**, it needs to be treated with greater care than other personal data"* (ICO, 2015).

Whilst in the US, there is much broader definition provided in the Computer Security Act of 1987 in which they define sensitive information as:

> *"any information, the loss, misuse, or* unauthorized access to or modification of which **could adversely affect the national interest** or the conduct of federal programs, or **the privacy to which individuals are entitled** under section 552a of *title 5, United States Code (the Privacy Act)…"* (Computer Security Act, 1987)

The US Federal Trade Commission considers sensitive information to be personal information. They have two primary categories; personally unidentifiable or personally identifiable information. Personally identifiable refers to information such as name, address, phone number and credit card information whereas unidentifiable refers to information such as gender, age, and occupation (FTC, 2015).

Within the research domain, the majority of studies do not provide a clear definition. However, there are two clear divides in the way that research has conceptualised information sensitivity. Some conceptualizations focus on the privacy and intimacy of information as a basis for evaluating sensitivity. For example, Weible (1993) defines it as "the level of privacy concern an individual feels for a type of data in a specific situation" (p.30). Sheehan and Hoy (2000)

present a broader definition and argue that information sensitivity is simply the distinction between what is private and what is not private. Other researchers consider sensitivity to relate to intimate self-disclosures. Lwin, Wirtz, and Williams (2007) define information sensitivity as the perceived intimacy level of information and Moon (2000) defines intimate self-disclosures as those information types that are high-risk and heighten vulnerability if disclosed. The second type of definition focuses more on the vulnerability and potential exploitative nature of information as a basis for evaluating sensitivity. For example, Gandy (1993) argues that some people view sensitive information as any information that if disclosed would cause harm. Mothersbaugh, Foxx, Beatty, and Wang (2012) also define sensitivity as potential losses associated with disclosing information.

The disclosure of certain types of information can have many negative effects towards individuals such as potentially opening them to discrimination, identity theft or have their access controls exploited on systems and services. Security is, therefore, a requirement to maintain the confidentiality of sensitive information.

4.1.2 | INFORMATION SENSITIVITY AND PRIVACY

The majority of research investigating the role of information sensitivity has explored its links to individuals' privacy concerns and their willingness to disclose information. Bélanger and Crossler's (2011) critical review of research on information privacy discusses the many definitions of privacy and information privacy specifically. They acknowledge that definitions of privacy can include the consideration of moral and legal rights with regards to the information or concern an individual's ability to control their information. They conclude with a broad definition by Clarke (1999) which defines information privacy as "the interest an individual has in controlling, or at least significantly influencing the handling of data about themselves".

Research (Adams & Sasse, 2001; Mothersbaugh et al., 2012; Phelps, Nowak, & Ferrell, 2000) suggests that information sensitivity works along a continuum of "willing to disclose" to "not willing to disclose" and that individuals do not make simple binary judgements of sensitivity. On this sensitivity continuum participants are most willing to disclose demographic (e.g. age, marital status and occupation) and lifestyle (favourite pastimes) information. They are less willing to disclose purchase-related or lifestyle-related information (e.g. recent credit purchases) and least willing to disclose personally identifiable or financial information (e.g. telephone number, social security number).

Research suggests that willingness to disclose may be linked to perceived risks associated with that information, with more sensitive information indicative of greater risks and losses. Malhotra, Kim, and Agarwal (2004) found that individuals' perceived risk of disclosure differed

depending on the sensitivity of the information. Sensitive personal information (e.g. financial data) had higher risks associated with disclosure than less sensitive information (e.g. product preferences). Highly sensitive personal data such as identifiable or financial information is open to exploitation and can lead to identity theft, which may explain the increase in protective measures taken by consumers in limiting their disclosure of this information.

Previous research has largely focussed on individuals' willingness to disclose different types of sensitive information (Cranor, Reagle, & Ackerman, 1999; Phelps et al., 2000). It is clear from research that individuals are more open to disclosing information that is less identifiable (such as lifestyle) than more personal information (such as health and financial). With the exception of a study by Malhotra et al. (2004) who focussed on risks of disclosure linked to information sensitivity, there is less research exploring if and how individuals appraise the sensitivity of information.

Furthermore, studies traditionally focus on individuals' own information however employees regularly work with information belonging to others and must abide by organisational and legislative regulations in the security and disclosure of this information. It is, therefore, important to understand how employees evaluate the sensitivity of information belonging to others and their organisation.

4.1.3 | INFORMATION SENSITIVITY AND SECURITY

There has been limited research exploring the direct link between information sensitivity and security in the workplace. Adams and Sasse (1999) found that employees perceived sensitive information within the workplace to require more protection and security. They found that confidential information about individuals (personnel files, emails) were rated as sensitive, whereas commercially-orientated information (such as customer databases and financial data) were often seen as less sensitive and consequently needing less protection.

The sensitivity of data has been found to have no effect on password length and composition (Zviran & Haga, 1999) but does have an impact on password re-use (Grawemeyer & Johnson, 2011). These findings suggest that users do consider the sensitivity of the data stored on a service and adjust their security behaviour accordingly.

The findings from the qualitative study (reported in Chapter 3) found that employees appraise the sensitivity of their work information by considering the perceived value of the information and the perceived interest to others. Health and financial information were deemed to be more sensitive than organisational data such as intellectual property and required more protection and security.

4.1.4 | STUDY FOCUS

4.1.4.1 | Research Aims

The study has two aims, the first aim is develop and validate a new measure exploring employees' evaluation of information sensitivity called the Workplace Information Sensitivity Appraisal (WISA) scale. The second aim is to then apply this scale to explore differences in information sensitivity and security behaviour for different information types, participants' knowledge about legal and organisational regulations applying to the information types and their frequency of data usage.

Specifically, the research steps involved to address these aims are to:

- Explore the underlying factor structure of the WISA scale
- Test the content, discriminant and criterion-related validity of the scale
- Ascertain the reliability of the scale
- Explore differences in WISA ratings for different information types
- Identify differences in sensitivity ratings for different information types and security behaviour based on participant perceptions of legal and organisational regulations and their frequency of data usage

4.1.4.2 | WISA scale development

There is currently no scale that measures information sensitivity within the workplace. Previous studies exploring information sensitivity have largely used scales investigating willingness to disclose (e.g. Cranor et al., 1999) or privacy concerns (e.g. Buchanan, Paine, & Joinson, 2007; Preibusch, 2013). However none of these explicitly investigate how individuals appraise sensitivity.

Previous research and the qualitative study in Chapter 3 identified four aspects of information sensitivity appraisal: the private nature of information, potential consequences associated with information, the value of information, and perceived (third party) interest in information.

The WISA distinguishes between two general types of information. The first is information about living individuals replicating the four information types used by Little, Briggs, and Coventry (2011). These four types are: personal information (e.g. address, gender, date of birth, marital status), health information (e.g. physical and mental health history, weight, family medical history), financial information (e.g. banking details, credit rating, loan history) and lifestyle information (e.g. shopping habits, hobbies, interests). However, the focus of the items has been changed to other individuals' information, rather than the employee's own information. The second refers to organisationally-owned information in which there are also four types: intellectual property (e.g. trade secrets, creative ideas that could lead to patents,

copyrights, new products), day-to-day business information (e.g. current customer & supplier details, quotes, purchase history, call records), commercial information (e.g. strategic plans, business financial data) and personnel/HR information (e.g. appraisal, disciplinary information, salary, sickness records).

As discussed earlier, individuals do not perceive organisational data as being as sensitive as personal information. By exploring principles of sensitivity analysis of personal and organisational information, it may identify reasons why individuals do not perceive such information as sensitive and if this affects their security behaviour.

4.2 | METHOD

4.2.1 | DESIGN

A non-experimental survey design was employed. The following approach (summarised in Figure 19) was used to explore the validity and reliability of the scale, following recommendations by Hinkin (1995, 1998). The specific forms of validity explored were: content, factorial, discriminant and criterion-related.

Stage 1: Face/Content Validity
Subject-matter experts and participants determine the suitability of items

Stage 2: Exploratory Factor Analysis (EFA)
Exploring the underlying factorability of the scale items and their associations with the constructs

Stage 3: Confirmatory Factor Analysis (CFA)
Testing the hypothesised factorial structure and estimating the degree to which it is a good fit to the sampled data

Stage 4: Discriminant Validity
Testing whether the WISA scale is unrelated to dissimilar constructs

Stage 5: Criterion Related Validity
Identifying the predictive power of the WISA scale on security behaivour

Stage 6: Reliability of measures
Determining the internal consistency of the WISA scale

Figure 19. The process of assessing the validity and reliability of the WISA scale

Content validity refers to the extent to which items within the scale represent the construct being measured (Hinkin, 1995) which can be further broken down into face validity and item validity. Face validity is whether the items are relevant, important and interesting to respondents (Onwuegbuzie, Daniel, & Collins, 2009), whereas item validity is the extent to which the items in the measure represent the intended construct (Onwuegbuzie et al., 2009). The content validity of the scale will be assessed using subject-matter experts and naïve participants to evaluate the suitability and comprehensibility of items.

Factorial or structural validity refers to how well the scoring structure of the tool corresponds to the domain of interest by assessing the composition of the scales (Onwuegbuzie et al., 2009). The factorial structure of the WISA appraisal will be undertaken to explore the four aspects of the WISA appraisal using exploratory factor analysis (EFA) and confirmatory factor analysis (CFA).

The discriminant validity of a scale refers to whether it is unrelated to similar, yet distinct constructs (Onwuegbuzie et al., 2009). To assess the discriminant validity of the WISA scale, organisational citizenship behaviour (OCB-O) was identified as an organisational construct that may be linked to sensitivity appraisal. An organisational behaviour was chosen because individuals who have high citizenship behaviours are involved in more activities that promote optimal functioning of their organisation (Organ, 1988). They comply with organisational rules and procedures (Borman & Motowidlo, 1997, 1993), which may include reading organisational policies about information security and information classification. However, it is theoretically distinct from information sensitivity so should not highly correlate with the WISA scale and may help demonstrate the discriminant validity of the scale.

Criterion-related validity is the extent to which the developed tool is related to the variable to which it is hypothesised to relate (Hinkin, 1998). As the current study is interested in the link between sensitivity appraisal and information security behaviour, the criterion-related validity of the scale was also measured using a self-report security behaviour questionnaire based on best practices for security identified in a report for Department of Business, Innovation and Skills (Coventry et al., 2014).

4.2.2 | PARTICIPANTS

An opportunity sample of 326 (Age, M= 31.75, SD= 11.51) individuals were recruited online. All recruited participants were currently in full time or part time employment or unemployed for less than 3 months. 87 males and 217 females (22 participants chose not to disclose their gender) took part with an average organisational tenure of 5.23 years (SD=6.66) and job tenure of 3.18 years (SD 4.7). 11% (34) were from a microenterprise (less than 10 staff), 13% from a

small enterprise (less than 50 staff), 9.2% from a medium-sized enterprise (less than 250 staff) and 61% from a large organisation (more than 250 staff). Appendix E presents the organisational sectors recruited participants were sampled from.

Participants were recruited using a variety of platforms based on recruitment recommendations from Branley, Covey, and Hardey (2014) which included dedicated participation sites (e.g. callforparticipants.com), social media (e.g. Facebook, Twitter, LinkedIn), mailing lists, student participation pools and websites and forums. Snowballing sampling technique was used to recruit participants in order to maximise recruitment, this involved encouraging participants to share the study with their acquaintances such as retweeting the study link on Twitter or sharing the recruitment advertisement on Facebook. In compensation for study completion, participants were entered into a prize draw to win an iPad or if they were university psychology students, they received institutional participation points.

4.2.3 | SCALE CONSTRUCTION

4.2.3.1 | Item generation and reduction

Existing literature on information sensitivity was consulted to aid item generation. This deductive approach outlined by Hinkin (1998) is deemed most suitable when there are sufficient theoretical grounds to base the generation of items on. However, given the lack of previous research on information sensitivity, specifically in the workplace, this approach was not used in isolation.

Therefore, the current study used a combination of inductive and deductive approaches to enhance item generation. As discussed earlier, an employee's information sensitivity appraisal comprises of the privacy, exploitability, value and perceived interest in the information. Using this definition, items were first generated using the quotes from the interviews with employees reported in Chapter 3. This allowed the dimensions to be clearly defined. This also helped ensure that the language used in the items was familiar to target respondents. Items were further developed based on recommendations by Hinkin (1998) including the use of short and simple items, avoidance of "double-barrelled" items and leading questions. Reverse-scored items were also included to help reduce response bias. Following this, items were further generated using the deductive approach. Existing literature on information sensitivity was explored. The WISA scale was validated across 8 information types. 4 types of sensitive information were taken from Little et al. (2011) and an additional 4 were added to include workplace specific information. Following the generation of items by the lead researcher, these were reviewed and modified by other members of the research team.

4.2.4 | MEASURES

Alongside the WISA questionnaire, participants also completed an existing measure of organisational citizenship behaviour so that discriminant validity could be assessed and a measure of security behaviour to assess criterion validity. Both scales are measured on a 7 point scale ranging from 1 (never) to 7 (always) for which participants indicated the extent to which they perform the behaviours. Participants' knowledge of legal and organisational requirements for information was also measured and on a 3 point scale: 'yes', 'no' or 'I do not know'.

4.2.4.1 | Organisational citizenship behaviour

This behaviour was measured using the same OCB-O subscale (Appendix A) by Lee and Allen (2002) as used in Chapter 3. The scale of OCB-O had strong internal reliability, Cronbach's α = .89.

4.2.4.2 | Security behaviour

Security behaviour was measured using a 16 item self-developed scale based on best practice security behaviours identified in the report for the Department for Business, Innovation and Skills (Coventry et al., 2014). Behaviours were worded to explicitly target the workplace setting (e.g. I share passwords with other people at work). The behaviours comprised access control, software updates, anti-malware, physical behaviours and reporting behaviours. The scope of the scale was broad to encompass the different working conditions employees may face. The security behaviour scale had strong internal reliability, Cronbach's α = .85. A copy of the scale can be found in Appendix I.

4.2.4.3 | Knowledge of legal and organisational requirements for information

For information types that participants worked with as part of their job role, they were also asked if they thought the information was (1) publicly available outside of my organisation, (2) access restricted by my organisation and (3) regulated by law. See Appendix F for scale.

4.2.5 | PROCEDURE

Table 9. Presentation of questionnaire sections and associated appendices

Section 1	Section 2	Section 3	Section 4	Section 5
Evaluation of the 8 information types using the WISA scale	Frequency of information usage and OCB scale	Knowledge of legal and organisational requirements of information that they stored and processed as part of their job role	Security behaviour questionnaire	Demographic information
Appendix G	Appendix H & Appendix A	Appendix F	Appendix I	Appendix J

Participants took part individually and were provided with a link to the online survey that was hosted on the Qualtrics website. The online survey first provided participants with information outlining the study requirements and exclusion criteria. Participants generated a unique code should they wish to withdraw at a later date and they then consented to take part in the online questionnaire. The online questionnaire was split into five sections. In section 1, participants evaluated the sensitivity of the 8 different types of information. Section 2 required participants to indicate the degree to which they work with each of the information types and they completed the OCB scale. Section 3 was tailored to participants' responses in section 2 where they were asked about their knowledge of legal and organisational requirements of information that they stored and processed as part of their job role. These were any information types that they worked with at least "rarely". Section 4 comprised the security behaviour questions which were presented to participants who used a computer as part of their daily work tasks, again at least "rarely". Section 5 requested demographic information from participants. Following completion of all five sections, participants provided their email address to be entered into the prize draw; this information was stored in a separate database to ensure the questionnaire data remained anonymous. Participants were then presented with debrief information. The online survey provided participants with the option to print or save a pdf version of the participant and debrief information to refer to at a later date.

4.3 | RESULTS

4.3.1 | CONTENT VALIDITY (STAGE 1)

The content validity of the scale was assessed using subject-matter experts as well as naïve participants to evaluate the suitability and comprehensibility of items. A workshop with subject-matter experts revealed that the items were suitable for measuring the construct of information sensitivity, however, concerns were raised regarding the information types targeted. Initially, two broad information types (organisational vs. individual) were used to compare potential differences in their sensitivity ratings. It was decided following the sessions that eight types were to be investigated as these adequately reflected the information types that employees may experience within their job role. Furthermore, targeting eight different information types would allow for greater comparison to previous research. Following the session, a consistent rating scale "strongly disagree to strongly agree" was implemented across the 4 areas of the WISA appraisal as research has highlighted issues in combining scores from different rating scales (Gliem & Gliem, 2003).

Ten participants were recruited as naïve subjects to assess the items. In a card sort activity, they were presented with the questionnaire items and asked to sort the items into clusters they felt most represented that collection of items. This followed a similar technique to that used by

MacKenzie, Podsakoff, and Fetter (1991). Participants were asked to define their categories, definitions were not provided to participants as it was hoped that this approach would provide better clarity over how the constructs could be defined and would not be a purely cognitive sorting task akin to traditional card sorting with definitions (Anderson & Gerbing, 1991). Participants were also asked to read the questionnaire instructions and items, and comment on the clarity and complexity of them, and highlight any potential issues. Finally, participants were asked to provide additional examples of types of information they would classify under the 8 target information types. 60% of participants sorted the items into the same constructs as the current study, this falls below the acceptable agreement index of 75% (Hinkin, 1998). This was to be expected as participants were not provided with the definitions. Therefore, another 4 participants were recruited to conduct the card sort with definitions in which 100% sorted them into their respective factors. Changes were made to instructions and definitions of the information types following the one-to-one sessions to improve the usability and comprehensibility of the questionnaire.

4.3.2 | DATA SCREENING AND CLEANING

Data was checked for errors before EFA. Six participants were removed due to incomplete data. Missing values analysis was conducted on the dataset and the findings revealed that the average percentage of missing data for the WISA scale items was 0.3%, indicating the amount of missing data was low. To retain as much data as possible, pairwise data deletion was subsequently used to retain data cases.

4.3.3 | ANALYSIS OF THE WISA STRUCTURE: FACTORIAL VALIDITY (STAGE 2 & 3)

Testing the factorial validity of the WISA scale involved two stages to assess its underlying structure. The first stage was EFA to explore its potential structure and the second stage was to confirm its structure using CFA. The data file was therefore first split into two so that EFA could be performed on one half and CFA on the other as recommended by Thompson (2004).

Following this, two statistical tests were conducted to determine the suitability of the dataset for factor analysis. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and the Bartlett tests of sphericity (BS) were calculated. KMO indicates the suitability of the data to factor analysis by exploring correlations between the variables. The analysis revealed that the KMO output was .86 indicating a "good" sample adequacy (Kaiser, 1974). The BS also assesses whether the data meets the requirements for factorial analysis and a significant finding indicates an appropriate sample. The BS test showed a significant result (BS x^2 (231) = 5586.27, p<.001). The findings from both tests, therefore, suggested that the data was suitable for EFA.

4.3.3.1 | Exploratory factor analysis (Stage 2)

To explore the factor structure of information sensitivity appraisal, Principal Component Analysis (PCA) was performed using varimax with Kaiser normalization. The 21 items of the original scale were entered into the factor analysis and factor loadings lower than 0.30 were suppressed.

Table 10. Factor loadings for each item (factor loadings lower than .30 are suppressed)

Item	Rotation Factor Loadings				
I think <information type> is…	Factor 1: **Privacy**	Factor 2: **Worth**	Factor 3: **Consequences**	Factor 4: **Low proximity interest**	Factor 5: **High proximity interest**
…confidential	.897				
…private	.898				
…secret	.850				
…restricted	.761				
…privileged	.656				
…insignificant*		.834			
…meaningless*		.895			
…worthless*		.890			
…embarrassing			.869		
…compromising			.753		
…discreditable			.656		
… humiliating			.866		
…of interest to my friends					.941
…of interest to my family					.946
…of interest to business competitors				.895	
… of interest to criminals				.861	
…of interest to fellow employees				.755	.360
Eigenvalues	**4.89**	**3.37**	**2.72**	**1.52**	**1.06**

REMOVED FACTORS					
…sensitive	.723	.451			
…valuable	.433	.733			
…important	.553	.685			
…exploitable		.359	.601	.359	
… of interest to the general public				.670	.514

*Reversed scored

The findings from the PCA revealed that five factors (eigenvalues were above 1) could explain the data accounting for 79.73% of the variance. This complied with the minimum acceptable

level of 60% variance and recommendations of eigenvalues above 1 for factors (Hinkin, 1998). All items loaded onto their expected factor above the accepted .40 criterion level.

The fourth-factor *"interest by others"* was found to be two distinct factors. Theoretically, this seems plausible as the factor contained various targets including family, friends, the general public, fellow employees, business competitors and criminals. Factor four from the PCA contained those targets that may be considered to be low proximity to individuals (i.e. business competitors, criminals and fellow employees). Factor five, on the other hand, contained those targets which are in high proximity to individuals (i.e. family and friends).

The PCA revealed five items that cross-loaded onto multiple factors and these were removed (see Table 10) as their values were above 0.4 (Hinkin, 1998). "I think <information type> is of interest to fellow employees" was left in the analysis as the cross-loading was less than .40 on the second factor (Hinkin, 1998).

Overall, the PCA revealed that the five factors explained a large amount of the variance in the data and the items had strong factor loadings (above .40). The next stage was then to confirm this structure using CFA.

4.3.3.2 | Confirmatory factor analysis (Stage 3)

CFA was carried out on the data using AMOS (version 22) to explore the hypothesised factor structure and estimate the degree to which the model was a good fit to the data. The five factors were presented as latent variables within AMOS and were permitted to co-vary. The items for each factor were only allowed to load onto their respective factor. Covariance between error terms was only allowed where items were related to the same factor; this followed advice from modification indices within AMOS. The item "privileged" was removed as it shared too much covariance across factors, had the lowest factor loadings and was deemed non-specific within the privacy factor. Figure 20 shows the average standardised item loadings for the hypothesised model.
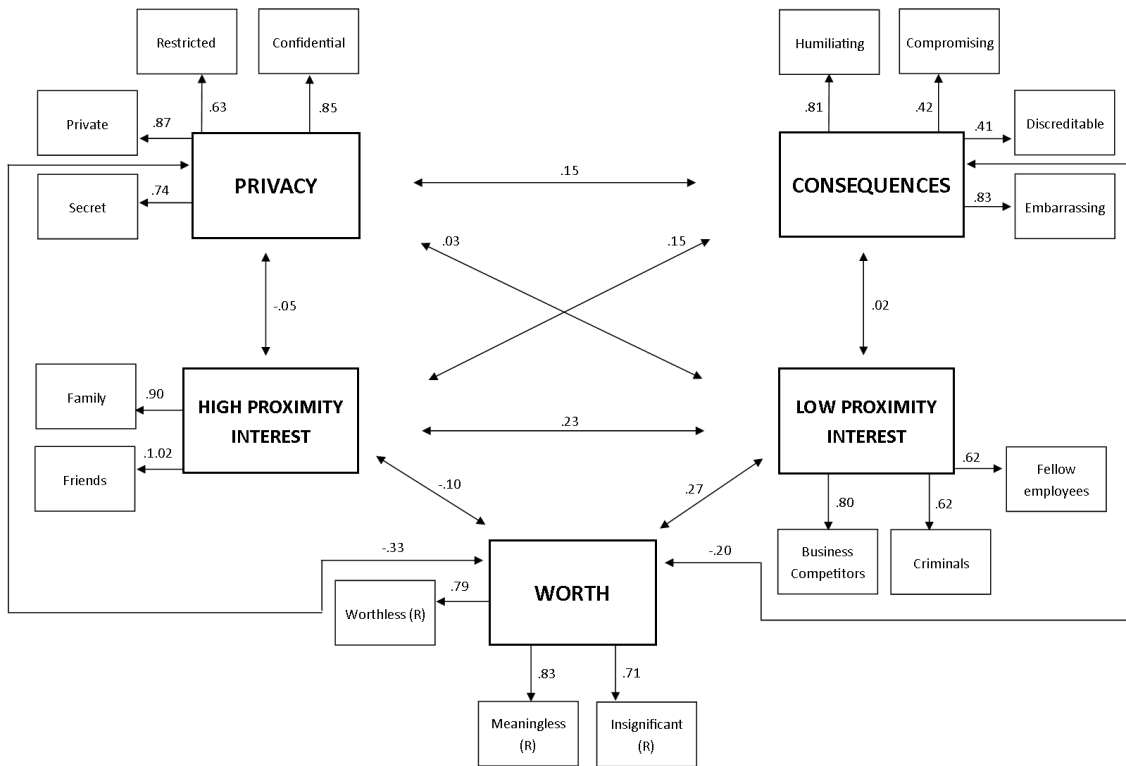
Figure 20. WISA Appraisal Confirmatory Factor Analysis with average Item Loadings (standardised path coefficients)

Maximum likelihood estimation methods were used and the input for each analysis was the covariance matrix of the items. The goodness-of-fit for the models was evaluated with the following absolute goodness-of-fit indices (Jöreskog & Sörbom, 1986): (1) the X^2 goodness-of-fit statistic; (2) the Root Mean Square Error of Approximation (RMSEA); (3) the Goodness of Fit Index (GFI); (4) the Adjusted Goodness of Fit Index (AGFI). Non-significant X^2 values indicate that the hypothesised model fits the data and RMSEA values smaller than or equal to .08 are indicative of acceptable fit. However, values above 0.1 should lead to model rejection (Browne & Cudeck, 1992). GFI values greater than .95 are indicative of good fit and values greater than .90 are indicative of an acceptable fit (Marsh & Grayson, 1995). AGFI values of .90 are indicative of a good fit and values greater than .85 may be considered an acceptable fit (Hu & Bentler, 1995).

Table 11. Goodness-of-fit indices for WISA appraisal for 8 target information types

Information type	X^2	RMSEA	GFI	AGFI
Personal	x^2(92)=201.456, p<.001	.061	.926	.890
Health	x^2(92)=211.818, p<.001	.065	.921	.883
Lifestyle	x^2(92)=216.460, p<.001	.065	.928	.893
Financial	x^2(92)=252.166, p<.001	.073	.907	.862
Intellectual Property	x^2(92)=179.095, p<.001	.054	.939	.910
Day to Day	x^2(92)=170.270, p<.001	.051	.941	.913
Commercial	x^2(92)=223.679, p<.001	.066	.923	.887
HR	x^2(92)=189.792, p<.001	.057	.931	.898

The final model (see Figure 20) indicated an acceptable level of fit for three of the four fit indices and this was evident across all 8 information types (see Table 11). The fit indices for GFI and AGFI were all above .9 and .85 and the RMSEA were all below .08. The chi-square indicated that the model was not a good fit to the data for all information types, however, chi-squared has been criticised for being too sensitive to large sample size, especially for samples over 200 (Hoe, 2008), as in the current study. Regarding the information types, the model had the best fit for intellectual property and the least best fit for financial information. However, it was an acceptable fit for all types. Therefore, the WISA appraisal was considered to be an acceptable model to explain the data that it was tested on.

Table 12 shows the standardised regression weights for the latent variables for each information type. See Appendix G for the final WISA scale.

Table 12. Standardised regression weights for latent variables per information type and overall means (& SDs)

	Privacy <> Worth	Privacy <> Consequences	Privacy <> High proximity interest	Privacy <> Low proximity interest	Consequences <> High proximity interest	Consequences <> Low proximity interest	Consequences <> Worth	High proximity interest <> Low proximity interest	Worth <> High proximity interest	Worth <> Low proximity interest
Personal	.29	.13	-.01	.03	.08	.05	-.21	.24	-.03	.24
Health	.44	.17	-.02	.01	.15	.12	-.08	.28	-.01	.22
Lifestyle	.09	.34	-.09	-.02	.07	.07	-.01	.23	.00	.22
Financial	.41	.05	-.15	-.14	.03	-.05	-.05	.55	-.08	.21
IP	.47	-.02	-.07	.18	.32	-.13	-.50	.13	-.16	.43
DTD	.27	.13	-.07	.08	.28	-.03	-.40	-.03	-.20	.32
Comm	.27	.10	.01	.07	.22	-.01	-.44	.03	-.25	.32
HR	.42	.28	-.05	.04	.07	.17	.07	.39	-.06	.18
Mean (SD)	**.33 (.13)**	**.15 (.12)**	**-.05 (.05)**	**.03 (.09)**	**.15 (.11)**	**.02 (.10)**	**-.20 (.22)**	**.23 (.19)**	**-.10 (.09)**	**.27 (.08)**

Table 13. Standardised regression weights for scale items per information type and overall means (& SDs)

| | PRIVACY -> | | | | CONSEQUENCES -> | | | | WORTH -> | | | LOW PROXIMITY INTEREST -> | | | HIGH PROXIMITY INTEREST -> | |
	Confidential	Restricted	Private	Secret	Humiliating	Compromising	Discreditable	Embarrassing	Insignificant	Worthless	Meaningless	Business Competitor	Fellow Employee	Criminals	Friends	Family
Personal	.84	.63	.92	.65	.74	.39	.53	.75	.62	.74	.78	.73	.62	.55	1.07	.90
Health	.86	.62	.86	.64	.81	.56	.39	.86	.72	.74	.77	.82	.70	.63	1.09	.84
Lifestyle	.84	.71	.85	.79	.85	.61	.39	.82	.71	.81	.74	.72	.55	.66	1.02	.94
Financial	.83	.56	.73	.61	.73	.40	.39	.96	.69	.73	.89	.77	.81	.56	1.07	.81
IP	.86	.70	.85	.83	.87	.29	.38	.77	.73	.79	.79	.88	.62	.75	.97	.92
DTD	.87	.59	.91	.81	.80	.30	.45	.78	.78	.86	.93	.83	.50	.61	.92	1.01
Commercial	.86	.61	.93	.88	.81	.24	.37	.81	.72	.86	.92	.78	.51	.65	1.04	.89
HR	.82	.63	.93	.73	.90	.59	.38	.82	.72	.80	.82	.86	.68	.58	1.01	.86
Mean (SD)	**.85 (.02)**	**.63 (.05)**	**.87 (.07)**	**.74 (.10)**	**.81 (.06)**	**.42 (.15)**	**.41 (.05)**	**.82 (.07)**	**.71 (.04)**	**.79 (.05)**	**.83 (.07)**	**.80 (.06)**	**.62 (.11)**	**.62 (.07)**	**1.02 (.06)**	**.90 (.06)**

4.3.4 | OBTAINING AN EMPLOYEES WISA SCORE

An employee's WISA score is calculated by taking the scores for all 5 WISA aspects for the information type they indicated they worked with most regularly (or the average if more than one).

4.3.5 | DISCRIMINANT AND CRITERION-RELATED VALIDITY (STAGE 4 & 5)

Table 14. Descriptive statistics for OCB and security behaviour

Factor	Mean (& SD)	N=
OCB – total	35.6 (9.2)	310
Security behaviour – Total	54.9 (11.1)	293
I share passwords with other people at work*	4.5 (.8)	292
I use trusted and secured connections, and devices (including Wi-Fi) when at work	4.1 (1.1)	292
I log out of websites when I finish at work	4.0 (1.3)	293
I use trusted and secure websites and services at work and connect securely	4.0 (1.1)	293
I am aware of my physical surroundings when online at work	4.0 (1.0)	293
I lock my computer when I leave my workstation	3.9 (1.3)	293
I avoid security risks online and in the workplace	3.9 (1.2)	292
I use complex passwords at work	3.6 (1.2)	293
I use different passwords for different work accounts	3.4 (1.4)	293
I stay informed about security risks online and in the workplace	3.4 (1.2)	293
I ensure I run the latest and official version of software (including operating system) at work	3.2 (1.4)	293
I report suspicious or criminal activities in the workplace	3.2 (1.4)	290
I personally back up data on my workplace devices	2.8 (1.5)	293
I adjust account settings on websites that I use at work	2.5 (1.3)	293
I personally run the security software including anti-virus, anti-spyware and firewalls at work	2.2 (1.4)	293
I personally scan work devices for available software updates and install them at work	2.1 (1.3)	292

*Reversed scored

Table 14 indicates that employees report engaging in not sharing passwords, using trusted and secured connections and services and logging out of websites the most. The means also suggest that employees are less likely to adjust account settings, personally scan for available software updates and run security software.

The WISA scale was explored to identify whether it was unrelated to OCB (discriminant validity) and the degree to which it can predict a composite measure of security behaviour and the individual security behaviours.

4.3.5.1 | Discriminant validity (Stage 4)

The findings revealed that 3 of the 5 aspects of the WISA scale were unrelated to organisational citizenship behaviour, therefore, providing partial support for discriminant validity for the WISA scale.

Table 15. Correlations between WISA components and OCB (n=284)

Predictor variable	1	2	3	4	5	6
1. WISA Privacy	-					
2. WISA Worth	.361**					
3. WISA Consequences	.209**	-.098				
4. WISA High Proximity	.032	-.041	.159**			
5. WISA Low Proximity	.071	.239**	.045	.193**		
6. OCB	.137*	149*	.021	-.039	.043	-

*p<.05; **p<.01

4.3.5.1.1 | Criterion-related validity (Stage 5)

Multiple regressions were performed to explore the predictive validity of the WISA scale in explaining security behaviour. The multiple regression revealed that $R^2 = .089$, $F(5, 287) = 5.586$, $p < .001$ indicating that the WISA scale accounts for 8.9% of the variance in the composite measure of security behaviour. 3 (Worth, Consequences & Low proximity) of the 5 WISA components were found to significantly contribute to the prediction, of which worth contributed the most.

Table 16. Tests of significance for the predicted variable of security behaviour from the predictors of the WISA appraisal

Predictor variable	β	B	SE B	P
WISA Privacy	.100	1.454	.918	p=.114
WISA Worth	.143	2.562	1.138	p<.05*
WISA Consequences	-.125	-1.887	.906	p<.05*
WISA High Proximity	-.075	-.729	.578	p=.208
WISA Low Proximity	.140	1.616	.692	p<.05*

*p<.05; **p<.01

Further analyses were conducted to estimate the degree to which the WISA scale predicts individual security behaviours. As shown in Table 17, the WISA scale best predicts security behaviours relating to access control and physical security.

Table 17. Regressions with specific security behaviours and the variance explained

Behaviour	Regression	Variance explained
I use complex passwords at work	$R^2 = .106$, $F(5, 287) = 6.807$, $p < .01$.	10.6%
I use different passwords for different work accounts	$R^2 = .056$, $F(5, 287) = 1.115$, $p < .01$.	5.6%
I use trusted and secured connections, and devices (including Wi-Fi) when at work	$R^2 = .086$, $F(5, 286) = 5.361$, $p < .01$	8.6%
I use trusted and secure websites and services at work and connect securely	$R^2 = .075$, $F(5, 287) = 4.670$, $p < .01$	7.5%
I stay informed about security risks online and in the workplace	$R^2 = .050$, $F(5, 287) = 3.019$, $p < .05$	5%
I avoid security risks online and in the workplace	$R^2 = .068$, $F(5, 286) = 4.198$, $p < .05$	6.8%
I am aware of my physical surroundings when online at work	$R^2 = .099$, $F(5, 287) = 6.281$, $p < .01$	9.9%
I adjust account settings on websites that I use at work	$R^2 = .040$, $F(5, 287) = 2.384$, $p < .05$	4%
I lock my computer when I leave my workstation	$R^2 = .032$, $F(5, 287) = 1.897$, $p = .095$.	3.2%

Overall, the WISA scale explains a proportion of the variance in security behaviour, therefore, demonstrating strong criterion-related validity.

4.3.6 | INTERNAL RELIABILITY (STAGE 6)

The final WISA scale comprises of 17 items. The majority of items demonstrated an acceptable alpha level normally deemed to be 0.70 or above (Hinkin, 1998; Kline, 1999). A few items fell short of this .70 level (e.g. Day-to-day- WISA Low Proximity Interest). These items were still above the .65 level considered to be at the lower end of the acceptable level for new scales (Hair, Anderson, Tatham, & Black, 2006).

Table 18. Reliability statistics for each WISA total and the WISA subscales across 8 information types

	Factor	No. of items	R (α =)	N=
Personal	WISA Total	16	.70	319
	WISA Privacy	4	.85	326
	WISA Worth	3	.75	326
	WISA Consequences	4	.69	326
	WISA High Proximity Interest	2	.98	320
	WISA Low Proximity Interest	3	.65	319
Health	WISA Total	16	.74	314
	WISA Privacy	4	.83	326
	WISA Worth	3	.78	326
	WISA Consequences	4	.76	326
	WISA High Proximity Interest	2	.96	319
	WISA Low Proximity Interest	3	.75	315
Lifestyle	WISA Total	16	.73	313
	WISA Privacy	4	.88	326
	WISA Worth	3	.80	326
	WISA Consequences	4	.77	326
	WISA High Proximity Interest	2	.98	318
	WISA Low Proximity Interest	3	.67	315
Financial	WISA Total	16	.68	311
	WISA Privacy	4	.76	326
	WISA Worth	3	.81	326
	WISA Consequences	4	.70	326
	WISA High Proximity Interest	2	.92	313
	WISA Low Proximity Interest	3	.76	314
Intellectual Property	WISA Total	16	.72	313
	WISA Privacy	4	.89	326
	WISA Worth	3	.82	326
	WISA Consequences	4	.68	326
	WISA High Proximity Interest	2	.94	316
	WISA Low Proximity Interest	3	.79	313
Day to day	WISA Total	16	.70	310
	WISA Privacy	4	.88	326
	WISA Worth	3	.86	326
	WISA Consequences	4	.67	326
	WISA High Proximity Interest	2	.96	314
	WISA Low Proximity Interest	3	.66	312
Commercial	WISA Total	16	.71	307
	WISA Privacy	4	.90	326
	WISA Worth	3	.84	326
	WISA Consequences	4	.63	326
	WISA High Proximity Interest	2	.96	314
	WISA Low Proximity Interest	3	.67	308
HR	WISA Total	16	.78	312
	WISA Privacy	4	.86	326
	WISA Worth	3	.82	326
	WISA Consequences	4	.77	326
	WISA High Proximity Interest	2	.93	314
	WISA Low Proximity Interest	3	.74	313

4.3.7 | INFORMATION SENSITIVITY DIFFERENCES

This section is dedicated to assessing the second aim of the study to explore differences in information sensitivity and security behaviour for the different information types, knowledge about legal and organisational regulations applying to these information types and employees' frequency of data usage.

Table 19. Means (and standard deviations) for the 5 WISA aspects for each information type

N=315	Information type	Mean (SD)
Privacy	Personal information	3.74 (.86)
	Health information	4.32 (.68)
	Lifestyle information	3.02 (.93)
	Financial information	4.55 (.58)
	Intellectual property	4.01 (.82)
	Day to day business information	3.67 (.86)
	Commercial information	3.86 (.88)
	HR information	4.34 (.71)
Worth	Personal information	4.10 (.71)
	Health information	4.25 (.69)
	Lifestyle information	3.68 (.81)
	Financial information	4.30 (.75)
	Intellectual property	4.25 (.65)
	Day to day business information	4.00 (.69)
	Commercial information	4.14 (.69)
	HR information	4.22 (.68)
Consequences	Personal information	2.34 (.68)
	Health information	3.08 (.82)
	Lifestyle information	2.70 (.72)
	Financial information	3.19 (.80)
	Intellectual property	2.56 (.70)
	Day to day business information	2.60 (.67)
	Commercial information	2.66 (.66)
	HR information	3.33 (.85)
High Proximity Interest	Personal information	2.76 (1.34)
	Health information	2.77 (1.28)
	Lifestyle information	2.93 (1.29)
	Financial information	2.20 (1.08)
	Intellectual property	2.21 (1.02)
	Day to day business information	1.89 (.93)
	Commercial information	1.89 (.93)
	HR information	2.17 (1.12)
Low Proximity Interest	Personal information	2.97 (.92)
	Health information	2.80 (1.06)
	Lifestyle information	3.05 (.99)
	Financial information	3.22 (1.08)
	Intellectual property	3.64 (1.06)
	Day to day business information	3.51 (.96)
	Commercial information	3.64 (.95)
	HR information	3.11 (1.05)

An 8 (information type) X 5 (WISA appraisal) repeated measures ANOVA was conducted to explore differences in ratings for the 8 information types.

4.3.7.1 | Main effect of WISA appraisal on ratings

There was a significant main effect of WISA appraisal on ratings (F(3.17, 994.48)=438.924. p<.001) with Greenhouse-Geisser correction.

Table 20. Mean differences for ratings for all aspects of the WISA appraisal and p values resulting from Bonferroni corrected repeated measures t-tests

	1	2	3	4	5
1 - WISA Privacy	-	-0.179**	1.131**	1.585**	.696**
2 - WISA Worth			1.310**	1.585**	.875**
3 - WISA Consequences				.454***	-.436**
4 - WISA High Proximity Interest					-.889***
5 - WISA Low Proximity Interest					

*p<.05; **p<.01, ***p<.001

Post-hoc analyses indicated that there was a significant difference in ratings between all WISA types. Worth had the highest ratings (M=4.12), followed by privacy (M=3.94), low proximity interest (M=3.24), consequences (M=2.81) and finally, high proximity interest (M=2.35).

4.3.7.2 | Main effect of information type on sensitivity ratings

There was a significant main effect of information type on rating = (F(5.73, 1799.27)=92.435. p<.001) with Greenhouse-Geisser correction. Table 21 shows the results of the posthoc analyses t-tests.

Table 21. Mean differences for ratings for all information types and p values resulting from Bonferroni corrected repeated measures t-tests

	Personal	Health	Lifestyle	Financial	Intellectual Property	Day to day business	Commercial	HR
Personal	-	-2.96**	.139**	-.309**	-.155**	.045	-.057	-.255**
Health		-	.435**	-.013	.141**	.341**	.239**	.041
Lifestyle			-	-.448**	-.293**	-.094*	-.196**	-.394**
Financial				-	.155**	.354**	.252**	.054
Intellectual Property					-	.199**	.098**	-.101*
Day to day business						-	-.102*	-.300*
Commercial							-	-.300*
HR								-

*p<.05; **p<.01, ***p<.001

Post hoc analyses indicated that financial information had the highest ratings (M=3.49), followed by health information (M=3.48), HR information (M=3.44), intellectual property (M=3.34), commercial information (M=3.24), personal information (M=3.18), day to day business information was second lowest for sensitivity ratings (M=3.14), and lifestyle information was the lowest for ratings (M= 3.04).

4.3.7.3 | The Interaction Effect of Information Type and WISA appraisal

There was a significant interaction effect of information type and WISA appraisal on ratings $(F(16.46, 5169.106)=110.43. p<.001)$ with Greenhouse-Geisser correction.
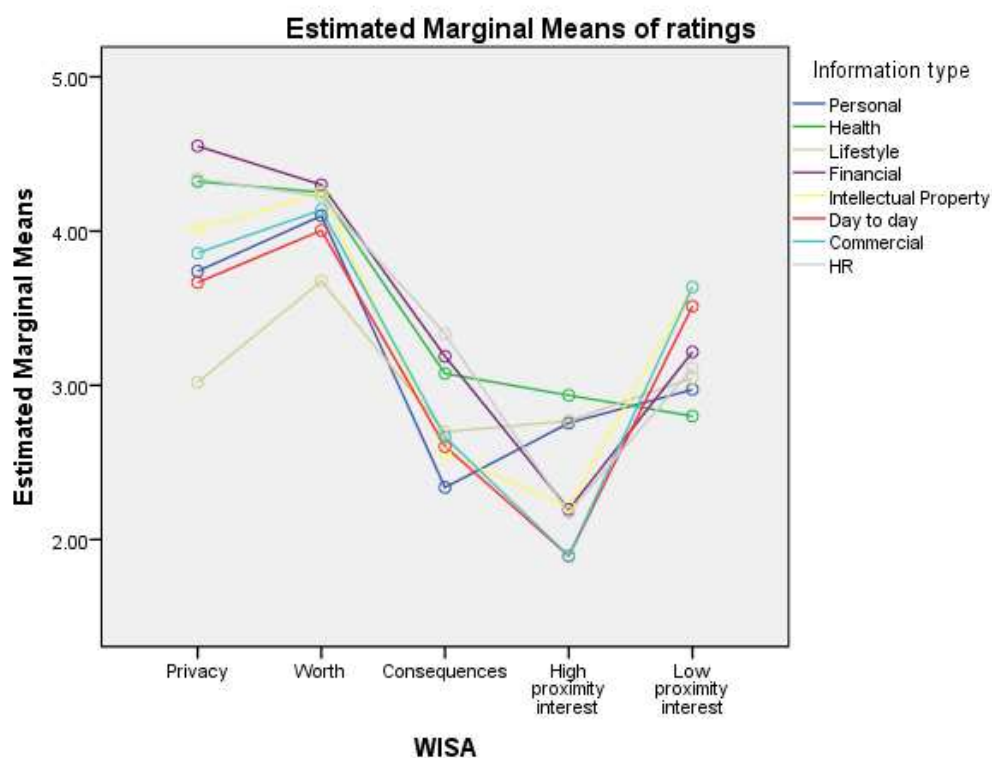
Figure 21. Line graph of ratings for each information type

Figure 21 shows that there appears to be a consistent trend in the order of the information types across privacy, worth and consequences. This ordering appears to change for high and low proximity interest, particularly for the information types of financial and HR for high proximity interest, and commercial and day to day for low proximity interest. These findings will be further explored in the additional analyses outlined below.

4.3.7.4 | Follow-up of interaction effect

Differences in WISA appraisal for information types were explored by running posthoc analyses using repeated measures ANOVAs for each WISA subscale.

4.3.7.4.1 | PRIVACY

Figure 22. Mean privacy ratings by information type

Table 22. Mean differences for privacy ratings for all information types and p values resulting from Bonferroni corrected posthoc analyses

	1	2	3	4	5	6	7	8
(1) Personal	-	-.583***	.715***	-.818***	-.293***	.056	-.133	-.610***
(2) Health		-	1.23***	-.235***	.290***	.639***	.450***	-.027
(3) Lifestyle			-	-1.53***	-1.01***	-.659***	-.847***	-1.32***
(4) Financial				-	.525***	.874***	.686***	.209***
(5) Intellectual Property					-	.349***	.160	-.317***
(6) Day to day business						-	.189**	-.666***
(7) Commercial							-	-.477***
(8) HR								-

*p<.05; **p<.01, ***p<.001

Pairwise comparisons of information type revealed that there were significant differences between each information type for privacy score. However, as shown in Table 22 the differences between some information types were not significant. Financial information was considered the most private (M=4.55). Followed by HR information (M=4.34) and then health information (M=4.31) and IP (M= 4.02) which were the third and fourth highest for privacy ratings. Commercial information (M=3.86), personal information (M=3.73) and day to day information (M=3.67) were the fifth, six and seventh in order of privacy ratings. Finally, lifestyle information (M=3.01) was considered the least private.

4.3.7.4.2 | WORTH

Figure 23. Mean worth ratings by information type

Table 23. Mean differences for worth rating for all information types and p values resulting from Bonferroni corrected posthoc analyses

	1	2	3	4	5	6	7	8
(1) Personal	-	-.143**	.426***	-.187**	-.143*	.103	-.022	-.105
(2) Health		-	-.570***	-.044	.016	.246***	.121	.038
(3) Lifestyle			-	-.613***	-.570***	-.323***	-.449***	-.532***
(4) Financial				-	.044	.290***	.165**	.082
(5) Intellectual Property					-	.246***	.121**	.038
(6) Day to day business						-	-.126**	-.209***
(7) Commercial							-	-.083
(8) HR								-

*p<.05; **p<.01, ***p<.001

Pairwise comparisons of information type revealed that there were significant differences between each information type for worth score. However, as shown in Table 23 the differences between some information types were not significant. Financial information was considered to have the most worth (M= 4.3), followed by IP (M= 4.25) and health information (M=4.25), HR (M=4.22), commercial (M=4.13), personal information (M=4.11), day to day (M=4.01) and finally lifestyle information (M=3.69).

133

4.3.7.4.3 | CONSEQUENCES

Figure 24. Mean consequences ratings by information type

Table 24. Mean differences for consequences rating for all information types and p values resulting from Bonferroni corrected posthoc analyses

	1	2	3	4	5	6	7	8
(1) Personal	-	-.744***	-.369***	-.856***	-.255***	-.274***	-.335***	-1.00***
(2) Health		-	.375***	-.112	.519 ***	.40***	.409***	-.258***
(3) Lifestyle			-	-.487***	.144*	.095	.034	-.633***
(4) Financial				-	.631***	.582***	.521***	-.146**
(5) Intellectual Property					-	-.049	-.110*	-.777***
(6) Day to day business						-	-.061	-.728***
(7) Commercial							-	-.666***
(8) HR								-

*p<.05; **p<.01, ***p<.001

HR was considered to have the highest consequences ratings (M=3.34), followed by financial (M=3.19), and health information (M=3.08). Lifestyle (M=2.70) was the fourth highest for perceived consequences, commercial information (M=2.67) was the fifth highest and day to day information was the sixth (M= 2.61). IP was second to last for lowest consequence ratings (M=2.56) and finally, personal information (M=2.33).

4.3.7.4.4 | HIGH PROXIMITY INTEREST

Figure 25. Mean high proximity interest ratings by information type
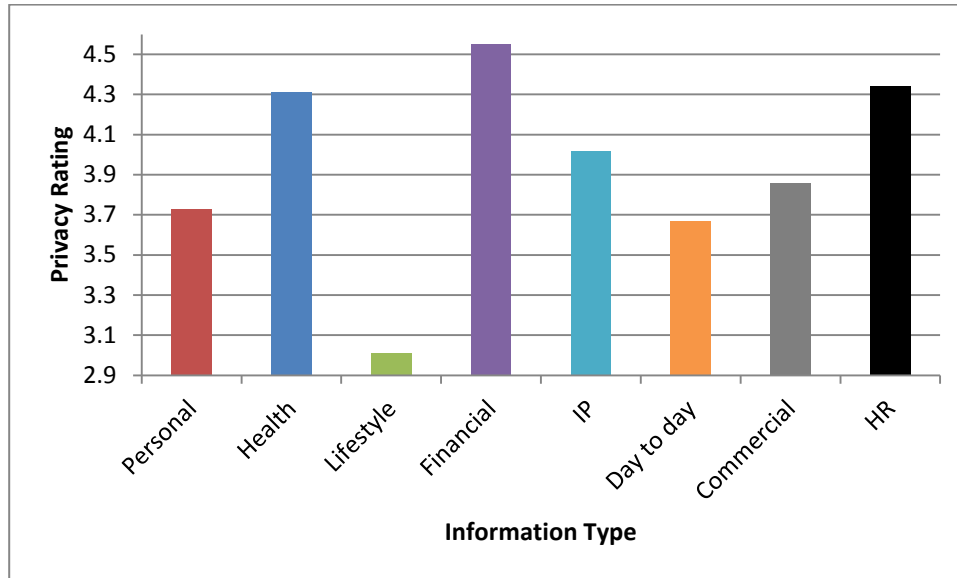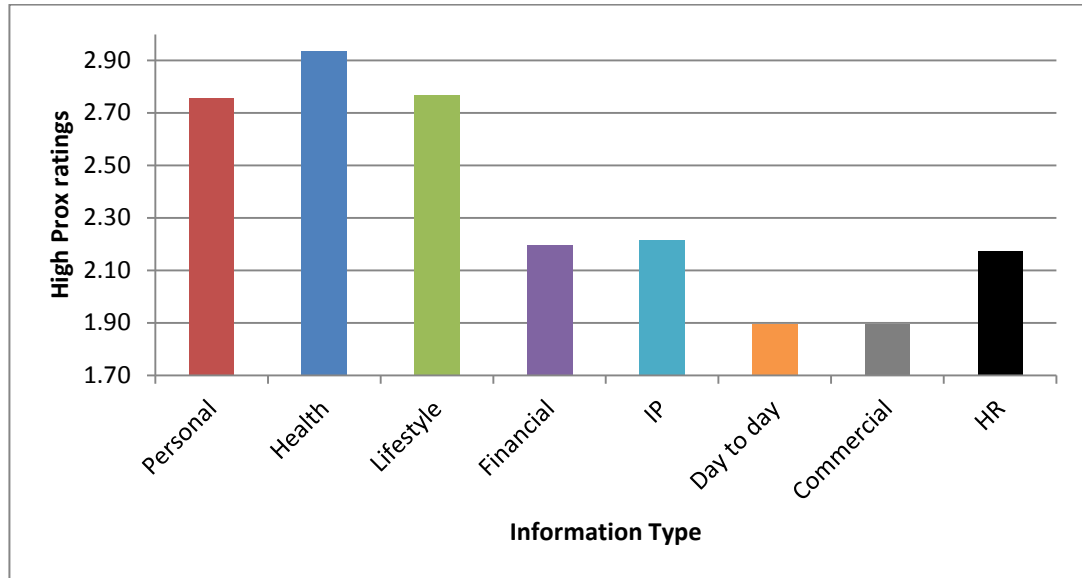

Table 25. Mean differences for high proximity interest ratings for all information types and p values resulting from Bonferroni corrected posthoc analyses

	1	2	3	4	5	6	7	8
(1) Personal	-	-.179	-.014	.560***	.541***	.862***	.862***	.581***
(2) Health		-	.165	.740***	.721***	1.04***	1.04***	.760***
(3) Lifestyle			-	.575***	.556***	.876***	.876***	.595***
(4) Financial				-	-.019	.302***	.302***	.021
(5) Intellectual Property					-	.321***	.321***	.040
(6) Day to day business						-	.000	-.281***
(7) Commercial							-	-.281***
(8) HR								-

*p<.05; **p<.01, ***p<.001

Pairwise comparisons revealed that there were significant differences between each information type for high proximity interest score. However, as shown in Table 25 the differences between some information types were not significant. Health information was the highest for high proximity interest (M=2.93), followed by lifestyle (M=2.77), personal (M=2.76), IP (M=2.21) and financial (M=2.20). HR (M=2.17) was sixth highest for high proximity interest ratings, and Day to day (M=1.89) and commercial (M=1.89) were lowest for ratings. The findings suggest that information types which involve individual's information (e.g. personal, health and lifestyle) are considered to be of interest to employees' high proximity groups (i.e. family and friends) compared to information of an organisational or commercial focus (e.g. IP, commercial and HR).

4.3.7.4.5 | LOW PROXIMITY INTEREST

Figure 26. Mean low proximity interest ratings by information type
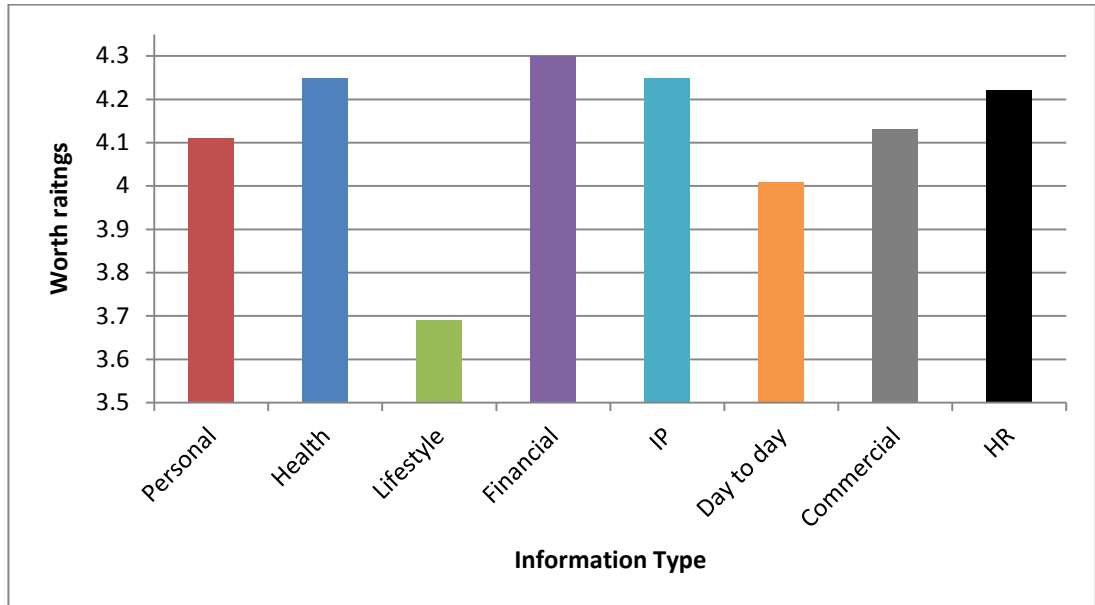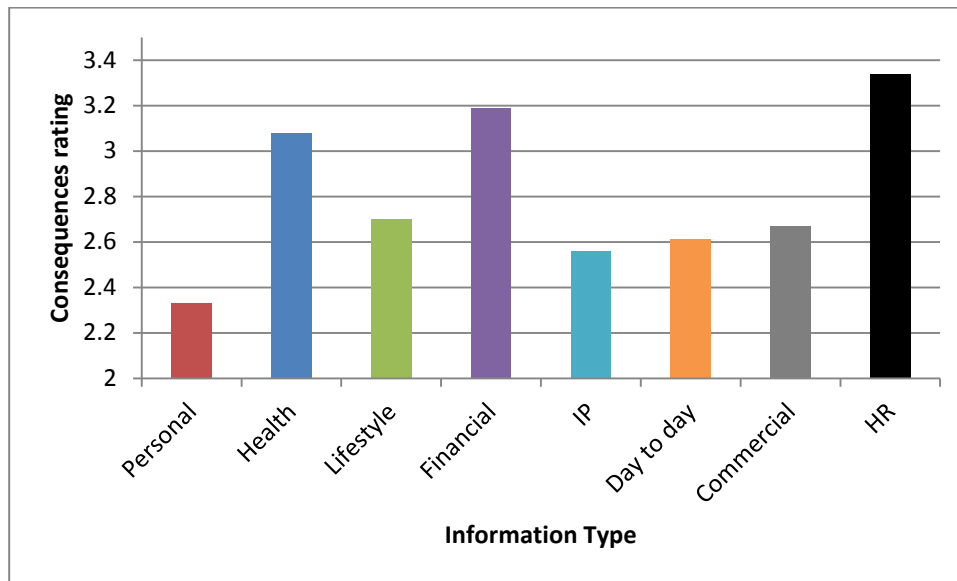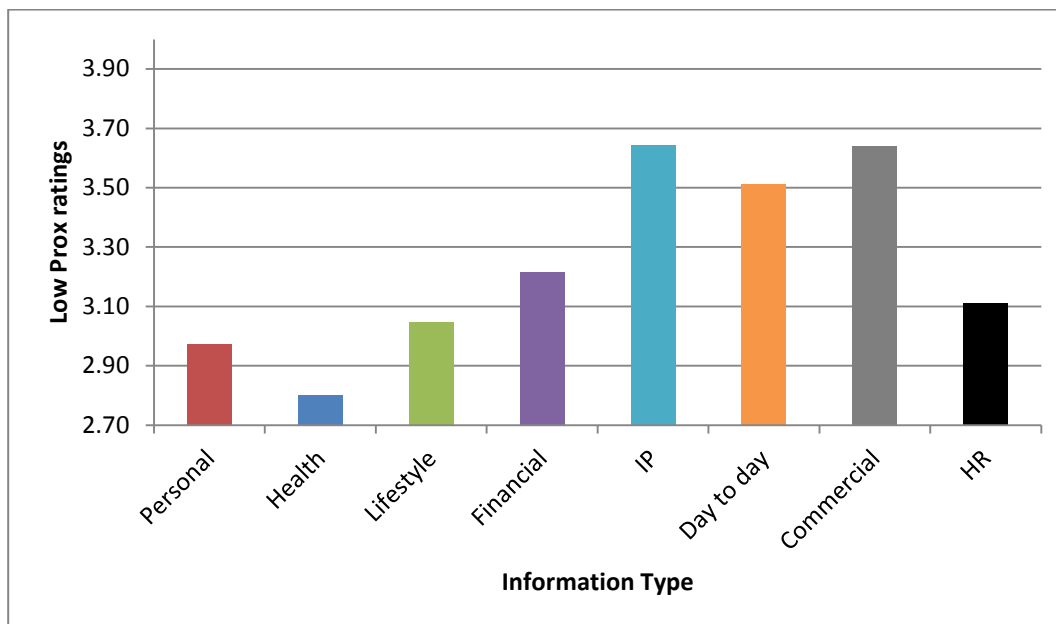

Table 26. Mean differences for low proximity interest ratings for all information types and p values resulting from Bonferroni corrected posthoc analyses

	1	2	3	4	5	6	7	8
(1) Personal	-	-.172**	-.075	-.243***	-.670***	-.540***	-.665***	-.139
(2) Health		-	-.247***	-.415***	-.842***	-.712***	-.837***	-.311***
(3) Lifestyle			-	-.168*	-.595***	-.465***	-.589***	-.064
(4) Financial				-	-.427***	-.296***	-.421***	.104
(5) Intellectual Property					-	.131**	.006	.531*
(6) Day to day business						-	-.125*	.401*
(7) Commercial							-	.525*
(8) HR								-

*p<.05; **p<.01, ***p<.001

IP (M=3.64) and commercial (M=3.64) were rated the highest for low proximity interest, followed by day to day (M=3.51) and financial (M=3.22). The fifth highest for low proximity interest was HR (M=3.11), followed by lifestyle (M=3.05), personal (M=2.97) and health (M=2.80). The is contrasting to the findings for high proximity interest as information with an organisational focus (e.g. IP, commercial and day to day) were rated as high interest for low proximity groups (i.e. criminals, business competitors and fellow employees) compared to information about individuals (e.g. health, personal).

4.3.7.5 | Summary of sensitivity differences by information type

Financial, HR and health were the three information types to be amongst the highest for privacy, worth and consequences dimensions whereas commercial, day to day, and personal are amongst the lowest for these three dimensions. IP is amongst the highest for privacy and worth, and lifestyle are amongst the lowest, however, this observation reverses for the consequences dimension. Intellectual property is considered to be highly private and has high worth but consequences of its disclosure are not perceived as severe. This may be due to the consequences dimension including emotional consequences (e.g. humiliating and embarrassing) which employees may not associate with information that is unrelated to living individuals. Lifestyle information is not perceived as highly private and having high worth, but it may have consequences if disclosed. For perceived interest in information, intellectual property is the only information type to be amongst the highest for high and low proximity interest. Health, lifestyle and personal information were considered to be of interest to high proximity groups whereas commercial, day to day and financial were perceived to be of interest to low proximity groups.

4.3.7.6 | Perceptions of legal and organisational regulations

It was also necessary to explore whether there were differences in employees' sensitivity ratings as well as their security behaviour, dependent on their perceptions of legal and organisational regulations. For each information type, the regulations explored were; whether the information was (1) publically available, (2) regulated by law and (3) access controlled by their organisation. In the following analyses, participants are grouped based on their response to these questions in which they rated 'yes', 'no' or 'I do not know'.

4.3.7.6.1 | Perceptions of publically available information and access restrictions by organisation on sensitivity ratings

For each information type, a one-way MANOVA was conducted to explore differences in perceptions of publically available information and perceptions of access restrictions by the organisation on sensitivity ratings. Findings revealed that there were no significant main effects of publically available information perceptions and access restrictions perceptions on sensitivity ratings ($p > .05$) for all information types.

4.3.7.6.2 | Perceptions of regulation by law on sensitivity ratings

For each information type, a one-way MANOVA was conducted to explore differences in perceptions of law regulations on sensitivity ratings for each information type. Findings revealed that there were no significant main effects of law regulations on sensitivity ratings ($p > .05$) for all information types apart from personal information.

The findings for personal information indicated a significant main effect of perceptions of law regulations on personal information sensitivity ratings (Pillai's Trace $=.091$, $F(10, 460)=2.202$, $p<.05$).

Further analyses indicated that the effect of perceptions of law regulations was significantly different for low proximity ratings for personal information ($F(2, 233) = 5.509$, $p<.05$).

Gabriel posthoc analyses were conducted in which pairwise comparisons revealed no significant difference between those with ($M= 3.12$) and those without ($M= 3.29$) perceptions of law regulations for personal information low proximity interest ($p>.05$). There was, however, a significant difference between those with and those without perceptions compared to individuals who indicated that they did not know ($M=2.55$) ($p<.05$). This suggests that those with lacked awareness of law regulations rated low proximity interests significantly lower than those with an incorrect awareness of law regulations pertaining to personal information and those with a perception that law regulations exist.

4.3.7.6.3 | Interaction effects

Findings from the MANOVAs indicated that there were no significant interactions between any of the perceptions of legal and organisational regulations on any information type.

4.3.7.6.4 | Perceptions of legal and organisational regulations on information security behaviours

The degree to which a difference in security behaviour depends on employees' perceptions of legal and organisational regulations was further investigated using one-way ANOVAs. These found no significant differences in security behaviour depending on regulation perceptions for all information types ($p>.05$) apart from personal information.

For personal information, differences were explored between those individuals with perceptions of access restrictions ($M=57.86$), those who indicated there were no access restrictions for personal information ($M=55.11$) and those who did not know if there were access restrictions ($M=50.11$). The ANOVA revealed that there was a significant difference in security behaviour depending on perceptions of access restrictions for personal information ($F(2,226)= 4.236$, $p=.016$). Gabriel posthoc analyses revealed that the only significant difference was between those with perceptions of access restrictions and those who did not know if there were access restrictions ($p<.01$).

Overall, this suggests that those individuals with perceptions that personal information is access controlled within their organisation have significantly higher self-reported security behaviour. This was in comparison to those individuals who lacked awareness of access restrictions relating to personal information within their workplace.

4.3.7.7 | Data usage
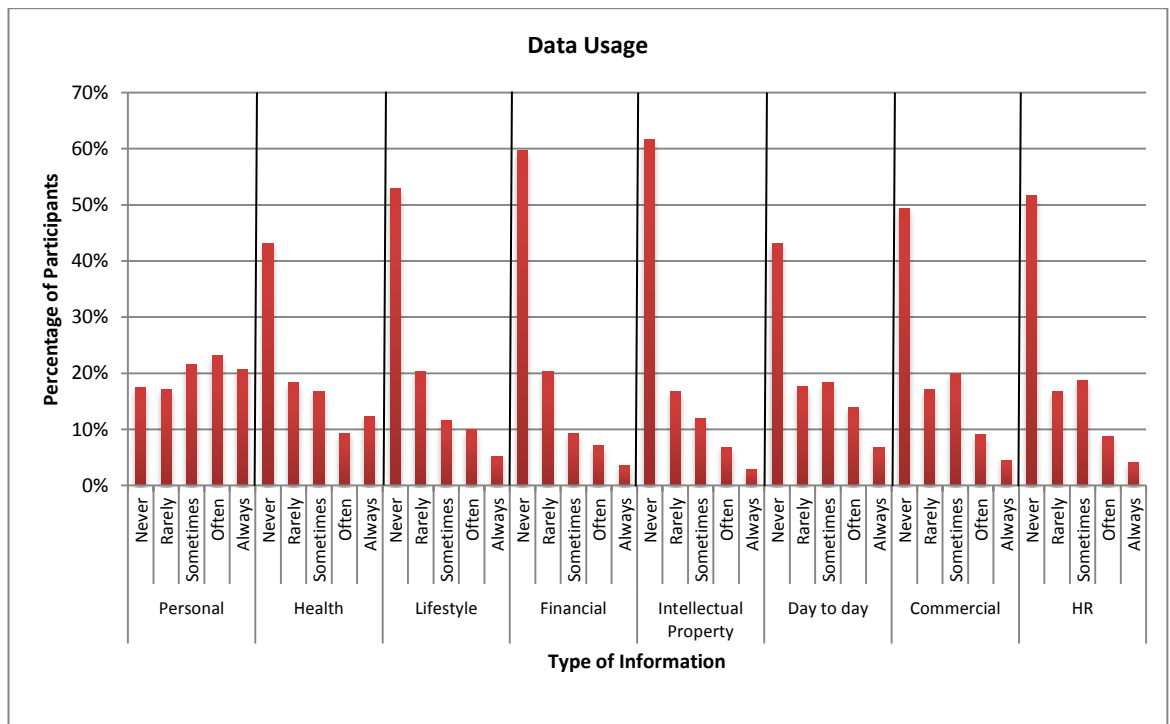
Figure 27. The frequency of data usage for each information type

Employees indicated their frequency of storing and processing the information types within their workplace. Personal information was the most used with 82.6% using this data at least 'rarely', followed by health information (56.8%), day to day business information (58.9%), commercial (53.1%) and HR information (50.9%). Lifestyle, financial and intellectual property were used by less than 50% of employees at least 'rarely'. Figure 27 shows the percentage of participants and their frequency of data usage for each information type.

4.3.7.7.1 | Data usage and information sensitivity and security

Employees were split into three groups for each information type, depending on their ratings of the frequency of data usage. Those who indicated that they never worked with the information type were grouped into the "no" user group, those who worked with the information rarely or sometimes were placed in the "low" user group and those who worked with the information often or always into the "high" user group.

One-way MANOVAs were conducted for each information type to explore if there were significant differences in sensitivity ratings for all 5 WISA dimensions dependent on data usage group. Findings revealed that there were no significant main effects or interaction effects of data usage groups on ratings (p>.05) for all information types. This, therefore, indicates that data usage does not influence sensitivity ratings.

One-way ANOVAs were conducted for each information type to explore whether there were significant differences in the security behaviour depending on data usage group. There was no significant difference in the security behaviour between data usage groups for health information, lifestyle, financial, IP and HR (p>.05).

Personal information. There was a significant difference in the security behaviour between data usage groups (F(2, 290)=6.595, p<.01). Post-hoc analyses indicated a significant difference between the 'no' usage group (M=50.41) and 'high' usage group (M=57.13) (p>.05) suggesting that individuals who are high regular users of personal information data significantly engage in more security behaviours compared to those individuals that do not work with personal information.

Day to day business information. There was a significant difference in the security behaviour between data usage groups (F(2, 290)=8.295, p<.01). Post-hoc analyses indicated that there was a significant difference between the 'no' usage group (M=52.57) and 'high' usage group (M=59.47) (p<.01) suggesting that individuals with high usage of day to day business perform significantly more security behaviours than low and no data users.

Commercial information. There was a significant difference in the security behaviour between data usage groups (F(2, 290)=6.884, p<.01). Post-hoc analyses indicated that there was significant difference between the 'no' usage group (M=52.55) and the 'low' usage group (M=56.95) and high usage group (M=57.98) (p<.01). This suggests that data users independent of usage frequency perform significantly more security behaviours as compared to users who do not work with commercial data.

4.4 | DISCUSSION

4.4.1 | SCALE VALIDATION

This study developed and validated a new measure for information sensitivity to be used within a workplace setting. The resulting 17-item scale has five sub-scales: privacy, worth, consequences, low proximity interest and high proximity interest. The WISA scale, alongside its five subscales was found to have strong factorial validity which was confirmed across 8 target information types. The scale also had good criterion-related validity as it was found to significantly predict security behaviour. Finally, the scale was found to have adequate discriminant validity as 3 of the 5 aspects of the WISA scale were found to be unrelated to organisational citizenship behaviour.

As discussed earlier, there is no clear consensus on defining information sensitivity. However, there were two clear themes in previous research of what comprises sensitive information. The

140

first focuses on the privacy and intimacy of the information and the second focuses on the vulnerability and exploitability of the information. The current study sought to add further understanding to defining information sensitivity by combining the previous literature definitions with the findings from Chapter 3. Following EFA, the final information sensitivity structure was found to comprise of privacy, worth, consequences, high and low proximity interest. The only difference between the initial information sensitivity structure and that which emerged from the EFA was that "interest by others" was found to be two distinct factors – 'high proximity' and 'low proximity' interest groups rather than one encompassing factor. This revised structure was found to be a strong fit to the data for the 8 target information types. This suggests that this definition of information sensitivity is a strong explanation of the data which was confirmed on 8 information types that may be stored and processed in organisations. This knowledge might be useful for how we conceptualise information sensitivity in further research and within government legislation such as the Data Protection Act (1998). Differences with regards to information types and the five aspects of sensitivity rating will be discussed in the next section.

The scale requires further exploration to improve its validity. The WISA scale while shown to significantly predict security behaviour explained less than 10% of the variance for the composite measure. However, when exploring its role on individual security behaviours, the scale was found to explain between 8-10% of the variance for use of complex passwords, secure Wi-Fi and awareness of physical surroundings. This indicates that the WISA scale may be able to provide improved predictive validity for some security behaviours in comparison to others. This is promising as not one factor would be able to predict security behaviour in isolation and the qualitative study and existing security literature has shown that there are a number of factors that influence security behaviour. The use of WISA may, therefore, explain additional variance in security behaviour alongside other important determinants such as PMT constructs. The aim of the next study is to further explore the extended-PMT model derived from the qualitative study, alongside the WISA scale, to estimate how much variance can be explained in security behaviour and which factors are the best predictors. This will help provide further evidence of the discriminant validity of the WISA scale. Further evidence of criterion-related validity will also be obtained by exploring its role in specific security behaviours (i.e. anti-malware behaviours). Further validation of the scale will provide more evidence for its potential utility for use within the workplace setting and for future research focussing on information sensitivity.

A limitation of the current study is that convergent validity (a form of construct validity) could not be assessed. Convergent validity is important as it measures the degree to which the current scale is correlated with scales that claim to measure the same construct (i.e. information

sensitivity) (Onwuegbuzie et al., 2009). Previous research (Cranor et al., 1999; Malhotra et al., 2004) have used related measures of information sensitivity. However, these were not considered adequate as they had not been under validation assessment nor did they measure information sensitivity in the workplace or were related to assessing information that is not about oneself. Furthermore, they measure the information sensitivity of consumers' own information and there is potential ownership and framing issues when used in comparison to the construct measured within the current study. However, despite this limitation, the current study provides a basis for further development of additional scales measuring information sensitivity within the workplace.

4.4.2 | INFORMATION SENSITIVITY DIFFERENCES

Financial information was found to have the highest ratings for sensitivity followed by health and HR. These aspects were also found to be the highest for 3 of the 5 sensitivity ratings; privacy, worth and consequences. As discussed in the introduction of this chapter and chapter 3, employees rate information about individuals to be more sensitive than organisational information. The current study supports these qualitative findings, however not all information types are considered sensitive. For example, lifestyle information overall had the lowest ratings for sensitivity. This difference in information sensitivity with regards to individuals' data supports previous research by Cranor et al. (1999) who found that individuals were willing to disclose lifestyle information (such as favourite snack) but not willing to disclose financial information (such as a credit card). Further research by Mothersbaugh et al. (2012) on information disclosure has found that sensitivity works along a continuum. The continuum ranges from willing to disclose to not willing to disclose with demographic and lifestyle factors being the information people are most willing to disclose and personal identifiable and financial information as least willing to disclose. The current study supports this literature, however, it adds a further level of understanding by exploring how individuals make this appraisal of sensitivity by considering its perceived privacy, worth, consequences and perceived interest by high and low proximity others and if it affects security behaviour.

This study is one of the first to explore how individuals appraise the sensitivity of organisationally-focused information (i.e. IP, day to day, commercial & HR). The findings by Adams and Sasse (1999), supported by the conclusions of Chapter 3, highlighted that individual's rate some information about individuals as more sensitive than organisational information. Information regarding health and financial data is consistently viewed as sensitive across the dimensions of privacy, worth and consequences. Likewise, HR information about individuals is also considered sensitive across these dimensions. Personal and lifestyle information, whilst they refer to individuals' information are not considered sensitive for

privacy, worth and consequences. Commercial and day to day organisationally-focussed information were consistently low for privacy, worth and consequences. Intellectual property was the only information type that did not relate to individuals but was highly rated for privacy, worth, high proximity and low proximity interest. IP was not highly rated for consequences and this was the same for other organisational information; commercial and day to day. There are a number of possible reasons for this finding; firstly this study defines consequences as humiliating, compromising, discreditable, and embarrassing, which individuals may not associate with information that is not about people. This could reflect the decline in sensitivity rating for consequences when comparing the two broad information types of organisational-focussed and individual-focussed. A second potential explanation could be that individuals lack awareness of consequences associated with organisational information and, therefore, rate them lower.

This study is one of the first to focus on how employees rate sensitivity of organisational information. The study confirms both the findings from Chapter 3 and those of Adams and Sasse (1999) but also showed that employees do consider some forms of organisational-focussed information to be sensitive i.e. intellectual property. This suggests that a binary judgement of sensitivity is not sufficient for understanding how sensitivity is appraised and consequently the current study suggests that individuals consider five components of this. The main difference between individually-focussed information and organisational-focussed is the perceived high or low proximity interest.

High proximity and low proximity interest revealed some interesting findings with regards to differences in the two broad information types. Information about individuals (e.g. personal, health and lifestyle) was considered to be of interest to employees' high proximity interest groups (i.e. family and friends) in comparison to organisational-focussed information as well as financial and HR information. For low proximity interest, the opposite effect is apparent with organisational-focussed information (IP, commercial and day to day) perceived to be of interest to low proximity groups (i.e. criminals, fellow employees & business competitors). There is limited previous research that looks at this form of sensitivity appraisal, the inclusion of which was driven by the findings of Chapter 3 which suggested that employees consider the audience (or interest) in information that they work with and use this as a basis to evaluate the sensitivity of the information. The current study contributes novel findings that suggest that future research may need to further explore perceived interest in information sensitivity conceptualisations.

This study also explored perceptions of legal and organisational regulations with regards to the information types, and the impact of these perceptions on their sensitivity ratings and security

behaviour. There was only an observed difference for personal information. For sensitivity ratings, a significant difference was found for perceptions of law regulations for personal information for the WISA component - low proximity interest. These differences were between those who had perceptions and those who did not know there were regulations. For security behaviour, those with perceptions that personal information is access controlled had significantly higher self-reported security behaviour compared to those who lacked awareness.

Taken together, these findings could be due to employees' knowledge of law regulations surrounding the Data Protection Act (1998) suggesting that knowledge may play a small role in personal information but not for any other. The DPA governs the information of living individuals, including their personal information. Companies must abide by the DPA and have restrictions in place to protect information governed by the act. This may account for why those who are aware of access controls and legal regulations rate the information more sensitive (for low proximity interest) and engage in more security behaviours.

These findings could also be due to attitudinal differences around personal information storage by those who indicated that they 'did not know' if there were regulations. These individuals may be complacent towards information sensitivity and security which may explain the significant difference in the low proximity component and self-report security behaviour between those with perceptions and those who indicated they did not know.

The role of frequency of data usage in information sensitivity (and security) was also explored. Findings revealed that there were no significant main effects or interaction effects of data usage groups on sensitivity ratings for all information types. This suggested that the more an individual works with an information type does not mean they rate the information any more sensitive than employees who do not work with the information. There were, however, some differences in the security behaviour of individuals for the information types: personal, day to day and commercial which suggested that individuals who work with these information types engaged in more security behaviours than those who did not.

This study is one of the first to explore how individuals rate the sensitivity of information belonging to other individuals in contrast to previous research (e.g. Cranor et al., 1999) that investigates how individuals evaluate the sensitivity of their own information. Future research is needed to explore differences in sensitivity evaluation of self vs. others information and whether individuals evaluate the sensitivity of their own information differently depending on data ownership.

Overall, this chapter has outlined the development and validation of a new scale to evaluate the sensitivity of workplace information. This study has identified differences in employees' sensitivity evaluation of different types of information stored by organisations. The scale will be further explored in the next chapter for a specific sub-set of security behaviours; anti-malware behaviours.

CHAPTER 5: EXPLORING THE EXTENDED-PMT MODEL FOR ANTI-MALWARE BEHAVIOURS

This chapter builds on the findings from Chapter 3 by investigating the influence of the identified factors with three specific behaviours; an anti-malware software behaviour (AMS security; using anti-malware software to scan USB sticks for malware), an email security behaviour (ES security; not clicking on links in suspicious emails) and a software update behaviour (SU security; installing software updates when prompted). The study adds to the body of knowledge by exploring an extended-PMT model. The extensions are derived from existing literature and Chapter 3 namely security responsibility, information sensitivity, experience, psychological ownership and organisational citizenship behaviour. In summary, the study addressed the following issues as identified in the literature review:

- An over-reliance on security policy compliance as representing a single security behaviour;
- A lack of studies exploring the behavioural determinants of single security behaviours, particularly in relation to a specific security threat;
- A lack of understanding of whether behavioural determinants differ by security behaviour.

These issues were addressed by focussing on malware as the specific threat and three different malware protection behaviours. The study found that an extended PMT-model and its components differed by security behaviour. The revised models were a strong fit to the data. Overall, the findings suggested that the coping appraisal components (self-efficacy, response costs and response efficacy) of the model could explain security behaviours better than the threat component (susceptibility and severity). In particular, response efficacy (an identified barrier from Chapter 3) was a significant predictor of all three behaviours. From the extended factors, responsibility was found to be an important predictor of the AMS and SU behaviour. A component of the WISA appraisal (WISA consequences) was also found to predict the AMS behaviour. Psychological ownership and organisational citizenship behaviour were not found to influence any of the behaviours.

This chapter starts by providing evidence of why these anti-malware behaviours are important and then outlines the hypotheses to be explored in the study, driven by existing literature and the findings from Chapter 3.

5.1 | MALWARE AND ANTI-MALWARE BEHAVIOURS

Malware continues to be one of the frequently experienced cyber-attacks faced by organisations (Ponemon Institute, 2012). Despite companies best efforts, attacks remain relatively stable with 317 million new pieces of malware created in 2014 (Symantec Corporation, 2015) and a rise in more innovate and diverse tactics (Sophos, 2014).

Malware threats and malware prevention behaviours were chosen because they are relatively understudied within the workplace. A number of studies have explored consumers' anti-malware behaviours (Chenoweth et al., 2009; Dang-pham & Pittayachawan, 2015; Gurung et al., 2009; Lee et al., 2008; Liang & Xue, 2009, 2010) but only the study by Ng et al. (2009) explored viruses in the workplace using behavioural models; investigating employees' threat and coping appraisal for checking email attachments. More attention is therefore warranted to understand employees' malware threat appraisal and their evaluation of different anti-malware behaviours.

5.1.1 | ANTI-MALWARE BEHAVIOURS

The current study seeks to address three specific anti-malware behaviours; use of anti-malware software to scan USB sticks, avoiding links in suspicious emails and installing software updates when prompted. The behaviours were chosen as they are important behaviours to prevent malware and require different levels of input from the user so may provide potential variation in the influence of their determinants. The current study seeks to address the gap in the lack of studies on behavioural security for these behaviours in relation to malware mitigation.

5.1.2 | USING ANTI-MALWARE SOFTWARE TO SCAN USB STICKS FOR MALWARE

USB sticks are used to store and share data as they are readily available, small, inexpensive and portable. However, they are an important security concern due to their ability to store hidden malware. Malware can be easily spread across computers as the user shares or plugs their USB device into other machines; potentially passing on malware, without the user being aware that their device is infected. Removable media is recognised as a risk for malware infection in businesses by the UK government (Gov.uk, 2015).

There are some recommendations to protect against this risk including disabling autorun for removable media and scanning USB sticks for malware (Zonealarm, 2013). The current study seeks to explore behaviours at the employee-level and identify the determinants of intentions to engage in scanning USB sticks for malware.

5.1.3 | LINKS IN PHISHING EMAILS

One form of phishing is "Malware-based phishing" or "Malicious spam", an attempt to get the user to download a malware-infected attachment or click on a malicious link where malware can be downloaded onto their machine. The tactics used by attackers are variable, often changing the way malware may be distributed by email. For example, in October 2014 only 7% of spam emails contained malicious links, this rose to 41% in November 2014 and continued to rise in December (Symantec, 2014). Links are less problematic for attackers as organisations' security software often scans and blocks attachments that they suspect of containing malware so URLs represent an opportunity to avoid detection from these security products.

Avoiding malware spread via phishing is an important deterrent in preventing a security breach. Habitual clicking on links by susceptible employees is problematic in the context of malware prevention. Existing research traditionally focuses on phishing emails as a threat towards collecting sensitive information, but there has been less attention on the role in distributing malware in behavioural information security research.

5.1.4 | INSTALLING SOFTWARE UPDATES ON DEVICES

Malware targets the vulnerabilities of computer systems and software. For example, drive-by downloads exploit vulnerabilities in web browsers or plugins that allow malware to be installed on users' machines. Software such as Java, Flash and Adobe Acrobat have been used as platforms for cybercriminals to install malware on users' machines and these need to be kept up to date (Microsoft, 2015). Security software and operating system updates are important to make sure vulnerabilities are quickly removed. Attackers compromise systems through zero-day exploits in which attackers exploit vulnerabilities in software that are unknown to the software provider (Sans, 2015) and through users delayed machine updates.

In the workplace, identifying and deploying updates are often the responsibility of the IT department. Even so, the employee may still be required to restart their machines to allow the installation. However, the findings from Chapter 3 suggest that employees may postpone or refrain from restarting their computer machines to reduce the impact on their productivity. In addition, software on employees' machines may be installed that is not maintained by IT that requires the user to manage the entire update process.

There is a lack of studies exploring motivations of employees intentions to install software updates when prompted by their machine, however, there are a few qualitative studies on consumers identifying the unintended consequences of installing software updates and the negative implications of this towards security behaviour (Wash, Rader, Vaniea, & Rizor, 2014).

5.2 | STUDY AIMS AND HYPOTHESES

The current study aims to identify key factors related to employees' protection motivation for a specific subset of security behaviours, in particular, anti-malware behaviours: removable media, software updates and suspicious links in relation to malware mitigation. It is intended that this will lead to a more concise model to understand the complexity surrounding individuals' motivations to engage in protective actions. Furthermore, the findings of the study will help to further explore threat and coping appraisal, alongside findings from the qualitative study and explore how they may differ dependent on security behaviour.

Chapter 3 led to the development of the modified PMT framework to be explored within the current study which is presented below:
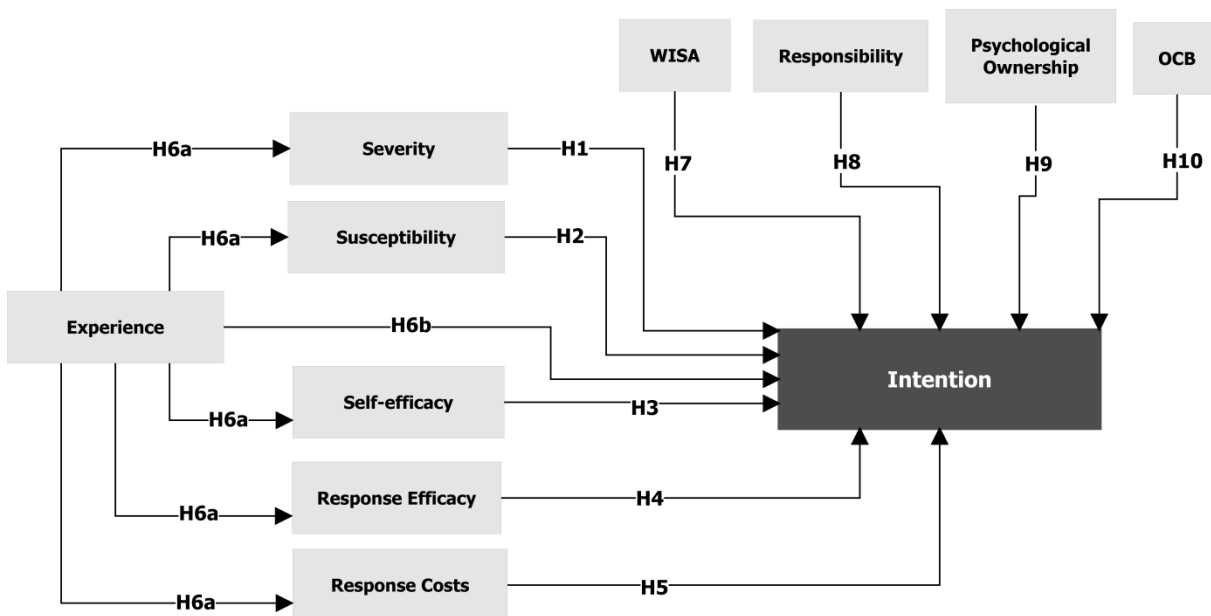
Figure 28. Extended Hypothesized Protection Motivation Theory in the context of security

In line with the original PMT model (as outlined in section 2.2.1.1) and existing research in section 2.2 and studies exploring these factors on specific anti-malware behaviours (Chenoweth et al., 2009; Gurung et al., 2009; Johnston & Warkentin, 2010; Liang & Xue, 2009; Ng et al., 2009), the following hypotheses are formulated:

- **Hypothesis$_1$:** There will be a positive relationship between perceived severity and intention
- **Hypothesis$_2$:** There will be a positive relationship between perceived susceptibility and intention
- **Hypothesis$_3$:** There will be a positive relationship between self-efficacy and intention
- **Hypothesis$_4$:** There will be a positive relationship between response efficacy and intention

150

- **Hypothesis₅:** There will be a negative relationship between response costs and intention

- **Hypothesis₆ₐ:** The effects of experience on protection motivation will be mediated by threat appraisal (susceptibility & severity) and coping appraisal (response efficacy, self-efficacy and response cost)

- **Hypothesis₆ᵦ:** There will also be a positive relationship between experience and intention

Based on the qualitative study (chapter 3) and chapter 4 for WISA, the following hypotheses were formulated:

- **Hypothesis₇:** There will be a positive relationship between workplace information sensitivity appraisal and protection intention

- **Hypothesis₈:** There will be a positive relationship between security responsibility and protection motivation

Previous research as outlined in section 2.2.5.5 for ownership and section 2.2.6.5.2 for citizenship lead to the development of the following hypotheses:

- **Hypothesis₉ₐ:** There will be a positive relationship between psychological ownership of data and intention

- **Hypothesis₉ᵦ:** There will be a positive relationship between psychological ownership of technology and intention

- **Hypothesis₁₀:** There will be a positive relationship between organisational citizenship and intention

5.2.1 | IMPLICIT SECURITY TASK

In addition to exploring self-report anti-malware behaviours, it was important to explore the factors in relation to an objective measure of actual behaviour and explore if there are differences in the determinants of those who engage in the secure behaviour. By using an implicit measure, it was possible to explore a behaviour that is not open to self-report bias. The implicit security measure will take the form of non-acceptance of an online cookie, while cookies are nothing more than text files and they are not malware. They are stored on users' machines and transmitted back to the website when they browse a site. They are associated with a number of security issues as they can store sensitive information such as passwords and credit-card details to pre-fill forms online. They are potentially open to exploitation by hackers if the security of the website and the user's browser is poor or there is not appropriate encryption in place to secure the data. This behaviour is not related to anti-malware, however, the current study is interested in exploring if there are differences in the researched factors for those who do

accept the cookie compared to those who do not accept the cookie. This will allow an understanding of the effects of the factors on an objective behavioural measure rather than solely focusing on self-report measures.

Hypothesis$_{11:}$ There will be a significant difference in levels of the extended-PMT factors between those individuals who accept the cookie and those who do not

5.3 | METHOD

5.3.1 | DESIGN

A correlational design was adopted to understand the relationship between the predictors (threat, coping and additional factors) and outcome variables (intention to engage in the three behaviours).

5.3.2 | PARTICIPANTS

An opportunity sample of 526 (Age, M= 35.52, SD= 12.22) individuals were recruited online of which 124 did not complete the demographic section. 422 completed the SU section, 324 completed the AMS section and 428 completed the email section. All recruited participants were currently in full time or part time employment. 152 males and 243 females (6 participants chose not to disclose their gender) took part with an average organisational tenure of 6.19 years (SD=7.31) and job tenure of 3.81 years (SD 5.17). 36% of which had managerial responsibilities.

58% stated they had read their organisation's information security policy, 13% were unsure, 22% had never read the policy and the remaining 7% stated that their organisation did not have a policy in place. Of those who said yes, 10% had read the policy within the last month, 29% in the last 1-6 months, 18% had read it 6-12 months ago and 23% was more than a year ago, the remaining 20% were not sure. 8% were from a microenterprise (less than 10 staff), 9% from a small enterprise (less than 50 staff), 10% from a medium-sized enterprise (less than 250 staff) and 73% from a large organisation (more than 250 staff).

71% of employees used their desktop PC most for work tasks, 26% used a laptop, 1% their smartphone and 2% their tablet. 84% of employees worked from their company-owned device while 16% used a personally-owned device. 83% of employees used Microsoft Windows, 13% Mac OS X, 2% Linux, 2% iOS and 1% used Android.

Appendix K presents the organisational sectors recruited participants were from.

5.3.3 | MEASURES

Unless otherwise stated all items were measured on a 5 point Likert scale that ranged from strongly disagree to strongly agree.

Perceived Susceptibility was measured with 4 items. 2 items were taken from Johnston and Warkentin (2010) in which the security threat was changed from spyware to malware. 2 items were also based on Milne et al. (2002) and were re-worded to reflect the area of security e.g. "My chances of developing CHD in the future are" was changed to "My chances of infecting my work device with malware in the future are high". The scale had an internal reliability of α = .72. See Appendix M for full scale.

Perceived Severity was measured with 13 items. 3 items were based on Johnston and Warkentin (2010) such as "If my work device were infected by malware, it would be severe". The remaining 10 items were self-developed and were based on the findings from the qualitative study. The inclusion of these items was to target the four areas of potential consequences (technological, personal, 3rd party and organisational) to provide a more grounded and contextual perceived severity measure. An example item is "If my work device were infected by malware, I could be severely disciplined". The total scale had an internal reliability of α =.88. See Appendix M for full scale.

Security Responsibility was measured using a self-developed 7 item scale in which participants scored themselves on a 7-point visual analogue scale from "my company's responsibility" to "my responsibility". An example item is *"to install anti-*malware software on devices I use for work". The scale had an internal reliability of α =.81. See Appendix N for full scale.

Workplace Information Sensitivity Appraisal developed in Chapter 4 was used consisting of 17 items (see Appendix G). Participants were asked to select the information type that they worked with most which were those information types used within the previous study. Their WISA appraisal was then measured for this information type. The full-scale had an internal reliability of α = .78. The sub-scale for privacy was α = .82, consequences α = .79, worth α = .85, low proximity interest α = .75 and for high proximity interest α = .94.

Psychological ownership was measured using the same 4 items as Chapter 3, section 3.2.3.1 (see Appendix B). The full-scale had an internal reliability of α = .87. The sub-scale for data ownership had an internal reliability of α = .80 and for device ownership α =.87.

Past experience was self-developed and consisted of 12 items. 6 items measured employees' direct personal experience of the consequences of security breaches and the other 6 items measured experience of these breaches in the workplace. An example of an item "My personal account (e.g. email, social media) has been used by someone without my permission". Items were measured on a 3 point scale consisting of 'yes', 'no' and 'I don't know'. A total composite score was created to represent their security experience as a continuous variable. See Appendix O for full scale.

Organisational citizenship behaviour was measured using the same OCB-O scale as Chapter 3, section 3.2.3.1 consisting of 8 items (see Appendix A). The scale had an internal reliability of α =.85.

The following constructs were measured for each of the three security behaviours. All the items were the same except the beginning of the sentence; here it is represented as <security behaviour>.

Response efficacy was measured with 13 items. 3 items were based on Witte, Cmaeron, McKeon, and Berkowitz (1996) response efficacy template such as "<security behaviour> works in preventing malware". Additional items were included to assess ratings of response efficacy for avoiding the negative consequences associated with the security threat as previous studies mainly focus on threat reduction in response efficacy measures. In line with perceived severity, these targeted the four areas of threat consequences. An example item is "<security behaviour> works in protecting the reputation of my organisation". RE for AMS (α =.95), ES (α =.95) and SU (α =.95). See Appendix P for full scales.

Self-efficacy was measured with 4 items based on Milne et al. (2002) such as "I feel confident in my ability to <security behaviour>". SE for AMS (α =.85), ES (α =.84) and SU (α =.84). See Appendix Q for full scales.

Response costs were measured with 2 items based on Gurung et al. (2009). Security behaviours had additional items that were specific to their associated costs. Anti-malware software had an additional 7 items such as "Using the anti-malware software on my device to scan for malware would slow my device down". The security behaviour installing operating system updates had an additional 6 items such as "Installing operating system updates on my work device could lead to *a less reliable or 'buggy' software version being installed*". Finally, not clicking on URL links in suspicious emails had 4 additional items such as "not clicking on URL links in suspicious emails would affect my productivity at work". RC for AMS (α =.84), ES (α =.89) and SU (α =.87). See Appendix R for full scales.

Protection motivation was measured with 3 items based on Johnston and Warkentin (2010) such as "I intend to <security behaviour> in the next 2 weeks". <time element> was specific to situation. PM for AMS (α =.92), ES (α =.88) and SU (α =.93). See Appendix S for full scales.

Implicit security measure

Before starting the survey, participants were prompted with the following message:

*"This cookie s*tores basic user information on your computer, potentially improving the browsing experience and helping us deliver more relevant information to you. Do you want to *use this option?"*

Clicking "don't accept" was indicative of the secure behaviour (scored 1=accept, 2=don't accept). See Appendix T for prompted message.

5.3.4 | PROCEDURE

Table 27. Presentation of questionnaire sections and associated appendices

Section 1	Section 2	Section 3	Section 4	Section 5	Section 6	Section 7	Section 8
			<---order randomized---->				
Previous security breach experience and OCB	Devices used at work, psychological ownership and WISA	Malware threat perception	AMS items	SU items	ES items	Security responsibility	Demographics
Appendix O & Appendix A	Appendix L, Appendix B & Appendix G	Appendix M	Appendix P Appendix R Appendix S Appendix U	Appendix P Appendix R Appendix S Appendix U	Appendix P Appendix R Appendix S Appendix U	Appendix N	Appendix J

After consenting to take part, participants were presented with the implicit security task. They were then directed to the first section of the questionnaire which asked questions about their previous security breach experience and their levels of organisational citizenship. The second section questioned participants about the devices they used at work, psychological ownership and the WISA scale. Section 3 asked questions about employees' malware threat perception. Section 4, 5 and 6 were questions about employees' response evaluation of the three anti-malware behaviours, the order of these sections was randomised. Participants were presented with the AMS section if they answered "Yes" to whether their organisation allowed them to use USB sticks. Each section presented instructions to participants, explaining key terms and images to help participants with answering the survey items. Section 7 measured employees' levels of security responsibility. The final section took demographic information from participants. On completion, participants were given the option to enter a prize draw to win an iPad, thanked for their participation and were provided with debrief information.

5.4 | RESULTS

5.4.1 | DATA ANALYSIS STRATEGY

A multi-stage process was adopted to test the hypotheses. Firstly, relationships between the variables were identified. Following this, EFA was employed on constructs that had newly developed items; both established (perceived severity, response efficacy and response costs) and

new (psychological ownership and responsibility). Hierarchical regression was then employed to identify which factors from PMT and which additional factors predict behavioural intention. Finally, SEM was used to explore the hypothesised model and the findings from the regressions to ensure that the model is the best fit to the sampled data.

5.4.2 | PRELIMINARY ANALYSES

First, the data was screened for multi-collinearity, missing data and outliers. Variance Inflation Factors were checked for multi multi-collinearity issues, all factors ranged from 1.13 to 2.04 for all behaviours and therefore were below the conservative cut off of 3 (Bowerman & O'Connell, 1990; Petter, Straub, & Rai, 2007) indicating that multi-collinearity was not present. The data file was split into three components per behaviour and EM estimation was performed on the data to retain as many participants as possible. This was only permitted where items had less than 10% missing data. Inspection of the data indicated that there were no outliers. Correlational analyses were conducted to explore relationships between the study variables. See for Table 28 for descriptive statistics.

Table 28. Descriptive statistics for variables under investigation

Variable	Mean	SD
WISA Privacy	4.03	0.78
WISA Consequences	2.10	0.81
WISA Worth	4.40	0.68
WISA Low proximity	3.25	0.87
WISA High proximity	1.72	0.93
Perceived susceptibility	2.21	0.73
Perceived Severity - Overall	3.49	.66
Perceived Severity - Organisational	3.45	0.87
Perceived Severity - Consequences	3.54	1.00
Perceived Severity - Personal	3.03	0.99
Perceived Severity - Productivity	3.91	0.68
Organisational Citizenship Behaviour (OCB)	3.58	0.68
Personal security experience	1.89	0.25
Work security experience	2.05	0.38
Psychological ownership – Data	3.74	1.12
Psychological ownership – Technology	2.05	0.38
Responsibility	2.94	0.83
Self-efficacy (AMS security)	3.69	0.89
Response efficacy (AMS security)	3.72	0.63
Response costs (AMS security)	2.62	0.67
Self-efficacy (Email security)	4.52	0.72
Response efficacy (Email security)	4.08	0.64
Response costs (Email security)	1.55	0.81
Self-efficacy (SU security)	3.73	1.03
Response costs (SU security)	2.73	0.84
Response efficacy (SU security)	3.37	0.69

AMS intention	3.54	0.99
SU intention	3.32	1.1
ES intention	4.67	0.65

The means show that employees intended to perform the email security behaviour the most. The software update behaviour has the highest ratings of response costs, followed by the AMS behaviour and email security behaviour respectively. The email security behaviour has the highest ratings for response efficacy, followed by the AMS behaviour and SU behaviour. Ratings for self-efficacy perceptions are highest for the email security behaviour, followed by the SU behaviour and AMS behaviour.

Ratings for perceived susceptibility appear to be relatively low, whereas severity and its components appear to be high with productivity severity having the highest ratings. Employees have higher ratings for psychological ownership of data compared to technology. For the WISA scale employees' ratings of privacy, worth and low proximity appears to be high whereas consequences and high proximity appear to be lower. Finally, organisational citizenship behaviour and responsibility appear to be trending towards a medium level.

Appendix V shows the inter-correlations of the variables. Inspection of the inter-correlations revealed the presence of many significant correlations suggesting that there are relationships between the variables under investigation. There appears to be strong correlations between coping appraisal components (SE, RE and RC) and the three behavioural intentions. Interestingly, threat appraisal (severity and susceptibility) does not appear to correlate with any behavioural intentions. These relationships will be explored in more depth in the following analyses.

5.4.2.1 | Exploratory Factor Analysis

EFA was employed using PCA to explore the factor structure of the following constructs: response efficacy (for all 3 behaviours), security experience, responsibility and perceived severity. This was undertaken as these constructs were self-developed or expanded from previous instruments. Only perceived severity suggested a factorial structure beyond one factor and, therefore, was subjected to further analysis.

Using the same procedure as Chapter 4, two statistical tests were conducted to determine the suitability of the dataset for factor analysis. The analysis revealed that the KMO output was .85 indicating a "good" sample adequacy (Kaiser, 1974) and the BS test showed a significant result (BS x^2 (78) = 3099.20, p<.001). The findings from both tests, therefore, suggest that the data was suitable for EFA.

To explore the factor structure of perceived severity, PCA was performed using varimax with Kaiser normalization. The 13 items from the initial scale were entered into the factor analysis and factor loadings lower than .30 were suppressed. See Table 29 for factor loadings.

Table 29. Factor loadings for each item (factor loadings lower than .30 are suppressed)

Item - If my work device were infected by malware…	Rotation Factor Loadings			
	Factor 1: **Organisational consequences**	Factor 2: **Consequence severity**	Factor 3: **Personal consequences**	Factor 4: **productivity consequences**
…the consequences would be severe		.854		
…the consequences would be serious		.892		
…the consequences would be significant		.879		
…it would run significantly slower				.811
…my organisation's computer network could be severely disrupted	.612			
…I could be severely disciplined	.435		.670	
…I would be seriously embarrassed			.879	
…it could significantly reduce my productivity				.717
…there would severe complications for my organisation's service users/customers	.812			
…it could lead to my organisation having severely dissatisfied service users/customers	.844			
…there could be severe consequences to company data and files	.754			
…the organisation's image could be seriously damaged	.813			
Eigenvalues	**5.356**	**1.510**	**1.293**	**1.037**
REMOVED FACTORS — …my personal information and data could be severely at risk			.448	.452

The findings from the PCA revealed that four factors could explain the data, which accounted for 70.75% of the variance above the 60% minimum acceptable level (Hinkin, 1998). All eigenvalues were above 1 conforming to acceptable values as suggested by Hinkin (1998).

Most items were found to load onto a respective factor above the accepted .40 criterion level (Ford, MaCallum, & Tait, 1986). Two items cross-loaded onto another factor: "my personal information and data could be severely at risk" was removed as it did not load onto one factor more than the other and both levels were below .46. The second item, "I could be severely disciplined" loaded more onto factor 3 and conceptually seemed to link better to that factor as it is more at the level of a personal consequence than an organisational one. The item was therefore retained in factor 3 and will be further explored within the CFA.

Overall, the PCA revealed that the factors explained a large amount of the variance in the data and the items had strong factor loadings (above .40). The next stage was to confirm the four factors using CFA.

5.4.2.2 | Confirmatory Factor Analysis

CFA was tested on the data using AMOS (version 22) to explore the factor structure and estimate the degree to which the factor structure is a good fit to the data. The four factors constituting severity were presented as latent variables within AMOS and were permitted to co-vary. The items for each factor were only allowed to load onto their respective factor. Covariance between error terms was only allowed where items were related to the same factor following advice from modification indices within AMOS. Figure 28 shows the standardised item loadings for the hypothesised model.
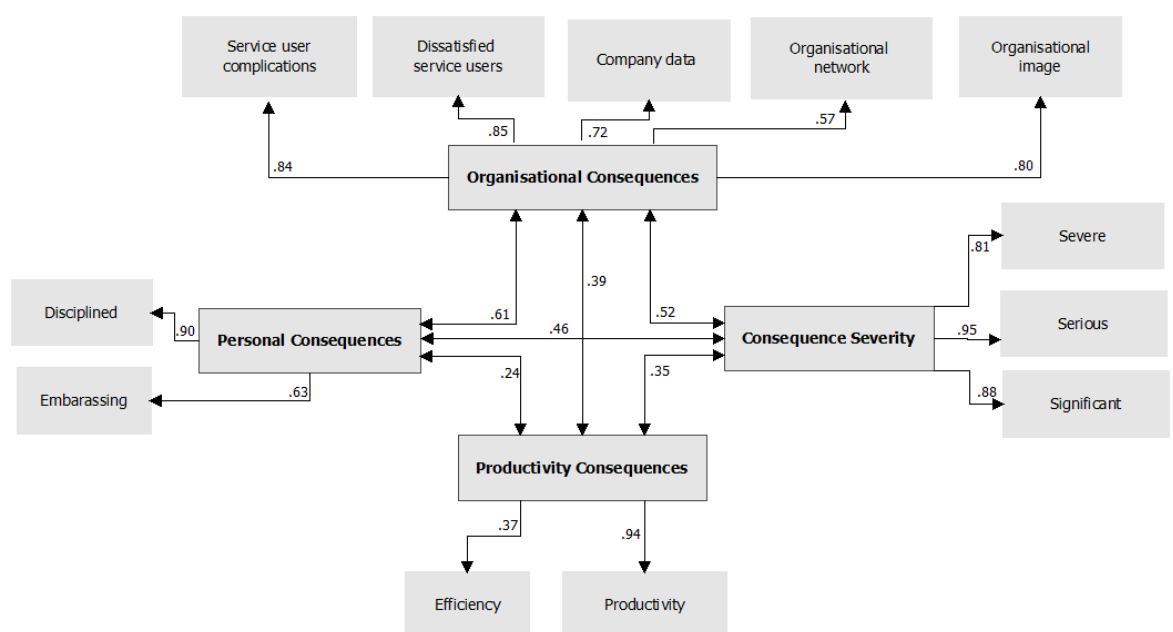
Figure 29. The perceived severity model with standardised path coefficients

159

The goodness-of-fit of the models was evaluated using the following absolute goodness-of-fit indices (Jöreskog & Sörbom, 1986): (1) the X2 goodness-of-fit statistic; (2) the Root Mean Square Error of Approximation (RMSEA); (3) the Goodness of Fit Index (GFI); (4) the Adjusted Goodness of Fit Index (AGFI) and (5) Comparative Fit Indices (CFI).

Table 30. Goodness-of-fit indices for perceived severity model

Model	X^2	RMSEA	GFI	AGFI	CFI
Perceived Severity Model	x^2 (47)=141.289, p<.001	.062	.958	.930	.971

The final model indicated a good level of fit for three of the four fit indices. GFI and AGFI were both above the cut-off point for a "good fit" (Hu & Bentler, 1995; Marsh & Grayson, 1995). RMSEA was smaller than .08 so led to model acceptance (Browne & Cudeck, 1992). The chi-square indicated that the model was not a good fit to the data for all information types, however, chi-squared has been criticised for being sensitive to large sample size especially if over 200 (Hoe, 2008), as in the case for the current study. The four factors were therefore considered to be a "good" fit to the data.

5.4.3 | EXPLORING THE THEORETICAL MODELS

5.4.3.1 | AMS security: Hierarchical Regression

Hierarchical regression was employed to explore the additional factors to the initial PMT framework. The first step included all predictors that had been previously explored in security research with protection motivation theory using the enter method. These were the following predictors: Susceptibility, self-efficacy, response efficacy, response costs and severity. The second step used the stepwise method to add each additional factor (responsibility, WISA, security breach experience, OCB, psychological ownership) to the initial PMT model.

Table 31. Coefficients for Model 1, Model 2 and Model 3 following hierarchical regression for AMS security

	B	SE B	β
Model 1			
Constant	-.222	.469	
Perceived Susceptibility	.091	.066	.066
Self-efficacy	.502	.055	.450***
Response efficacy	.286	.076	.182***
Response costs (R)	.274	.072	.184***
Perceived Severity (Organisational)	-.022	.068	-.002
Perceived Severity (Productivity)	-.017	.074	-.011
Perceived Severity (Personal)	-.012	.059	-.011
Perceived Severity (Consequences)	-.049	.053	-.048
Model 2			
Constant	-.792	.487	
Perceived Susceptibility	.081	.064	.059
Self-efficacy	.455	.056	.407***
Response efficacy	.279	.075	.178***
Response costs (R)	.269	.070	.181***
Perceived Severity (Organisational)	.036	.068	.030
Perceived Severity (Productivity)	-.005	.072	-.003
Perceived Severity (Personal)	-.026	.058	-.025
Perceived Severity (Consequences)	-.040	.052	-.040
Responsibility	.211	.058	.170***
Model 3			
Constant	-1.182	.507	
Perceived Susceptibility	.065	.064	.047
Self-efficacy	.469	.056	.420***
Response efficacy	.280	.074	.178***
Response costs (R)	.311	.072	.209***
Perceived Severity (Organisational)	.019	.068	.016
Perceived Severity (Productivity)	.005	.072	.004
Perceived Severity (Personal)	-.034	.058	-.032
Perceived Severity (Consequences)	-.038	.052	-.037
Responsibility	.195	.058	.157***
WISA (Consequences)	.152	.061	.117***

Note. R^2=.37 for step 1. ΔR^2=.02 for step 2. ΔR^2=.01 for step 3. ***p<.001.

The findings from the regression analyses (see Table 31) shows that model 1 is able to account for 37% of the variance in employees' intentions to scan USB sticks for malware (R^2 = .37, $F(8,315)$ = 22.72, p <.001) with self-efficacy as the strongest significant predictor (β = .50, $t(315)$ = 9.084, p <.001), followed by response costs (β = .184, $t(315)$ = 3.827, p <.001), and response efficacy (β = .50, $t(315)$ = 9.084, p <.001). The addition of responsibility contributed to an increase in R^2 of 2% in model 2 (R^2 = .39, $F(1,314)$ = 13.138, p <.001) in which responsibility was a significant predictor (β = .170, $t(314)$ = 3.625, p <.001). The final model, the addition of WISA consequences was a significant predictor (β = .117, $t(313)$ = 2.501, p <.001) and contributed to an increase in R^2 of 1% (R^2 = .40, $F(1,313)$ = 6.254, p<.05). The addition of responsibility and WISA consequences predicts unique variance in the behaviour.

Overall, the final model consisting of the following significant predictors (in order of contribution to regression): self-efficacy, response costs, response efficacy, responsibility and WISA consequences explain 40% of the variance in employees' intentions to scan USB sticks for malware.

5.4.3.2 | AMS security: Structural Equation Modelling
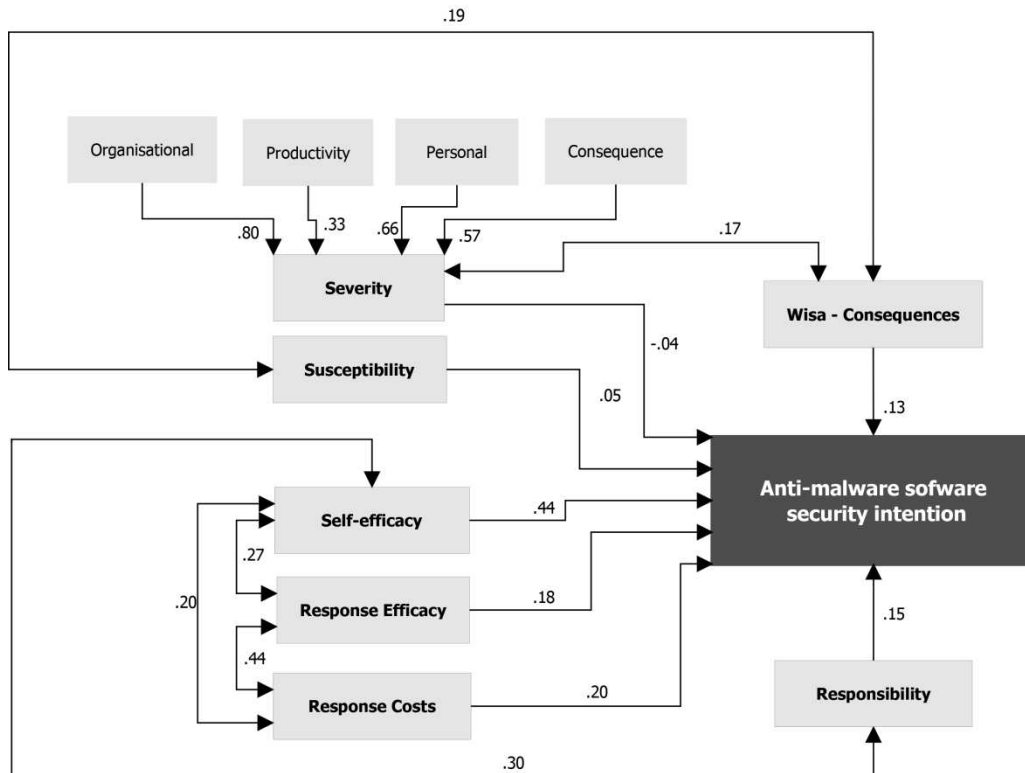
Figure 30. The extended PMT model with standardised path coefficients for AMS security

The model was then tested using SEM to ascertain how well the model explains the data. Severity remained as part of the model as its part of the original PMT. The chi-square indicated that model was not a good fit to the data, $x2$ (177)=386.195, p<.001. However, the fit indices for GFI and AGFI were .90 and .87 which are indicative of an acceptable fit. RMSEA was .051 and CFI was .95 which also indicated a good fit. Overall, the final model was a good fit to the sampled data for four out of the five goodness-of-fit indices.

Modification indices suggested covariance between some constructs that lead to a stronger fit, this was only between constructs derived from PMT e.g. constructs from response appraisal were allowed to co-vary. Suggested modifications were also allowed between PMT constructs and additional factors (Responsibility and WISA Consequences) as these were exploratory. These modifications had to make conceptual sense, for example, WISA Consequences is conceptually similar to severity and susceptibility but related to information so was allowed to co-vary.

Table 32. The regression weights and critical ratio values for the main effects of the hypothesised model

Parameter	Unstandardised (standardised) Path Coefficient	Critical Ratio (CR)	P
Self-efficacy→ Intention	.278 (.439)	7.432	<.001*
Response efficacy→ Intention	.070 (.178)	3.712	<.001*
Response costs → Intention	.155 (.195)	3.738	<.001*
Severity → Intention	-.061 (-.041)	-.783	.434
Susceptibility → Intention	.032 (.054)	1.146	.252
WISA (Consequences) → Intention	.179 (.134)	2.904	.004*
Responsibility → Intention	.066 (.023)	2.898	.004*

For threat appraisal, neither severity nor susceptibility had a significant positive relationship with intention therefore not supporting hypothesis 1 or 2. The findings from the regression and SEM indicated that coping appraisal had the biggest influence on intention. Within coping appraisal, self-efficacy had a significant positive relationship with intention and was the strongest predictor of the behaviour as shown in Table 32. Self-efficacy had the strongest standardised path coefficient (.439), followed by response costs (.195) and response efficacy (.178). Reponse costs (R) had a significant positive relationship with intention, indicating that low levels of response costs influence intentions to scan USB sticks for malware. Finally, response efficacy also had a significant positive relationship with intention. Hypotheses 3, 4 and 5 were therefore supported.

The additional factors of responsibility and WISA (consequences) were found to significantly relate to intention supporting hypothesis 8 and providing partial support for hypothesis 7. Hypothesis 7 was partially supported as only 1 component of WISA was supported. The findings indicated no relationship between; experiences (H2), psychological ownership (H9) and OCB (H10) on intention.

Overall, the modified PMT model was a good fit to the sampled data of employees and the regression analysis indicated that the final model could explain 40% of the variance in employees' intentions to scan USB sticks for malware.

5.4.3.3 | Software updates: Hierarchical Regression

Table 33. Coefficients for Model 1 and Model 2 following hierarchical regression for SU security

	B	SE B	β
Model 1			
Constant	-.883	.459	
Perceived Susceptibility	.237	.066	.155***
Self-efficacy	.118	.050	.110*
Response efficacy	.504	.073	.315***
Response costs (R)	.328	.064	.250***
Perceived Severity (Organisational)	-.057	.072	-.044
Perceived Severity (Consequences)	.079	.055	.072
Perceived Severity (Personal)	-.033	.056	-.030
Perceived Severity (Productivity)	.123	.075	.075
Model 2			
Constant	-1.405	4.75	
Perceived Susceptibility	.212	.066	.139***
Self-efficacy	.080	.050	.075
Response efficacy	.487	.072	.304***
Response costs (R)	.329	.063	.252***
Perceived Severity (Organisational)	-.001	.072	-.001
Perceived Severity (Consequences)	.082	.054	.074
Perceived Severity (Personal)	-.070	.056	-.064
Perceived Severity (Productivity)	-135	.074	.083
Responsibility	.217	.060	.161***

Note. R^2=.27 for step 1. ΔR^2=.02 for step 2. *p<.05 **p<.01 ***p<.001.

The findings from the regression analyses, as shown in Table 33, shows that model 1 is able to account for 27% of the variance in employees' intentions to install software updates (R^2 = .27, $F_{(8,413)}$ = 18.663, p <.001) with response efficacy as the strongest significant predictor *(β = .315, t(413) = 6.921, p <.001)*, followed by response costs *(β = .250, t(413) = 5.251, p <.001),* and perceived susceptibility *(β = .155, t(413) = 3.226, p <.01).*

In the final model, the addition of responsibility was a significant predictor *(β = .161, t(412) =* 3.599, p <.001) and contributed to an increase in R^2 of 2% (R^2 = .29, $F_{(1,412)}$ = 12.954, p<.001) predicting unique variance in the behaviour.

Overall, the final model consisting of the following significant predictors (in order of contribution to regression); response efficacy, response costs, perceived susceptibility, and responsibility explain 29% of the variance in employees' intentions to install software updates.

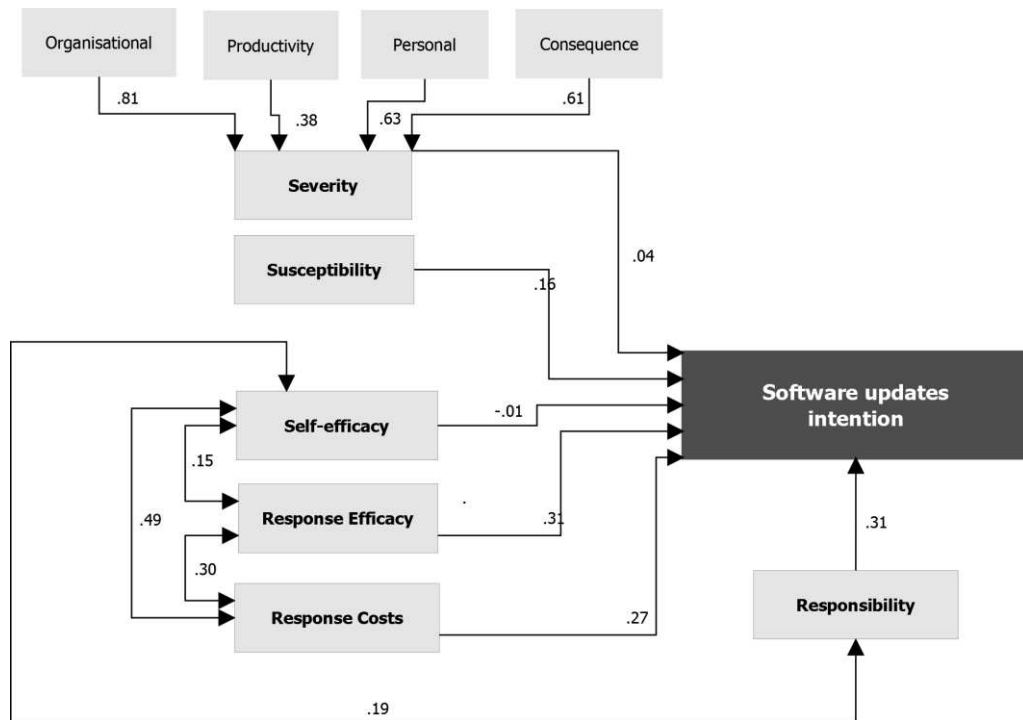### 5.4.3.4 | Software updates: Structural Equation Modelling

Figure 31. The extended PMT model with standardised path coefficients for SU security

The chi-square indicated that the model was not a good fit to the data, x^2 (45)=142.056, p<.001. However, the fit indices for GFI and AGFI were .91 and .88 which are indicative of a good fit. Finally, RMSEA was .065 and CFI was .94 which also indicated a good fit. Overall, the final model was a good fit to the sampled data for four out of the five goodness-of-fit indices.

Table 34. The regression weights and critical ratio values for the main effects of the hypothesised model

Parameter	Unstandardised (standardised) Path Coefficient	Critical Ratio (CR)	P
Self-efficacy → Intention	-.008 (-.013)	-.247	.805
Response efficacy → Intention	.094 (.307)	6.372	<.001*
Response costs → Intention	.160 (.271)	4.780	<.001*
Severity → Intention	.158 (.041)	.824	.410
Susceptibility → Intention	.134 (.157)	2.695	.007*
Responsibility → Intention	.071 (.188)	3.853	<.001*

As shown in Table 34, response efficacy had the strongest standardised path coefficient and a significant positive relationship with intention, thus supporting hypothesis 4. Response costs also had a significant positive relationship with intention and, therefore, hypothesis 5 was supported. Self-efficacy was the only component of coping appraisal not to significantly relate to intention, its standardised path coefficient indicates a marginally negative relationship which is in the opposite direction what was hypothesised (H3).

For threat appraisal, susceptibility had a significant positive relationship with intention, therefore, supporting Hypothesis 2. However, severity did not have a significant positive relationship with intention and hHypothesis 1 was therefore not supported.

For the additional constructs, responsibility was found to have a significant positive relationship with intention supporting hypothesis 8. OCB, WISA, psychological ownership and experience did not significantly relate to intention and therefore, Hypothesis 6, 7, 9 and 10 were not supported.

Overall, the modified PMT model was a good fit to the sampled data of employees and the regression analysis indicated that the final model 29% of the variance in employees' intentions to install software updates.

5.4.3.5 | Email security: Hierarchical Regression

Table 35. Coefficients for Model 1 and Model 2 following hierarchical regression for ES security

	B	SE B	β
Model 1			
Constant	1.937	.243	
Perceived Susceptibility	-.065	.034	-.073
Self-efficacy	.416	.041	.485***
Response efficacy	.094	.042	.092*
Response costs (R)	.138	.037	.172***
Perceived Severity (Organisational)	-.032	.035	-.043
Perceived Severity (Consequences)	.042	.028	.064
Perceived Severity (Personal)	-.017	.029	-.026
Perceived Severity (Productivity)	.008	.038	.008
Model 2			
Constant	1.969	.241	
Perceived Susceptibility	-.091	.035	-.102*
Self-efficacy	.415	.040	.484***
Response efficacy	.092	.041	.089*
Response costs (R)	.144	.037	.180***
Perceived Severity (Organisational)	-.024	.035	-.032
Perceived Severity (Consequences)	.040	.028	.062
Perceived Severity (Personal)	-.022	.028	-.034
Perceived Severity (Productivity)	-.001	.038	-.001
Experience work	.084	.028	.110**

Note. R^2=.46 for step 1. ΔR^2=.01 for step 2. *p<.05 **p<.01 ***p<.001.

The findings from the regression analyses suggested that the final model accounted for 47% of the variance in employees' intentions to not click on suspicious links within emails. Self-efficacy was found to contribute the most, followed by response costs, security breach experience at work, susceptibility and response efficacy.

The findings from the regression analyses, as shown in Table 35, shows that model 1 is able to account for 46% of the variance in employees' intentions to not click on links in suspicious emails (R^2 = .46, $F(8,419)$ = 44.655, p <.001) with self-efficacy as the strongest significant

predictor *(β = .485, t(419) = 10.190, p <.001)*, followed by response costs *(β = .172, t(485) =* 3.708, p < .001) and response efficacy *(β = .092, t(419) = 2.214, p <.05).*

In the final model, the addition of security breach experience at work was a significant predictor *(β = .110, t(418) = 2.954, p <.01),* alongside contributing susceptibility to the prediction *(β = -* .102, t(418) = -2.592, p <.01) led to an increase in R^2 of 1% (R^2 = .47, F(1,418) = 8.725, p<.01).

Overall, the final model consisting of the following significant predictors (in order of contribution to regression); self-efficacy, response costs, security breach experience at work and perceived susceptibility explain 47% of the variance in employees' email security behaviour.

5.4.3.6 | Email Security: Structural Equation Modelling
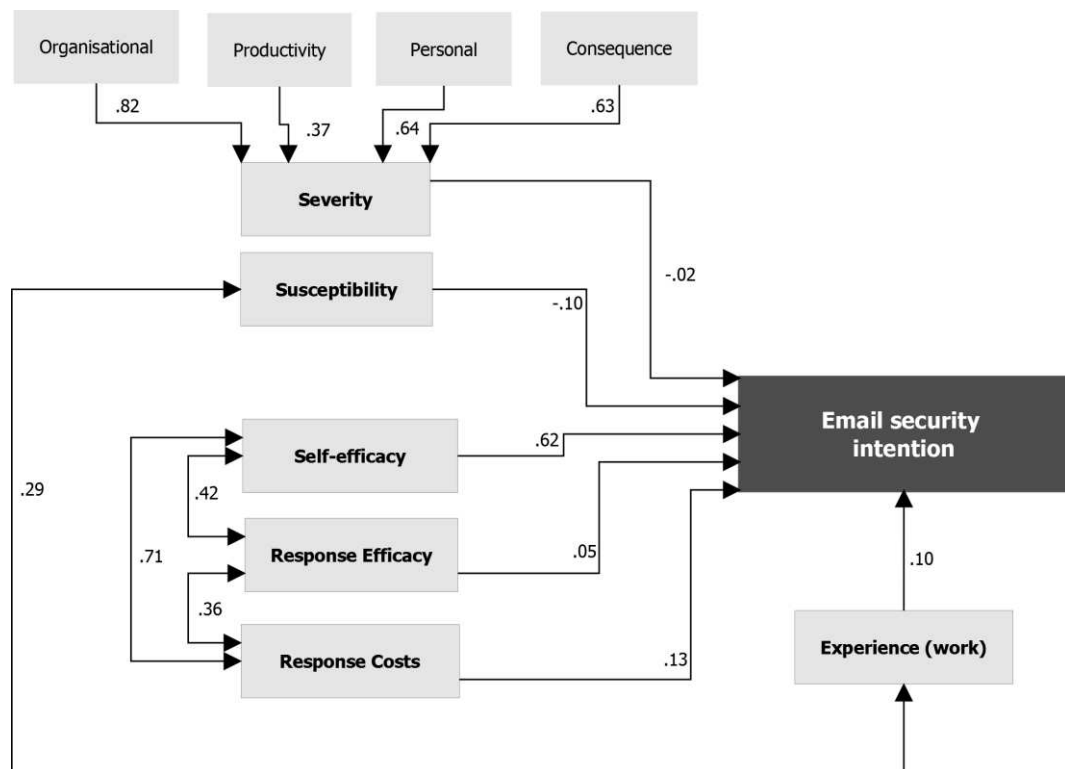
Figure 32. The extended PMT model with standardised path coefficients for email security

The chi-square indicated that model was not a good fit to the data, x^2 (143)=309.098, p<.001. However, the fit indices for GFI and AGFI were .93 and .91 which are indicative of a good fit. Finally, RMSEA was .05 and CFI was .97 which also indicated a good fit. Overall, the final model was a good fit to the sampled data for four out of the five goodness-of-fit indices.

Table 36. The regression weights and critical ratio values for the main effects of the hypothesised model

Parameter	Unstandardised (standardised) Path Coefficient	Critical Ratio (CR)	P
Self-efficacy → Intention	.252 (.615)	8.539	<.001*
Response efficacy → Intention	.011 (.049)	1.182	.237
Response costs → Intention	.045 (.128)	2.323	.020*
Severity → Intention	-.018 (-.020)	-.493	.622
Susceptibility → Intention	-.079 (-.105)	-.2491	.013*
Security breach experience (work) → Intention	.078 (.117)	3.080	.002*

The findings indicated that coping appraisal had the biggest influence on intention. Within coping appraisal, self-efficacy had a significant positive relationship with intention and was the strongest predictor of the behaviour as shown in Table 36. Response costs also significantly predicted intention. Hypothesis 3 and 5 were therefore supported. Response efficacy was a significant predictor within the hierarchical regression. However, this was not supported in the SEM. Hypothesis 4 is therefore partially supported.

Security breach experience at work was also found to have a significant positive relationship with intention supporting H6b. WISA (H7), responsibility (H8), psychological ownership (H9) and OCB (H10) did not significantly relate to intention.

For threat appraisal, severity had a marginally negative relationship with intention but it was non-significant, thus not supporting hypothesis 1. Susceptibility did significantly relate to intention but this was negative and in the opposite direction to what was hypothesised, therefore not supporting hypothesis 2.

Taken together, the modified PMT model was a good fit to the sampled data of employees and the regression analysis indicated that the final model could explain 47% of the variance in employees' email security behaviour.

5.4.4 | IMPLICIT SECURITY TASK

Logistic regression was performed to explore which factors predict whether individuals' accepted or did not accept the use of a cookie using stepwise-forward method for participants who completed all sections of the survey (n=278). Don't accept (17%) and accept (83%).

Table 37. Coefficients of the model predicting whether the participant accepted the cookie

		95% CI for the Odds Ratio		
Variable	B(SE)	Lower	Odds Ratio	Upper
Constant	2.888(.582)			
Perceived Susceptibility	-.555* (.231)	.365	.574	.903

R^2 = .021 (Cox & Snell), .035 (Nagelkerke), .035 (Hosmer & Lemeshow) Model $\chi^2(2)$ = 5.913, p<.05.
* p<.05, **p<.001

The full model was tested against a constant only model and it was found to be statistically significant, indicating that the only predictor (susceptibility) reliably distinguished between accepters and decliners of the cookie ($\chi^2(2)$ = 5.913, p<.05). Nagelkerke's R^2 .035 indicated a low effect size between the prediction and cookie acceptance. The findings indicate that as the level of perceived susceptibility of malware increases, the likelihood of cookie acceptance decreases.

5.4.5 | EXPLORING THE EFFECTS OF EXPERIENCE MEDIATED BY THREAT AND COPING APPRAISAL

To further explore Hypothesis 6a, a mediation analysis was employed to explore whether experience was mediated by the PMT components. Before proceeding with mediation analysis, four conditions must be met. Baron and Kenny (1986) outline the four conditions to determining mediation

1. IV (experience – personal or work) predicts the DV (AMS, SU or ES intention)
2. IV predicts the mediator (threat and coping appraisal constructs)
3. The mediators predict the DV while controlling for the IV
4. IV does not predict the DV (when controlling for the mediator)

Multiple regression analyses were conducted to explore the first condition for work and personal security experience on AMS, SU and ES intention. Personal security experience did not significantly predict AMS intention (β=-.009, SE=.261, p=.874, R^2=.00), SU intention (β=-.058, SE=.248, p=.252, R^2=.00) and ES intention (β=-.069, SE=.130, p=.167, R^2=.00). As condition 1 was not met for personal security experience, full mediation was not employed.

Security experience at work did not significantly predict AMS intention (β=-.271, SE=.177, p=.127, R^2=.01) and SU intention (β=-.158, SE=.154, p=.306, R^2=.00). However, it did significantly predict ES intention (β=-.248, SE=.086, p<.01, R^2=.02). Further analysis was

therefore employed to explore work security experience mediated through threat and coping appraisal on ES intention.

For condition 2, the findings from the earlier hierarchical regression showed that self-efficacy (β=484, SE=.040, p<.001), susceptibility (β=-.091, SE=.241, p<.05), response efficacy (β=.089, SE=.041, p<.05) and response costs (β=.180, SE=.037, p<.001) significantly predicted ES intention.

Further meditation analysis was performed to explore security experience at work mediated through self-efficacy, susceptibility, response efficacy and response costs. The results indicated that there was no significant indirect effect of experience on ES intention through; response efficacy (b= -.060, BCa CI [-.153, .000]), self-efficacy (b= -.098, BCa CI [-.260, .073]), response costs (b= -.045, BCa CI [-.120, .067]) and susceptibility (b= -.00, BCa CI [-.056, .066]). The findings, therefore, suggest that experience is not mediated by threat or coping appraisal but only has a direct effect on ES intention in isolation as shown by the findings of the SEM.

5.4.6 | FURTHER EXPLORATION OF RESPONSE EFFICACY AND RESPONSE COSTS

5.4.6.1 | Response efficacy perceptions

A repeated measures MANOVA was conducted to explore whether there were differences in efficacy perceptions across the three anti-malware behaviours (n=311)

Table 38. The means (and standard deviations) for response efficacy perceptions by behaviour

Response efficacy perception	AMS	SU	ES
Protecting my personal data	3.75 (.77)	3.47 (.82)	4.23 (.74)
Reduce likelihood of getting malware	3.94 (.73)	3.54 (.84)	4.22 (.75)
Protecting my productivity	3.85 (.75)	3.50 (.82)	4.17 (.69)
Effective in preventing malware	3.79 (.74)	3.38 (.82)	4.14 (.78)
Securing my organisation's data and files	3.79 (.76)	3.47 (.83)	4.13 (.73)
Effective in preventing embarrassment	3.56 (.82)	3.23 (.84)	4.11 (.77)
Works in preventing malware	3.85 (.74)	3.38 (.83)	4.10 (.75)
Works in ensuring that my work device runs as efficiently as possible	3.72 (.79)	3.67 (.81)	4.09 (.79)
Preventing problems for my organisation's service users/customers	3.79 (.75)	3.38 (.82)	4.07 (.80)
Protecting network from malware	3.78 (.79)	3.50 (.81)	4.00 (.82)
Protect organisation's reputation	3.57 (.83)	3.36 (.85)	3.84 (.86)
Prevents dissatisfied service users	3.59 (.84)	3.33 (.84)	3.82 (.89)
Reduces chances of getting disciplined	3.32 (.92)	2.94 (.89)	3.51 (.97)
	3.71 (.17)	**3.40 (.18)**	**4.03 (.20)**

The MANOVA revealed that there was a significant main effect of behaviour on response efficacy ratings for all behaviours (p<.01). Pairwise comparisons (see Appendix W) revealed that the email behaviour response efficacy ratings were significantly higher for all efficacy perceptions compared to the AMS behaviour and software update behaviour (p<.01). The AMS behaviour also had significantly higher efficacy ratings compared to the software update behaviour (p<.01) except for beliefs that the behaviours work in ensuring that the device runs as efficiently as possible.

5.4.6.2 | Response costs perceptions

Response costs are different for each behaviour; it was therefore not possible to compare differences by item using inferential statistics. They are presented together in the table below to allow comparisons for items that are the same. See Appendix X for pairwise comparisons for each behaviour.

Table 39. Means (and standard deviations) of the response costs perceptions for scanning USB sticks with anti-malware software (n=422), Installing software updates and for not clicking on URL (n=422) and not clicking on links in suspicious emails (n=428)

Response cost perception	AMS Mean	SU Mean	ES Mean
...would slow my work device down	3.28 (.97)	2.74 (1.05)	1.61 (1.03)
...would reduce my productivity	3.42 (.91)	2.66 (1.05)	1.58 (.97)
...can lead to non-malicious files being identified as infected with malware	2.92 (.93)	-	-
..would be time consuming	3.05 (.99)	2.91 (1.1)	1.54 (.90)
...could lead to important files being destroyed	3.47 (.93)	2.58 (1.09)	
...would require considerable effort	3.59 (.94)	2.49 (1.07)	1.47 (.84)
...would have a considerable financial cost for me	3.91 (.90)	-	-
...could lead to a less reliable or 'buggy' software version being installed	-	3.00 (1.07)	-
	3.38 (.33)	**2.73 (.20)**	**1.55 (.06)**

Of the three behaviours, AMS was perceived to be most costly followed by the SU behaviour and the ES behaviour. This trend follows for shared items; requiring effort, reducing productivity and slowing down their work device.

5.4.7 | OVERALL FINDINGS SUMMARY

Table 40. The hypothesised relationships for the three anti-malware behaviours and whether the hierarchical regression (HR) or structural equation modelling (SEM) supports the hypothesis

Hypothesis	AMS		SU		ES	
	HR	SEM	HR	SEM	HR	SEM
H1: Severity -> Intention	NS	NS	NS	NS	NS	NS
H2: Susceptibility -> Intention	NS	NS	S	S	S (-)	S (-)
H3: Self-efficacy -> Intention	S	S	NS	NS	S	S
H4: Response efficacy -> Intention	S	S	S	S	S	NS
H5: Response costs -> Intention	S	S	S	S	S	S
H6a: Experience -> Threat and Coping Appraisal	NS	NS	NS	NS	NS	NS
H6b: Experience -> Intention	NS	NS	NS	NS	S	S
H7: WISA -> Intention	PS	PS	NS	NS	NS	NS
H8: Responsibility -> Intention	S	S	S	S	NS	NS
H9: Psychological ownership -> intention	NS	NS	NS	NS	NS	NS
H10: OCB -> Intention	NS	NS	NS	NS	NS	NS

*Supported (S), Not supported (NS), Partially Supported (PS)

Overall, the findings indicate that the significant negative relationship between response costs and intention is the most consistent across the three behaviours. The relationship between response efficacy and intention is also consistent across the three behaviours. There appears to be differences in behaviour as the positive influence of self-efficacy is important for the AMS security and ES security behaviour but not for SU security. Responsibility has a significant positive relationship to intention for AMS security and SU security but not for ES security. The positive relationship between severity and intention is not supported for any of the behaviours, and the positive relationship between susceptibility and intention is inconsistent as the direction is supported for SU security but in the opposite direction for ES security. The findings also demonstrate support for the additional constructs; WISA for AMS security, experience for ES security and responsibility for AMS and SU security.

In summary, the behaviours are influenced by (in order of strength):

- AMS security – self-efficacy, response costs, response efficacy, responsibility and WISA (consequences)
- SU security – response efficacy, response costs, responsibility and susceptibility
- ES security – self-efficacy, response costs, experience (work), susceptibility and response efficacy

5.5 | DISCUSSION

5.5.1 | INFLUENCES ON MOTIVATIONS TO PERFORM ANTI-MALWARE BEHAVIOURS

5.5.1.1 | Coping appraisal

Within coping appraisal, lower levels of response costs were significantly related to intention for all behaviours indicating that higher levels of response costs lead to lower levels of motivation for all three behaviours. When comparing all three behaviours, response costs was strongest for the anti-malware software behaviour, followed by software updates and finally, the email security behaviour. Employees who perceive that anti-malware behaviours have lower costs (such as productivity, effort and time) are more likely to intend to perform the behaviours, suggesting that costs are a potential barrier to security behaviour.

The relationship between response costs and security behaviour is consistent with studies exploring the relationship with anti-spyware software in consumers (Chenoweth et al., 2009; Liang & Xue, 2010), and adds to the body of knowledge in this underexplored area and costly security in general (e.g. Beautement et al., 2009). For email security behaviour, Ng et al., (2009) found no support for a negative relationship between response costs and engagement in employees' email security behaviour for virus prevention. They had a particular focus on email attachments, whereas the current study was concerned with suspicious links. The differences could be due to employees perceiving "being cautious with attachments" as less costly than checking suspicious links. Additionally, the employment sample of the Ng et al. (2009) study was primarily IT organisations, whose staff may have higher awareness and knowledge of security so may not perceive security behaviours to be as costly as non-IT employees (as used in the current study). The current study used a cross-section of employees from different organisations and found support for the role of response costs that may explain the inconsistent finding by Ng et al. (2009).

Response efficacy was also shown to be a key influencer of motivation to follow anti-malware security behaviours. The relationship between response efficacy and intention was highest for the AMS security. Response efficacy has been regarded as one of the worst predictors of compliance and IS misuse in the workplace (Sommestad et al., 2014) as the existing research has been inconsistent either supporting a positive relationship (Ifinedo, 2011; Wall et al., 2013; Zhang & McDowell, 2009), a negative relationship (Vance et al., 2012) or finding no relationship (Siponen et al., 2010). The current study shows that response efficacy is important for security behaviour when focusing on specific behaviours and security threats. This is in line with PMT which posits that adaptive behaviour is enhanced by beliefs that it is effective in reducing threat. Employees perceive that all three behaviours are important in reducing malware

threats, and their associated consequences. Of three behaviours, the ES behaviour was perceived to be the most effective in preventing malware, followed by the AMS behaviour and finally, the SU behaviour. Employees may be unaware of how a system that is not updated is vulnerable to be compromised by malware and associate software updates more with improving device efficiency, the perception that was rated highest for this behaviour. This finding indicates that the connection between software updates and malware may need to be improved to heighten employees' response efficacy perceptions.

The influence of self-efficacy was supported for the AMS and ES security behaviour but not for the software update behaviour. Self-efficacy was the strongest predictor for both the AMS and ES behaviour. The lack of support for the SU behaviour indicates that employees beliefs in their capabilities is not important for installing software updates when prompted. This highlights that perceptions of capability is not important for all security behaviours, installing software updates may be perceived as an easy behaviour to perform as this often involves responding to a dialog box and, therefore, other factors may be better able to explain the lack of engagement. On the other hand, the AMS and ES security behaviours require a level of skill. The first requires the user to know how to access and run the AMS software and the ES behaviour requires the users to have the ability to detect suspicious links. The current study supports the existing research on the role of self-efficacy in using anti-spyware software (Gurung et al., 2009; Lee & Kozar, 2008; Liang & Xue, 2010; Sriramachandramurthy et al., 2009) and those exploring email security behaviour in relation to malware threats (Ng et al., 2009). Self-efficacy is also consistently supported in the IS compliance literature. There is little research looking at software update behaviour. However, the current study suggests that for passive behaviours that require less input from the user, self-efficacy may not be important for motivating employees to undertake them.

5.5.1.2 | Threat appraisal

The current study provided greater insight into the complexities and inconsistencies surrounding the support for and against threat appraisal in security research. Following factor analysis, perceived severity was found to comprise of four components (organisational, personal, productivity and consequences). However, these components did not significantly relate to intention. The current study does not support previous research showing a significant relationship between perceived severity and compliance intention (Chenoweth et al., 2009; Gurung et al., 2009; Siponen et al., 2014; Vance et al., 2012) and intentions to adopt anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009; Liang & Xue, 2009). However, the current study does support Lee et al. (2008) who found that severity did not affect anti-virus protection behaviours. Ng et al. (2009) found that severity did not have a significant effect on being cautious with emails with attachments but had moderating effects on other variables that

influenced security behaviour. The lack of support could be due to a number of factors. Firstly, there are few studies exploring specific security threats in the workplace as the majority that do focus on particular types (e.g. malware) have been within a consumer population. This study, alongside Ng et al. (2009), are the only studies to explore malware threats in an employment sample and both did not find a direct relationship to intention. Within the workplace setting, employees may perceive the severity of malware threats to be less severe. The consequences of malware to consumers are different to that of organisations as there is greater potential for complications for individuals including loss of personal data, performance disruption of their personal devices and the potential for identity theft. In the workplace, people may be less concerned with the severity of security threats as the personal consequences may not be seen as great. The lack of support could reflect the security threat under investigation; employees may lack awareness of the consequences of malware in the workplace. There is little research exploring whether employees' severity perceptions differ depending on organisational and personal consequences. The current study broke down severity into both organisational consequences and personal consequences (e.g. productivity, embarrassment) and found that neither influenced security behaviour. Meta-analytic research exploring the efficacy of PMT in other domains has found that severity and intention have the weakest association amongst all of the PMT relationships (Milne et al., 2000). The current study suggests that employees' perceptions of the severity of malware are not important for driving anti-malware behaviour.

The second aspect of threat appraisal, susceptibility, was also found to have a complicated relationship with security behaviour. The current study found that it was a significant predictor of software update intention and the cookie acceptance task. This partially supports research by Lee et al. (2008) who found that susceptibility was a significant predictor of virus protection behaviours, one of which was installing OS updates. The current study found that susceptibility did not predict AMS security behaviour which is supportive of other research that has found no role for susceptibility in consumers use of anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009). This further highlights that factors play differing roles for each security actions. The SU behaviour and cookie behaviour rely on prompts either from the computer or a website, whereas the AMS security behaviour relies solely on the employee to scan the USB stick in which case other factors such as those pertaining to ability evaluation (i.e. self-efficacy) may be more important in motivating the behaviour. This is somewhat confirmed by the current studies' findings as self-efficacy was not a significant influencer for the software update behaviour or the cookie acceptance task. When ability is not a requirement for security behaviour, threat appraisal may, therefore, play more of an important role.

The relationship between susceptibility and the ES behaviour was in the opposite direction to the hypothesis with lower levels of susceptibility indicative of greater motivation to perform the

behaviour. This is unexpected, as according to PMT, individuals with greater perceived susceptibility to malware would be more likely to adopt behaviours to mitigate it. This negative relationship may relate to the behaviour in reducing malware threats as phishing emails are often more associated with information disclosure or phishing scams (Getsafeonline.org, 2015) rather than the distribution of malware. There is a lack of research in exploring malware and email behaviour, however, Ng et al. (2009) found that susceptibility of malware attachments influenced cautious email behaviour. There may be differences in relation to link behaviour in emails, employees may not perceive email links to be associated with malware threats but may have a greater awareness of the likelihood of attachments being infected with malware. The majority of research exploring organisational security behaviour has been supportive of the link between susceptibility and behaviour, however, a number of these studies do not focus on specific security threats (Herath & Rao, 2009b; Ifinedo, 2011; Siponen et al., 2014). The current study explored a specific security threat: malware and found malware susceptibility to have differing effects on behaviours highlighting users' inability to connect behaviour to threats.

Overall, employees' malware susceptibility perceptions were low. This may be consistent with the tendency for individuals to believe that they are more likely than others to experience positive events in their lives and less likely to experience negative events. This has been referred to as optimism bias (Weinstein, 1980) where peoples' perceived susceptibility is unrealistically positive so they engage in protective behaviours less. This may account for the low levels of susceptibility within the employees and differences for its influence on the security behaviours. Optimism bias is most likely to occur for events that have a high degree of perceived control (Harris, 1996; Weinstein, 1980). Employees may perceive that malware received via email is under greater control as they can engage in multiple behaviours that directly prevent the threat at this medium (e.g. checking links and not opening attachments); whereas malware received from browsing the internet or distributed via removable media may be seen as less controllable. Software update behaviour is important for reducing malware threats; however an employee may not be aware of this. Malware that has exploited these vulnerabilities may be seen as less controllable (as users are often unaware of how malware has compromised their system) and therefore, less open to optimism bias. This may account for differences in the positive and negative direction of effects for susceptibility on these behaviours.

The complicated role of susceptibility on security behaviour is supported by research by Boehmer et al. (2015) who found that moderate levels of susceptibility were associated with lower levels of security behaviour in students but individuals with a high or low threat susceptibility perception engaged in higher levels of security behaviour. They argue that undertaking safe behaviour may cause their threat perception to be low as those who engage in the protective actions may perceive they are not vulnerable because they perform the behaviour.

This explanation may also explain the negative relationship to the ES security behaviour in the current study.

Experience of security issues at work were also found to significantly influence the ES security behaviour. After self-efficacy, it was the strongest predictor of the behaviour indicating that experience of the negative aspects of security/computer related issues in the workplace influences email-related security behaviour. Experience is considered within PMT to directly influence threat and coping appraisal. However, the current study found that it was not mediated by the threat and coping appraisal on intention. The role of experience is relatively understudied in existing research focusing on PMT in security research. However, the findings do support the qualitative study (Chapter 3) which found that experiencing the negative consequences of security threats influence current behaviour. The current study suggests that experience has a direct role in some behaviours, as it did not relate to the AMS or SU behaviour. For ES security, experiencing the negative consequences of security issues may promote awareness and greater detection surrounding email phishing.

5.5.1.3 | Additional factors

The current study found that the WISA factors did not influence SU or ES security. There was partial support for the AMS security behaviour in which the consequences component of WISA significantly related to intention, suggesting that employees who have a greater perception that the disclosure of the data they work with has consequences (such as compromising and discreditable) intend to scan USB sticks with AMS to protect the information. Employees working with information that has the potential for serious consequences if disclosed may, therefore, have greater motivation to protect it in relation to USB stick usage and anti-malware software. This was the first study to specifically explore the role of WISA for a particular security threat and sub-set of behaviours. Chapter 4 found that the WISA scale explained greater variance in security behaviours relating to access control and physical security. The WISA scale may play more of a role in behaviours that have a direct link to information and data that employees work with. The connection between malware prevention and data sensitivity may not be clear compared to other behaviours such as physical security that is physically protecting information and assets. Further work is required to explore the WISA scale for other behaviours, particularly those where its links to information protection are clearer such as access control.

The current study found that responsibility was a strong predictor of AMS security and SU security. Individuals with higher perceptions of personal responsibility for security had greater motivation to undertake anti-malware actions. There was no support for the email security behaviour which suggests that other factors may be more important for influencing email

behaviours. This supports the findings from the qualitative study (chapter 3, section 3.3.2.6) that employees may diffuse responsibility onto third parties for certain behaviours. Interestingly, the qualitative study suggested that employees were more likely to perceive behaviours such as virus prevention as the responsibility of their organisation. However the current study suggests that employees with a sense of responsibility for security are likely to undertake anti-malware behaviours pertaining to use of anti-malware software and installing software updates. On the other side, lower levels of personal responsibility may lead to lower levels of security engagement for malware prevention. Empowering users with a sense of responsibility is, therefore, important to promote uptake of behaviours. The lack of support for the ES behaviour may be due to the level of involvement. The AMS and SU behaviours are required to be performed less frequently than the ES behaviour. Employees regularly use email as part of their job so may actively carry out the behaviour on a daily basis. Due to the repeated occurrences, the behaviour may become more habitual and therefore, not require a conscious deliberation on responsibility.

Psychological ownership was not significantly related to any of the behaviours. The findings suggest that employees' data and technology ownership perceptions do not influence their anti-malware security behaviour. This contradicts Anderson and Agarwal (2010) who found ownership perceptions influenced home users' intentions to perform security behaviours. However, they used a non-specific measure that referred to security behaviour in general. The lack of support in the current study may reflect the specific behaviours under investigation. The affective components of ownership are apparent when others lay claim to objects/target for which an individual has a sense of ownership (Pierce et al., 2003). Ownership perceptions may be more important for other security behaviours such as physical security or where the security threats may put their ownership of data and technology in jeopardy such as theft. As perceived severity also did not influence behaviour, employees may not perceive malware threats to compromise their work devices and, therefore, do need to lay claim to the ownership of their data and work devices.

The current study also found no support for a relationship between organisational citizenship behaviour and security intentions. This does not support the qualitative findings that suggested that employees, who engage in actions that aided the organisation in business continuity and recovery, may have better security behaviour. The lack of support could be due to the measure that was used in the current study. The scale adopted was a well-validated scale and looks at OCB broadly within the organisation, exploring citizenship behaviours that contribute to the optimal functioning of the organisation. A specific measure looking at security citizenship behaviours may have shown a direct relationship. Future research could, therefore, develop and

validate a measure of security citizenship behaviour to allow a more detailed exploration of the relationship.

5.5.2 | REVISED MODELS

The study found that using an extended-PMT model could explain 40% of the variance in employees' intentions to scan USB sticks for malware, 29% of the variance in employees' intentions to install software updates and 47% of the variance in employees' email security behaviour. The variance explained for the AMS behaviour and ES behaviour is line with other research using PMT, Chenoweth et al. (2009) explained 43% of the variance in consumers intentions to use anti-spyware software, whereas Liang and Xue (2010a) explained 56% of users' intentions to use anti-spyware software. Lee et al. (2008) using PMT in combination with other theories explained 45% of the variance in a composite measure of anti-virus behaviours. Ng et al. (2009) used the HBM and explained 61% of the variance in being cautious with email attachments. The current study is line with those using PMT to explain users' behaviour; however it does mean 50-60% of the variance for these two behaviours is explained by factors not considered in the study.

The variance explained for the software update behaviour is relatively small, however, there is a lack of research exploring this type of security behaviour to make appropriate comparisons. This behaviour is different from the others in that it can be automated for employees and this may be influenced more readily by factors such as the Health Belief Model's "cues to action" which prompt users to behave in desirable ways such as a prompt on their machine to install software updates. Individuals who know when to conduct the secure behaviour (i.e. when prompted by the machine) may be more likely to engage in it whereas others may disregard it and postpone the update. Further research is required to understand what may also influence software update behaviour.

This study is one of the first to explore specific security behaviours in an organisational context using this approach and explained adequate variance for two of three behaviours using an extended-PMT model. PMT is consistently used within security. However, the findings from the current study suggest that in isolation it may not be the most appropriate model for understanding the diversity of specific security behaviour as not all of its components are adequate to explain security behaviour. Expanding PMT from the findings of the qualitative work allowed further variance to be explained within the behaviours. However a portion of the variance is still explained by factors that were not investigated in the study. Further research is needed to explore additional factors to understand fully what influences security behaviour within the workplace.

5.5.3 | LIMITATIONS

Attempts were made to reduce common method bias, however as security behaviours can be considered to be a form of job performance, social desirability bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) may have inflated participants intentions to engage in the behaviours. Furthermore, the study relied on self-report measures and actual performance measures would have been more beneficial. Future research would benefit from utilizing multi-method approaches to measuring security performance such as supervisor ratings (Harris & Schaubroeck, 1988) or objective logs from employees computers (Workman et al., 2008).

The survey was piloted with subject-matter experts and a small group of naïve participants. However there may have been some issues with the measurement items. In particular, items that related to the email security behaviour had the use of double negative in its wording. This may have been misinterpreted by participants and potentially negatively skewed the data. Future research would benefit from piloting the self-developed items with a larger sample to pre-empt any potential issues with item wording.

5.5.4 | LEADING TO THE INTERVENTION: INFORMING STUDY 4 (CHAPTER 6)

The current study suggested that employees' intentions to perform the email security behaviour were high, however, a wealth of research shows that employees are still susceptible to phishing emails (McAfee, 2014) suggesting that whilst employees may be motivated, they may not follow through with the required behaviour and that their self-report email behaviour may be inflated. This suggests that there is an intention-behaviour gap with regards to employees' email behaviour as intention accounts for only 1/3 of the variance in actual behaviour (Sheeran, 2002). The next study will seek to bridge this intention-behaviour gap by promoting employees' email security behaviour in regards to malware threat mitigation and using implementation intentions to help translate motivation into behaviour change.

The ES behaviour was influenced by (in order of strongest predictor); self-efficacy, security breach experience at work, susceptibility, response costs and response efficacy. Self-efficacy can be enhanced through enactive mastery, performance accomplishments and vicarious experience. Persuasive information could also be provided on the effectiveness of the behaviour and minimising perceptions of response costs (e.g. effort expended, slowing device down). Experience would be difficult to target. However employees could reflect on situations when they have experienced security issues and the benefits of security behaviours could be re-iterated to reduce the likelihood of the issues.

Susceptibility has a significant negative relationship with the behaviour, it would be inappropriate to manipulate users towards lower levels of malware susceptibility. However as discussed, the negative relationship could be due to lack of awareness between the behaviour

(suspicious links in emails) and malware mitigation or could reflect an unrealistic optimism bias (Weinstein, 1980). Providing information or fear appeals surrounding the likelihood and probability of email malware threats may, therefore, enhance awareness of the relationship between email malware and behaviours, motivating users towards malware mitigation in phishing emails and not just focusing on information disclosure as a threat in phishing emails. This would be in line with existing research that has shown that simply reminding users of risk is important for changing secure behaviour regardless of the level of risk presented to them (Davinson & Sillence, 2010) and that low and high threat levels but not moderate levels are important for motivating protective behaviour (Boehmer et al., 2015). Furthermore, meta-analyses on fear-arousing communications have found that it is necessary that people feel vulnerable to the portrayed risk to be effective in changing behaviour (de Hoog, Stroebe, & de Wit, 2007).

To this end, the intervention will be motivation-based to improve the strongest predictors of behaviour to enhance self-efficacy, minimise response costs, build a sense of responsibility, increase susceptibility and maximise response efficacy. Implementation intentions will be used to bridge the intention-behaviour gap between the motivational intervention and actual email security behaviour.

CHAPTER 6: MALWARE-BASED PHISHING IN THE WORKPLACE: AN INTERVENTION TO IMPROVE EMPLOYEE EMAIL SECURITY BEHAVIOURS

6.1 | INTRODUCTION

The previous chapters have explored the motivational processes underpinning security behaviours in general and then focused more specifically on anti-malware behaviours. This chapter presents how this knowledge was then applied to the design of a motivational and volitional intervention that aimed to increase the objective (email legitimacy task) and subjective (self-report engagement in) email security behaviour of employees. The main email behaviour of interest was not clicking on suspicious links in emails, the determinants of which were identified in chapter 5. This behaviour was explored alongside a subset of email security behaviours that are necessary for detection of phishing emails. The motivational component of the intervention was primarily self-efficacy-based but also targeted security breach experience at work, susceptibility, response costs and response efficacy. The volitional component sought to bridge the intention-behaviour gap through implementation intentions by providing participants with "volitional help sheets" in which they identified barriers to goal attainment (checking links are genuine before clicking) and strategies to overcome those barriers in relation to email usage. An RCT design was adopted to evaluate the intervention in which participants were randomly allocated to one of four conditions: A combined motivational and volitional condition, a motivational-only condition, volitional-only condition or a control condition. The change in behaviour was measured alongside an examination of its effectiveness in changing employees' perceptions, i.e. their threat and coping appraisals.

The study found that those exposed to the motivational intervention either alone or in combination with implementation intentions had significantly better task performance compared to the control group immediately post-exposure. The combined intervention had sustained performance compared to control at 1-week follow-up but there was a significant reduction in performance for the motivational-only group. This suggests that the motivational intervention alongside implementation intentions led to sustained performance at 1-week follow-up compared to a control group. Further analyses revealed that these observed differences were for participants' overall accuracy in detecting genuine and phishing emails and approaching significance for participants' genuine precision detection ability but had no effect on phishing precision ability. The study also found no effect of the intervention on self-reported email security behaviour. It also found that there was significant improvement in some components of threat and coping appraisal perceptions regardless of condition. Response efficacy was the only

factor to change significantly as a result of the intervention in which the combined and motivational-only interventions had a significant increase in their perceptions of response efficacy.

This chapter starts by outlining the design of the intervention and then states the hypotheses to be explored in the study.

6.2 | DESIGNING THE INTERVENTION

6.2.1 | THE MOTIVATIONAL COMPONENT

In chapter 5, self-efficacy was the strongest predictor of not clicking on links in suspicious emails, so the motivational component of the intervention is primarily self-efficacy based with additional persuasive information to target the other PMT constructs.

Existing PMT approaches have used fear appeals (Johnston & Warkentin, 2010, 2015) by highlighting the risk of security threats (such as susceptibility to downloading malware and its severity) and information about how to cope with such a security threat (e.g. using anti-malware software, not downloading attachments that are executable files). Other approaches have focussed on highlighting perceived severity within fear appeals (Boss et al., 2015; Jenkins et al., 2013). The findings from Chapter 5 suggested that severity did not influence individuals intentions. However the other PMT constructs (susceptibility, response costs and self-efficacy) alongside security breach experience at work played a role in determining high or low levels of intentions to engage in the email behaviour. In addition to self-efficacy, persuasive information will also target these factors.

There are four information sources important for self-efficacy which can be targeted in interventions: performance accomplishments, vicarious experience, verbal persuasion and physiological states. Maddux and Lewis (1995) claim that a combination of different sources is best for enhancing self-efficacy and a combination of all four is most effective. The current study will focus on two sources (performance experiences and verbal persuasion) as these were deemed most appropriate to target within the motivational component. Previous self-efficacy based interventions for protective online behaviour have been shown to be effective, even when targeting only one source of self-efficacy (enactive mastery) (Wirth et al., 2007).

6.2.1.1 | Performance accomplishments

Self-efficacy is enhanced through the successful enactment of the behaviour by the individual. Performance accomplishments are regarded as the most influential source of self-efficacy because they are personal experiences and, therefore, provide greater authenticity to the individual (Bandura, 1997). This involves the individual learning to master the task, increasing their self-efficacy as they develop their ability to undertake the task. Rapid successes are

beneficial for building self-efficacy, whereas failures reduce self-efficacy. Repeated failures are particularly problematic for self-efficacy when they cannot be linked to adverse external factors (Bandura, 1986) and can lead to states of helplessness (Anderson & Jennings, 1980). On the other hand, linking failures to adverse external factors can enhance self-efficacy (Bandura, Blanchard, & Ritter, 1969). Disappointments in performance at an early stage may reduce self-efficacy. Therefore it is important that the task or behaviour be broken down into small achievable components to build up confidence (van de Laar & van der Bijl, 2001). It is also important to allow people to experience a success and interpret it as their own achievement (Maddux, Brawley, & Boykin, 1995).

In the motivational component, participants are given a practice exercise to train themselves on the main behaviour of interest (detecting suspicious links). Only one training exercise was provided to prevent fatigue and to keep in-line with recommendations to keep the task in achievable components (van de Laar & van der Bijl, 2001). However, participants were also provided with feedback on their performance on the phishing detection task, giving them the opportunity to experience multiple accomplishments (Maddux et al., 1995).

To further enhance levels of self-efficacy, alternative ways to cope with checking URLs were provided. Participants were told that if they were unsure a link was safe, they could use an online link scanner that checked the authenticity of it. They were provided with details of such websites and how to use them.

6.2.1.2 | Verbal persuasion

Gaining positive feedback from professionals or others is an important reward to motivate individuals to carry out and maintain a specific behaviour (Bandura, 1997). People who are persuaded that they have the capability to behave in a certain way are more likely to expend energy and persevere with it. Self-efficacy increased through persuasion leads people to try harder to succeed and can promote the development of skills and a sense of self-efficacy (Bandura, 1986). However, if not done correctly, can also lead to decreases in self-efficacy (Bandura, 1997).

In the motivational component, participants were given feedback and encouragement on their performance on two occasions. Firstly, for the main behaviour of interest (not clicking on links in suspicious emails), they were trained to detect genuine domain names and provided with feedback on their performance on a test in which they identified whether the web address was genuine or fake. The second exercise, during the second phishing test, also provided feedback and encouragement on their performance. Written feedback was provided as it has been shown to be more effective than feedback provided verbally (Ashford, Edmunds, & French, 2010).

An important aspect of effective verbal persuasion is the reliability and credibility of the educator (Bandura, 1997). In particular, individuals give consideration to the perceived reliability, skill, expertise, and ability of the persuasive source (Holloway & Watson, 2002). People trust the educator more when they are seen to have in-depth knowledge and experience of assessing and judging the ability of others (Bandura, 1982). The intervention appeared reliable and credible by telling participants that a computer security company prepared the information and that the training they received was part of a larger "computer hub". The content was kept professional and designed to appear credible, which has been shown to facilitate trust (Sillence, Briggs, Fishwick, & Harris, 2005).

Raising unrealistic beliefs can discredit the persuader and undermine individuals' beliefs in their capabilities (Bandura, 1997). Realistic feedback was therefore designed around their performance on the suspicious link training and the email legitimacy task. Participants were provided with feedback that was framed around their results. For example, for the phishing test participants were presented with how many phishing and genuine emails they correctly identified. Performers achieving above 70% correct were told "WELL DONE. You clearly have the capable skills and knowledge to detect phishing emails", whereas those scoring less than 70% were told "*Good attempt but could do with improvement*" and were provided with a recap of the detection rules from the training. This was to ensure that that the programme was not raising unrealistic beliefs and potentially undermining participants' self-efficacy beliefs.

6.2.2 | DECEPTION INDICATORS

The motivational component used principles from the Theory of Deception (Johnson et al., 1992) to help users detect cues that indicate deception by highlighting message content and the need to inspect emails for emotional triggers that get users to react quickly: greed, urgency, curiosity, and fear. Design heuristics to look out for and spelling and grammar issues were also highlighted to the user. To equip users with the skills to cope with this particular threat, the training dealt with the two main ways users can get malware from emails: downloading and opening attachments or clicking on suspicious URLs. Users were educated about the different file types and how to behave when receiving emails with attachments. More attention was given to training users how to detect fake URLs, as discussed above. Participants were also informed about the dangers of shortened URLs and were provided with information about how to check the authenticity of these.

6.2.3 | THREAT AND COPING MANIPULATIONS

The following additional factors were also targeted by the intervention but were given less attention than self-efficacy.

Perceived susceptibility was manipulated by highlighting the role employees play in information security breaches and the likelihood of receiving malware-based phishing.

Experience was manipulated by getting participants to reflect on times when they may have experienced the negative consequences caused by security breaches. Participants were also persuaded that engaging in security behaviours will reduce the likelihood of these events happening again.

Response efficacy and response costs were also manipulated. Response efficacy outlined the effectiveness and response costs emphasising that the behaviours being outlined only take a small amount of time.

6.2.4 | THE VOLITIONAL COMPONENT: IMPLEMENTATION INTENTIONS HELP SHEET

Two approaches can be used in the formation of implementation intentions; the first is participant-generated in which they are given instructions and develop their own implementation intentions. The second is research-guided in which the research team identify critical situations and strategies based on research and the evidence-base. The first opens a degree of variability as choices will be driven by participants which do mean they may be more salient to the individual. However, existing research has shown that a proportion of participants find this difficult with between 20-40% not forming a single plan (Skår, Sniehotta, Molloy, Prestwich, & Araújo-Soares, 2011, Michie, Dormandy, & Marteau, 2004, Rutter, Steadman, & Quine, 2006). The second approach provides participants with pre-defined critical situations and responses; an approach recommended by Hagger and Luszczynska (2014) in their review of implementation intentions literature. Studies in other domains have adopted this approach (e.g. Bell, Toth, Little, & Smith, 2015; Sheeran, Webb, & Gollwitzer, 2005). However, the critical situations chosen in the implementation intentions need to be appropriate for the target population as there is likely to be between-person variation in exposure and salience of critical situations and the strategies depicted in them. Providing participants with many implementation intentions to choose from is, therefore, a more effective solution and can be implemented with volitional help sheets.

Volitional help sheets require participants to link critical situations with responses by selecting the situations and responses that they feel are most appropriate for them. The critical situations used are evidence-based, guided by existing research on situations that lead to the undesired behaviour. The goal-directed responses are theory-based, using the processes of change (Prochaska et al., 1994) from the trans-theoretical model and aim to help overcome the situations as they reflect strategies that individuals use to try to initiate or sustain behaviour change.

Volitional help sheets have been found to be successful for a variety of behaviours including quitting smoking (Armitage, 2008), increasing physical activity (Armitage & Arden, 2010), reducing binge drinking (Arden & Armitage, 2012) and reducing speeding (Brewster et al., 2015). They are seen to be more effective than a purely user-guided or researcher-guided approach, as they can account for more between-person variation in exposure to critical situations and sensitivity to behaviour change techniques (Brewster et al., 2015).

The design of the volitional help sheet (see Appendix Z) was based on the approach used by Brewster et al. (2015). The 20 critical situations were identified from existing phishing literature and the research team's knowledge and experience. They covered situations in which people are known to or are likely to habitually click on links without checking their legitimacy. They were identified as critical cues that are relevant and salient to the individual. Like the Brewster paper, the 20 goal-directed responses were based on the processes of change from the transtheoretical model (Prochaska & DiClemnte, 1983) and 2 responses were provided for each of the processes of change. Where appropriate these responses were adapted from the existing volitional help sheet literature (Armitage & Arden, 2010, 2012; Armitage, 2008; Brewster et al., 2015).

6.2.5 | CONTROL CONDITION

The control group information consisted of an overview of the history of computers and email use based on information available at http://www.webcitation.org/6dfr7Nboz

6.2.6 | INTERVENTION SUMMARY

To summarise, the intervention is unlike existing approaches on improving phishing protection behaviour because it utilises factors identified from previous work with the population and the target behaviour. The motivational component combines training alongside threat and coping manipulations. The intervention also benefits from the use of implementation intentions to help bridge the gap between increased motivation caused by the motivational component and actual behaviour change. Additional benefits of the intervention include that it is a short programme (15 minutes), low cost and can be easily distributed across companies. Furthermore, it focusses on the context of malware-based phishing threat rather than accidental disclosure of information threat.

The intervention was checked for validity by three other security researchers and piloted with 6 participants who were not security-based. The intervention materials are provided in Appendix Y.

6.3 | HYPOTHESES

The behaviour change approach as outlined in Chapter 2 (section 2.3) and principles of RCTs as outlined in Chapter 2 (section 2.4.5) led to the formation of the following hypotheses:

Hypothesis$_1$: Those who receive the motivational component will have better performance on an email legitimacy task than the control and the implementations intention-only groups, immediately post intervention (T2) and at 1-week follow-up (T3).

Hypothesis$_2$: The combination of a motivational and volitional intervention will lead to the reporting of more email-security behaviours immediately post intervention (T2) and at 1-week follow-up (T3) than the other 3 conditions (PMT-only, implementation intentions-only and control).

Hypothesis$_3$: The effects of the motivational component on the email legitimacy task will be greater for participants with lower baseline security behaviour scores than those with higher baseline security behaviour scores.

Hypothesis$_4$: Those exposed to the motivational component will significantly increase their susceptibility, self-efficacy and response efficacy perceptions and reduce their perceptions of response costs immediately post intervention (T2) and at 1-week follow-up (T3).

6.4 | METHOD

6.4.1 | DESIGN

The study adopted a 2 (implementation intentions: yes/no) x 2 (PMT: yes/no) independent groups design in which participants were randomly allocated to one of the four intervention groups: protection motivation theory and implementation intentions (IMP + PMT), protection motivation theory-only (PMT-only), implementation intentions-only (IMP-only) and control (CTRL). They completed measures at baseline before allocation (T1), immediately post-exposure to intervention (T2) and at 1-week follow-up (T3). The intervention group represented the independent variable. The dependent variables were the score on the email legitimacy tests, self-reported primary email and secondary security behaviours and PMT measures - perceived severity, susceptibility, response efficacy, response costs and self-efficacy.

6.4.2 | PARTICIPANTS

An opportunity sample of 59 participants took part in the study (Age, M= 33.86, SD= 10.08). All recruited participants were currently in full time or part time employment, were not from a computing profession and used an email and computer daily as part of their job role. 21 males and 38 females took part with an average organisational tenure of 5.04 years (SD=5.49) and job tenure of 3.28 years (SD=3.87). 6.8% were from a microenterprise, 3.4% from a small enterprise, 6.8% from a medium-sized enterprise and 83.1% from a large organisation. 39% had read the information security policy of their organisation, 35.6% had never read the policy, 23.7% indicated that they did not know if they had read the policy and 1.7% stated that their organisation did not have a policy. For those that had read the policy, 6.3% read it within the last month, 15.6% 1-6 months ago, 11.9% 6-12 months ago, 15.3% more than 12 months ago and 15.3% were unsure when they last read the policy. Participants were provided with £10 for reimbursement of their time.

6.4.3 | MATERIALS

An online questionnaire hosted on Qualtrics was used to deliver the questionnaires and the intervention content was delivered using Microsoft PowerPoint.

6.4.3.1 | Phishing tests

The email task was designed using phishing emails that were obtained from millerscams.co.uk and myonlinesecurity.co.uk. For each role-play task, participants were presented with 10 fake/spam emails (see Appendix AA for example) and 10 genuine emails (see Appendix BB for example) from the inbox of a fictional Lisa Thompson and were asked to identify which emails were genuine and which were not. Participants were also requested to complete the task as quickly as possible. Each test was balanced with half of both fake and real emails containing half links and half with attachments. To ensure sufficient difficulty and to mimic sophisticated

spam, the number of real and fake emails was varied in which some were addressed to Lisa and had the correct sender email. All emails had correct spelling and grammar to mimic spam representative of that received in organisations in 2015. The content of these emails included invoices, newsletters, password resets, security concerns and generic file sharing emails.

The emails were presented as a static image so participants were not able to interact with the emails. They were asked if they thought the email was genuine and were given a 4 point rating scale from "Definitely, probably, probably not to definitely not' from Blythe, Petrie, and Clark, (2011).

6.4.3.2 | Measures
Unless otherwise stated, all items were measured on a 5 point likert scale that ranged from strongly disagree to strongly agree in which participants indicated the extent to which they agreed with the statement.

6.4.3.2.1 | Protection motivation theory variables
Measures of PMT variables were the same at all three time points and were the items used within Chapter 5. 4 items measured Perceived Susceptibility (see Appendix M) and 13 items measured Perceived Severity (see Appendix M) which was comprised of four sub-constructs based on the previous study: organisational consequences, consequence severity, personal and productivity consequences.

To overcome difficulties of the double negative wording used in the previous version, the wording of the behaviour was changed to allow the measurement of a number of anti-phishing email behaviours. For the response appraisal measures, the behaviour was therefore changed to "Checking an email is genuine before clicking on a link within it". Response efficacy (see Appendix P) was measured with 13 items, Self-efficacy (see Appendix Q) was measured with 4 items and Response costs (see Appendix R) were measured with 4 items.

Self-reported primary email behaviour was measured using a 10 item scale to measure security behaviour in the context of malicious spam over the last 7 days (e.g. In the past 7 days, I check the sender email before clicking on links from within emails), this was taken at T1 and T3. Intention was measured at T2 and was the same items but worded to reflect their motivation to perform the behaviour in the next 7 days (e.g. In the next 7 days, I intend to check the sender email before clicking on links from within emails). See Appendix CC for scale.

Self-reported secondary security behaviour was measured using the same scale used in Chapter 5 comprised of 16 items (see Appendix I). This measure was only taken at T1 and T3.

6.4.3.2.2 | Other measures

Past experience at work was self-developed and consisted of 6 items which measured employees' direct personal experience of the consequences of security breaches and the breaches in the workplace. An example of an item: "My work device has been infected by malicious software (e.g. viruses, Trojans, worms)". Items were measured on a 3-point scale consisting of yes, no and I don't know (see Appendix O). This measure was only taken at T1.

Personality constructs: Impulsivity was measured with 12 items from the Dickman (1990) scale in which 6 items measure functional impulsivity (e.g. *"People have admired me because I can think quickly"*) and 6 items to measure dysfunctional impulsivity (e.g. *"I often say and do things without considering the consequences"*). Participants rated themselves on a 5-point scale of "Very inaccurate" to "Very accurate". This measure was only taken at T1. This measure was used to mask the true aim of the study.

Readiness to change was measured with 5 statements to assess how ready to change their security behaviour employees felt they were. These statements were adopted from Armitage's (2006) measure of readiness of change and aimed to reflect the five stages of change (Prochaska & DiClemnte, 1983): (1) the pre-contemplative stage (I currently do not always check that all emails are genuine before clicking on links within them), (2) the contemplative stage (I currently do not always check that all emails are genuine before clicking on links within them but I am thinking about starting), (3) the preparation stage (I currently check that all emails are genuine before clicking on links within them but not always), (4) the action stage (I currently check that all emails are genuine before clicking on links within them but have only begun to do so recently/in the last 6 months) and (5) the maintenance stage (I currently check that all emails are genuine before clicking on links within them and I have done so for a long time/longer than 6 months). Participants were required to identify which stage they felt most represented their current behaviour.

6.4.3.2.3 | Scale reliabilities

Table 41. Scale reliabilities, means and standard deviations for each time point

Variables	Time	Items	α	M	SD
Threat appraisal					
Perceived susceptibility	T1	3*	.69	2.35	.68
	T2	3*	.69	2.64	.64
	T3	3*	.71	3.71	.70
Perceived severity – total	T1	13	.84	3.46	.59
	T2	13	.92	3.75	.68
	T3	13	.91	3.71	.70
Perceived severity - (organisational consequences)	T1	5	.80	3.50	.67
	T2	5	.93	3.82	.78
	T3	5	.90	3.79	.75
Perceived severity - (consequence severity)	T1	3	.95	3.51	1.00
	T2	3	.96	3.76	.91
	T3	3	.92	3.81	.90
Perceived severity - (personal consequences)	T1	2	.78	2.80	1.00
	T2	2	.81	3.15	1.03
	T3	2	.89	3.09	1.13
Perceived severity - (productivity consequences)	T1	2	.82	3.82	.62
	T2	2	.81	4.00	.64
	T3	2	.76	3.92	.69
Coping appraisal					
Response efficacy	T1	13	.87	3.88	.45
	T2	13	.92	4.11	.52
	T3	13	.93	4.07	.54
Self-efficacy	T1	4	.90	3.86	.89
	T2	4	.81	4.00	.70
	T3	4	.79	3.99	.69
Response costs	T1	4	.93	2.06	.88
	T2	4	.90	2.02	.72
	T3	4	.89	1.97	.69
Other measures					
Intention	T2	10	.90	4.49	.48
Email security behaviour	T1	10	.83	3.52	.79
	T2	-	-	-	-
	T3	10	.85	4.07	.60
Secondary security behaviour	T1	16	.78	3.05	.56
	T2	-	-	-	-
	T3	16	.83	3.22	.61
Functional impulsivity	T1	6	.84	2.93	.86
Dysfunctional impulsivity	T1	6	.83	2.40	.90
Readiness to change	T1	1	n/a	3.98	1.41

*was reduced to 3 items as one item was unreliable due to reverse-wording

6.4.4 | PROCEDURE

Participants were asked to attend a session at the university that would last around 45-50 minutes. Participants were told that they were taking part in a study looking at "personality and email use in the workplace"; this was to mask the true aim of the study. Participant information and consent were delivered via the online program. Following consent, participants were asked to generate their own code using a series of questions to anonymise data. Following this, they were then randomly assigned to one of the four conditions. They then completed the baseline questionnaires and the pre-intervention phishing test. Following this, participants either completed the control task, PMT-only, implementation intentions-only or PMT with the implementation intentions. After these tasks, participants were then presented with the post-exposure phishing test and measures. Completion of the post-manipulation measures marked the end of the session and participants were presented with a final screen that asked them to refrain from discussing the study with colleagues in case they were also taking part. Participants were then sent a link to the follow-up questionnaire seven days after taking part and asked to complete in their own time. At the end of the follow-up, they were fully debriefed about the true nature of the experiment and those who were not exposed to the training, were given the opportunity to read the information.

6.5 | RESULTS

Following data collection, 3 participants data had not been recorded due to a Qualtrics error so were removed from the analysis resulting in a final sample size of 56.

6.5.1 | RANDOMISATION CHECK

To verify that randomization to conditions had been successful, a MANOVA was run with intervention condition as the independent variable and baseline measures of the PMT measures, phishing test score and self-report primary (email behaviours), readiness to change and secondary security behaviours as the dependent variables. The MANOVA revealed that there was no significant differences between conditions at baseline $F(24, 136.92)=1.02$, $p=.442$; Wilk's $\Lambda = .620$, partial $\eta 2 = .15$, indicating that participants had been successfully randomly allocated to conditions.

6.5.2 | MAIN ANALYSIS

6.5.2.1 | Volitional help sheet

Table 42. Critical situations and goal-directed responses from volitional help sheet and percentage of participants choosing each situation and response

Critical situations/goal-directed responses	%
Critical situations ("If I am tempted to click on a link in an email without checking it's genuine…")	
…when the email is from a colleague	15
…when the email is from somebody that I trust	13
…when it's from a well-known company	10
…when a colleague tells me to click on it	8
…when I am interested in what is on the link	6
…when it's not labelled as spam by my email client	6
…when the email address from the sender looks real	6
…when I need to as part of my job	6
…when the email link looks real	5
…when it has been addressed to me personally	5
…when the email is urgent	3
…when I have got lots of emails to get through	3
…when I don't have enough time	3
…when the email message highlights a security issue	3
…when I am busy	2
…when I might suffer negative consequences if I don't click on it	2
…when it would require too much effort	2
…when there is a financial reward for clicking	2
…when it would disturb my work flow	0
…when I have just started the working day	0
Goal-directed responses ("Then I will…")	
…seek out more information (e.g. from colleagues, IT, the internet) about the email (CR)	25
…try to control my impulses to click on links without checking if they are real first (SC)	16
…remind myself that I am not saving much time by not checking if its real (CR)	8
…tell myself that I am capable of checking whether emails are genuine (SL)	8
…remind myself that people in my organisation will be supportive of me checking emails before clicking on links (HR)	7
…make a concerted effort to ignore the urge/pressure to not check emails (CC)	5
…tell myself that I am protecting my organisation from malware by taking extra steps to check if the email is real (RM)	5
…try to avoid putting myself in that situation again in the future (SC)	4
…think about how irritated I will be if my computer is unusable due to malware (DR)	4
…remind myself that I have a commitment to my organisation to protect its data (SL)	3
…seek advice from others (e.g. colleagues, IT, those more experienced in computers) about how to avoid such situations in the future (HR)	3
…remember that when I have not checked whether the email is real, I will become concerned about my computer security (SE)	3
…think about the embarrassment I will suffer if I cause a security breach at work (DR)	3
…remind myself that the government could fine my organisation up to £500, 000 for a security breach (SocLib)	3
…remember that I could spread malware onto my friends and colleagues computers (ER)	2
…remember that not checking email authenticity contradicts the view I have of myself as a responsible person (SE)	1
…rather than viewing checking emails as simply another rule to follow, I will see it as my opportunity to help protect data (CC)	1
…remind myself that I will have a more efficient and secure computer (RM)	1
…remind myself that I could get in trouble by my organisation/management for not checking whether emails are real (SocLib)	1
…think about how if I check whether emails are genuine, it will prevent me from becoming a burden to my organisation/ IT department (ER)	0

Note: Acronyms indicate the processes of change that the responses were designed to tap: **CR**: consciousness raising; **ER**: environmental reevaluation; **DR**: dramatic relief; **SocLib**: social liberation; **SR**: self-reevaluation; **SL**: self-liberation; **HR**: helping relationships; **CC**: counter conditioning; **RM**: reinforcement management; **SC**: stimulus control

Table 42 shows the most commonly selected critical situations and goal-directed responses. From the critical situations, the findings show that employees perceive that they are most likely to click on a link without checking its authenticity when it appears to come from a colleague or someone they trust. Situations such as "not checking when it would disturb work flow" and "when I have just started the working day" were not chosen by any employees. These scenarios reflect potential productivity costs but do not appear to be situations in which employees would be unlikely to check link authenticity. Of the goal-directed responses, strategies relating to consciousness raising and stimulus control are the most commonly chosen by participants. The table shows that while the most appropriate barriers and goal-directed responses are unique to the individual, there appears to be some consensus in those chosen by participants.

The effectiveness of the combined intervention on outcome measures will now be discussed.

6.5.2.2 | Effects of intervention on phishing detection ability on the email legitimacy task

Table 43. Means and standard deviations for phishing detection ability for each condition and time point

	IMP + PMT	PMT-only	IMP-only	CTRL
T1 – Phishing test percentage	74.11 (10.92)	65.42 (14.73)	66.83 (11.52)	73.66 (9.55)
T2 – Phishing test percentage	76.43 (15.50)	77.33 (15.80)	70.77 (13.82)	63.57 (14.47)
T3 – Phishing test percentage	74.29 (11.41)	66.33 (14.07)	63.08 (10.90)	65.00 (10.19)
N= 56	14	15	13	14

To determine the effects of the intervention on post-manipulation phishing detection ability, participants overall percentage for correct detection was taken at time 1, time 2 and time 3. Data was analysed using a mixed 4 (condition; IMP+PMT/PMT-only/IMP-only/CTRL) x 2 (Time; T2/T3) ANCOVA, with the condition as the between-subjects factor and time as the within-subject factor. Baseline phishing ability was the co-variate (to control for differences in pre-intervention ability). The analysis revealed a significant main effect of condition on ability $F(3,51)=3.456$, $p<.05$ with a large effect size, partial $\eta^2 =.169$.

There was no significant main effect of time $F (1, 51) =.906$, $p=.346$, partial $\eta^2 =.017$; and no significant interaction between time and condition, $F (3, 51) =.1.233$, $p=.307$, partial $\eta^2 =.068$, demonstrating that the effect of condition was consistent across post-exposure and 1-week follow-up.

Pairwise comparisons revealed that there was a significant difference between the IMP + PMT condition and control condition (p<.01) and that the difference between the PMT-only condition and control condition was also significant (p<.05). There were, however, no significant differences between the other conditions. Therefore, those receiving IMP+PMT and PMT-only had significantly higher performance compared to the control condition when controlling for baseline performance, following exposure to treatment.

Follow-up ANOVAs were conducted to further explore these differences and revealed that the difference between the IMP + PMT condition and the control condition at T2 was significant (p<.05) and the difference between the PMT-only condition and the control condition at T2 was also significant (p<.05). For T3, the difference between the IMP + PMT condition and control condition was significant (p<.05), and approaching significance for the IMP-only condition (p=.52). However, the difference in performance between the PMT-only condition and the control condition was no longer significant (p=.280). There were no significant differences between the other conditions.

Additional ANOVAs explored a difference in performance between T2 and T3. No significant difference was found for the IMP + PMT condition (p=.622), IMP-only condition (p=.163) and control condition D (p=.710). However, PMT-only condition had a significant reduction (p<.05).
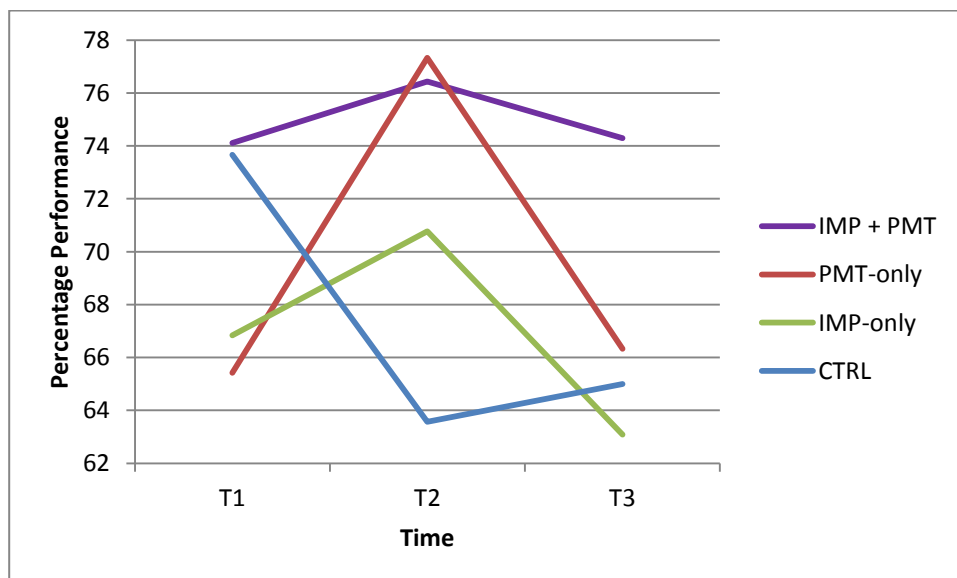
Figure 33. The percentage performance on the email legitimacy for T2 and T3 for each condition

As shown in the Figure 33, post-exposure (T2) and 1-week later (T3) performance in the IMP + PMT condition and control condition remains relatively stable, with the IMP + PMT group performing significantly better than the control condition at both T2 and T3. The findings

indicate that the combined intervention (IMP + PMT) leads to sustained performance compared to training in isolation (PMT-only) which significantly reduces between T2 and T3.

6.5.2.2.1 | Effects of intervention due to baseline differences

As there was was an observed effect of condition on post-exposure and follow-up phishing detection ability, it was important to explore whether the intervention lead to better performance amongst individuals with poorer baseline performance. To explore this, a median split was conducted to categorise participants as either high or low performers (see Table 44).

Table 44. Means and standard deviation for performance scores by time point for baseline groupings

Condition	Baseline grouping	N	Mean performance score at baseline (SD)	Mean performance score at post-manipulation	Mean performance score at 1-week follow-up
IMP + PMT	Low	7	65.18 (6.10)	75.71 (17.18)	71.43 (10.69)
	High	7	83.04 (5.94)	77.14 (14.96)	77.14 (12.20)
PMT-only	Low	9	55.56 (9.60)	78.89 (17.64)	62.22 (16.60)
	High	6	80.21 (4.70)	75.00 (13.78)	72.50 (6.12)
IMP-only	Low	9	61.11 (.814)	70.00 (14.14)	61.67 (10.61)
	High	4	79.69 (5.98)	72.50 (15.00)	66.25 (12.50)
CTRL	Low	6	64.58 (5.10)	58.33 (9.83)	65.83 (9.17)
	High	8	80.47 (5.22)	67.50 (16.69)	64.38 (11.48)

A 2 (baseline group; low vs high baseline performance) x 2 (time; T2 vs T3) x 4 (condition; IMP+PMT/PMT-only/IMP-only/CTRL) mixed design ANCOVA was conducted with baseline performance as a covariate. The analysis revealed a significant main effect of condition on performance, $F(3,47)=3.319$, $p<.05$, partial $\eta^2 =.175$. There was no main effect of baseline performance grouping on performance, $F(1, 47)=1.965$, $p=.168$, partial $\eta^2 =.040$ and no significant interaction between condition and baseline performance grouping, $F(3, 47)=.171$, $p=.915$, partial $\eta^2 =.011$.

There was no significant main effect of time, $F(1, 47)=.008$, $p=.929$, partial $\eta^2 =.000$, no significant interaction between time and condition, $F(1, 47)=1.393$, $p=.257$, partial $\eta^2 =.082$, or between time and baseline grouping, $F(1, 47)=.273$, $p=.604$, partial $\eta^2 =.006$ and no significant interaction between time and condition and baseline grouping, $F(3, 47)=10.521$, $p=.268$, partial $\eta^2 =.080$.

The findings indicated that the effects of condition were not greater for participants who had better or worse performance at baseline.

6.5.2.2.2 | Accuracy and precision of phishing detection

Participants' phishing detection ability was further broken down using principles of signal detection. When receiving a phishing or genuine email, there are a number of possible outcomes that are summarised in the table below from Blythe et al. (2011):

Table 45. Possible outcomes resulting from receiving a phishing or genuine email

		Respondents think the email is:	
		Genuine	**Phish**
But it is actually:	**Genuine**	TRUE NEGATIVE Respondent correctly detects a real email	FALSE POSITIVE Respondent is over cautious and thinks a real email is a phish
	Phish	FALSE NEGATIVE Respondent is taken in and thinks a phish is a real email	TRUE POSITIVE Respondent correctly detects a phishing email

(Blythe et al., 2011) creates two measures from these four outcomes based on detection tasks:

1. Accuracy measures the proportion of correct responses within the total set of responses. This is calculated with the following equation:

   Accuracy= (Number of True Positives + Number of True Negatives)/(Number of True Positives + Number of True Negatives + Number of False Positives + Number of False Negatives)

2. Phishing precision measures the proportion of correct positives within all the positive responses. This is calculated with the following equation:

   Phishing Precision= Number of True Positives/ (Number of True Positives + Number of False Positives)

3. Genuine precision was also created within this study which measures the proportion of correct negatives within all the negatives responses. This is calculated with the following equation:

   Genuine Precision= Number of True Negatives/ (Number of True Negatives + Number of False Negatives)

Table 46. Means and standard deviations for accuracy, phishing precision and genuine precision by condition and time point

	IMP + PMT	PMT-only	IMP-only	CTRL
T1 – Overall accuracy	.74 (.11)	.65 (.15)	.67 (.12)	.74 (.10)
T2 – Overall accuracy	.76 (.15)	.77 (.16)	.71 (.14)	.64 (.14)
T3 – Overall accuracy	.79 (.12)	.71 (.14)	.67 (.13)	.69 (.10)
T1 – Phishing Precision	.68 (.20)	.59 (.21)	.60 (.22)	.71 (.21)
T2 – Phishing Precision	.76 (.27)	.79 (.28)	.76 (.30)	.63 (.33)
T3 – Phishing Precision	.85 (.10)	.74 (.16)	.70 (.16)	.75 (.16)
T1 – Genuine Precision	.82 (.12)	.73 (.21)	.76 (.16)	.78 (.20)
T2 – Genuine Precision	.79 (.18)	.75 (.16)	.70 (.15)	.64 (.19)
T3 – Genuine Precision	.77 (.15)	.74 (.18)	.66 (.12)	.68 (.09)
N=56	14	15	13	14

**Scores closer to 1 indicate better performance

To determine the effects of the intervention on post-manipulation phishing detection, overall accuracy and phishing and genuine precision were taken at the three-time intervals. Data was analysed using a mixed 4 (condition; IMP+PMT/PMT-only/IMP-only/CTRL) x 2 (Time; T2/T3) ANCOVA, with condition as the between-subjects factor and time as the within-subject factor. Baseline phishing detection accuracy and phishing and genuine precision were the co-variate (to control for differences in pre-intervention ability). The analysis revealed a significant main effect of condition on accuracy, $F(3, 50)=3.691$, $p<.05$ with a large effect size, partial $\eta^2 =.181$ and on genuine precision, $F(3, 50)=3.353$, $p<.05$ with a large effect size, partial $\eta^2 =.168$ but no significant main effect of condition on phishing precision, $F(3, 50)=1.343$, $p=.271$, partial $\eta^2 =.075$.

There was no significant main effect of time on accuracy ($F(1, 50)=3.753$, $p=.058$, partial $\eta^2 =.070$), phishing precision ($F(1, 50)=1.152$, $p=.288$, partial $\eta^2 =.023$) or genuine precision ($F(1, 50)=3.549$, $p=.065$, partial $\eta^2 =.066$). There was also no significant interaction between time and condition on accuracy, ($F(3, 50)=1.049$, $p=.379$, partial $\eta^2 =.059$), phishing precision ($F(3, 50)=1.302$, $p=.284$, partial $\eta^2 =.072$) or genuine precision ($F(1, 50)=.541$, $p=.656$, partial $\eta^2 =.031$).

Bonferroni-corrected pairwise comparison on accuracy revealed that there was a significant difference between the IMP+PMT condition and control condition ($p<.01$) and between the PMT-only condition and control condition ($p<.01$). There were no significant differences between the other conditions.

Bonferroni-corrected pairwise comparison on genuine precision revealed that a significant difference between the IMP+PMT condition and control condition ($p<.01$) and between the PMT-only condition and control condition ($p<.05$). There were, however, no significant differences between the other conditions.

For phishing precision, there were no significant differences between conditions.

This re-emphasizes the findings from the earlier analyses and shows that the observed differences were for accuracy, genuine precision detection but no significant changes for phishing precision.

6.5.2.2.3 | Effects of intervention on primary self-report email security behaviour

Table 47. Means and standard deviations for email behaviour for each time point and condition

	IMP + PMT	PMT-only	IMP-only	CTRL
T1 – Baseline email behaviour	3.46 (.93)	3.33 (.90)	3.58 (.57)	3.77 (.61)
T2 – Email intention	4.66 (.39)	4.56 (.39)	4.34 (.66)	4.44 (.41)
T3 – Follow-up email behaviour	4.04 (.63)	4.03 (.64)	4.17 (.45)	4.05 (.72)
N= 56	14	15	13	14

Behavioural measures were taken at T1 (baseline), T2 (intentions, post-exposure) and T3 (1-week follow-up). Repeated measures 4 (condition; IMP+PMT/PMT-only/IMP-only/CTRL) x 3 (Time; T1/T2/T3) ANOVA was conducted to explore the effects of the intervention on self-report email behaviour. Condition was the between-subject factor and time (self-report email behaviour) was the within-subject factor. The ANOVA revealed that there was no significant main effect of condition on self-reported email security behaviours, $F(3,52)=.153$, $p=.927$, $\eta^2 =.009$. There was a significant main effect of time, $F (2, 104)=48.032$, $p<.05$, partial $\eta^2 =.48$ but no significant interaction between time and condition, $F (6,104)=1.359$, $p=.238$, partial $\eta^2 =.073$. Pairwise comparisons revealed that there was a significant increase in self-report email security behaviour between T1 and T2 ($p<.001$) and a significant decrease between T2 and T3 ($p<.001$). Follow-up email behaviour was still significantly higher at T3 compared to T1 ($p<.001$). These results suggest that participating in the intervention regardless of condition significantly increased self-report email behaviour.

6.5.2.2.4 | Effects of intervention on secondary self-report security behaviours

Table 48. Means and standard deviations for secondary security behaviour for time points and conditions

	IMP + PMT	PMT-only	IMP-only	CTRL
T1 – Baseline secondary security behaviour	2.85 (.53)	3.08 (.47)	3.06 (.56)	3.24 (.68)
T3 – Follow-up secondary security behaviour	3.24 (.69)	3.17 (.43)	3.30 (.63)	3.20 (.72)
N= 56	14	15	13	14

A repeated measures 4 (condition; IMP+PMT/PMT-only/IMP-only/CTRL) x 2 (Time; T2/T3) ANOVA was conducted to explore the effects of the intervention on secondary security behaviours not covered within the intervention program. Condition was the between-subject factor and time (self-report security behaviour) was the within-subject factor. The ANOVA revealed that there was no significant main effect of condition on secondary security behaviours, $F(3,53)=.310$, p=.818, $\eta^2 =.017$.

There was a significant main effect of time, $F (1, 53)=4.939$, p<.05, partial $\eta^2 =.085$ but no significant interaction between time and condition, $F (3, 53)=1.476$, p=.232, partial $\eta^2 =.077$. These results suggest that participating in the intervention regardless of condition significantly increased self-report secondary security behaviour.

6.5.2.2.5 | Effects of intervention on PMT constructs

Table 49. Means and standard deviations for PMT constructs for each time point and condition

Measure	IMP + PMT			PMT-only			IMP-only			CTRL		
	T1	T2	T3	T1	T2	T3	T1	T2	T3	T1	T2	T3
Perceived susceptibility	2.12	2.55	2.64	2.33	2.76	2.64	2.59	2.67	2.92	2.48	2.57	2.55
	(.50)	(.66)	(.77)	(.78)	(.66)	(.84)	(.73)	(.76)	(.75)	(.65)	(.61)	(.55)
Response efficacy	3.91	4.09	4.35	3.78	4.35	4.11	3.99	4.02	4.09	3.82	3.96	3.72
	(.40)	(.54)	(.58)	(.55)	(.49)	(.55)	(.50)	(.45)	(.39)	(.36)	(.57)	(.50)
Response costs	1.98	1.75	1.86	2.08	1.80	2.13	2.31	2.35	2.27	1.86	2.27	1.93
	(.92)	(.54)	(.61)	(.990)	(.54)	(.69)	(.92)	(.92)	(.82)	(.61)	(.82)	(.56)
Self-efficacy	3.68	4.13	4.04	3.98	4.18	4.18	3.56	3.83	3.92	4.16	3.95	3.88
	(1.20)	(.73)	(.73)	(.97)	(4.18)	(.61)	(.67)	(.93)	(.74)	(.49)	(.54)	(.68)
Perceived severity:												
Organisational Consequences	3.51	3.94	3.87	3.61	4.09	3.96	3.68	3.82	4.03	3.23	3.41	3.29
	(.66)	(.77)	(.70)	(.70)	(.72)	(.70)	(.44)	(.47)	(.67)	(.81)	(.97)	(.81)
Consequence severity	3.26	3.79	3.98	3.26	3.76	3.84	3.64	3.92	3.82	3.64	3.57	3.60
	(.94)	(.85)	(.80)	(.94)	(.76)	(.87)	(1.06)	(.88)	(.92)	(1.07)	(1.19)	(1.09)
Personal severity	2.64	3.39	3.39	2.70	3.10	2.97	2.85	3.04	3.38	2.79	3.00	2.64
	(.82)	(.96)	(.94)	(1.15)	(1.26)	(1.32)	(.90)	(.83)	(1.12)	(1.01)	(1.09)	(1.10)
Productivity severity	3.93	4.25	3.96	3.83	4.13	4.10	3.69	3.77	4.04	3.75	3.82	3.57
	(.39)	(.55)	(.66)	(.65)	(.58)	(.63)	(.56)	(.44)	(.43)	(.85)	(.87)	(.90)

Repeated measures 4 (condition; IMP+PMT/PMT-only/IMP-only/CTRL) x 3 (Time; T1/T2/T3) ANOVA was conducted to explore the effects of the intervention on PMT constructs. Condition was the between-subject factor and time (PMT constructs) was the within-subject factor.

6.5.2.2.5.1 | Main effect of condition

The ANOVA revealed that there was no significant main effect of condition on response appraisal; self-efficacy ($F(3, 52)=.877$,p=.459, partial $\eta^2 =.048$), response efficacy ($F(3, 52)=.1.294$,p=.286, partial $\eta^2 =.069$) and response costs ($F(3, 52)=1.536$, p=.216, partial $\eta^2 =.081$), and on threat appraisal; perceived susceptibility ($F(3, 52)=.569$, p=.569, partial η^2

=.038) and the sub-constructs of perceived severity; organisational consequences (F(3, 52)=2.513,p=.069, partial η^2 =.127), consequence severity (F(3, 52)=.132,p=.940, partial η^2 =.008), personal consequences (F(3, 52)=.391, p=.760, partial η^2 =.022) and productivity consequences (F(3, 52)=.1.211, p=.315, partial η^2 =.065).

6.5.2.2.5.2 | Main effect of time on PMT constructs

There was no significant main effect of time on; self-efficacy (F(1.737, 100.37)=.1.430, p=.245, partial η^2 =.027), response costs (F(2, 104)=.274,p=.761, partial $\eta2$ =.005) and productivity consequences (F(2, 104)=2.756,p=.068, partial η^2 =.050). There was a significant main effect of time on; organisational consequences (F(1.723, 90.316)=9.210, p<.01, partial η^2 =.150), consequence severity (F(1.695, 89.594)=4.921, p<.05, partial η^2 =.086), personal consequences (F(2, 104)=6.058, p<.01, partial η^2 =.086), response efficacy (F(2, 104)=7.617, p<.01, partial η^2 =.092), susceptibility (F(2, 104)=5.272, p<.01, partial η^2 =.092) and response cost (F(2, 104)=.274, p=.761, partial η^2 =.005).

Bonferroni-corrected pairwise comparisons revealed that there was a significant increase in organisational consequences between T1 and T2 (p<.05) but no significant difference between T2 and T3 (p=1.000). For consequence severity, the increase between T1 and T2 was not significant (p=.089) but the increase between T1 and T3 was significant (p<.05). For personal consequences, there was a significant increase between T1 and T2 (p<.05) but no significant difference between T2 to T3 (p=1.000) and still significantly higher than T1 (p<.01). Response efficacy also significantly increased from T1 to T2 (p<.05), no significant difference between T2 to T3 (p=1.000) but still significantly higher than baseline (p<.01). Following Bonferroni correction, there was no significant difference in time points for response cost.

6.5.2.2.5.3 | Interaction between condition and time

The ANOVA revealed that there was no significant interaction effect between condition and time on response appraisal constructs; self-efficacy (F(5.211, 90.316)=1.130, p=.351, partial η^2 =.061), and response costs (F(6, 104)=.726, p=.629, partial η^2 =.040), and on threat appraisal constructs; perceived susceptibility (F(6, 104)=.785,p=.584, partial η^2 =.043) and the sub-constructs of perceived severity; organisational consequences (F(5.169, 89.594)=1.028,p=.407, partial η^2 =.056), consequence severity (F(5.084, 88.119)=1.227,p=.303, partial $\eta2$ =.066), personal consequences (F(6, 104)=.1.624, p=.148, partial η^2 =.086) and productivity consequences (F(6, 104)=1.671,p=.136, partial η^2 =.088).

6.5.2.2.5.4 | The Interaction between condition and time on response efficacy

The ANOVA revealed that there was a significant interaction effect between condition and time on response efficacy, (F(6, 104)=3.712,p<.01 with a large effect size, partial η^2 =.176).

One-way ANOVAs were conducted to explore this interaction. There was no significant difference between conditions at T1 ($F_{(3, 54)}$=.569, p=.638, partial η^2 =.031) and T2 ($F_{(3, 53)}$=1.724, p=.173, partial η^2 =.089). There was a significant difference between conditions for T3 ($F_{(3, 53)}$=3.509, p=.021, partial η^2 =.166). Pairwise comparisons revealed that there was a significant difference between the IMP+PMT condition and control condition (p<.05).
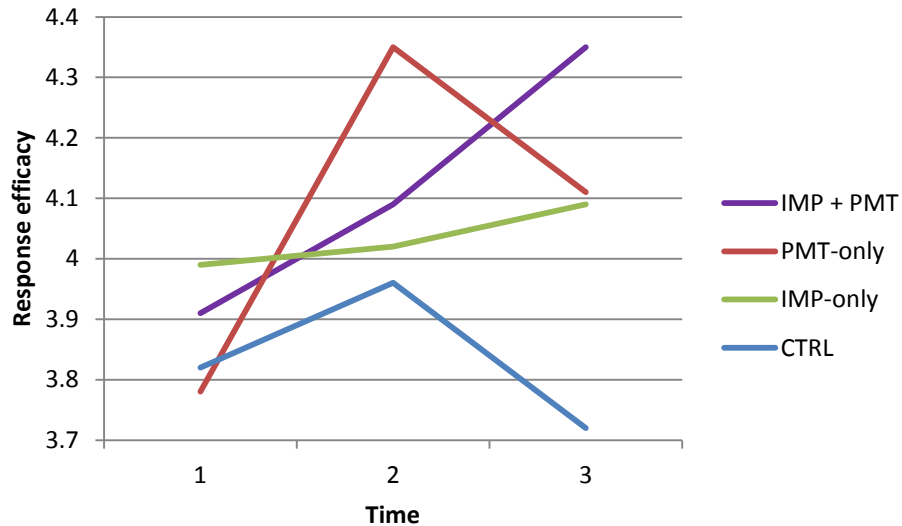
Figure 34. Response efficacy perceptions across the three points for each condition

Additional repeated measures ANOVAs were conducted for each condition. For the IMP+PMT condition, there was a significant main effect of time, $F_{(2, 26)}$=5.250, p<.05, partial η^2 =.288, in which there was no significant increase between T1 and T2 (p=.872) and T2 and T3 (p=.087), however, the increase from T1 to T3 was significant (p<.05). For the PMT-only condition, there was a significant main effect of time, $F_{(2, 28)}$=7.659, p<.01, partial η^2 =.354, in which there was a significant increase from T1 to T2 (p<.01) but no significant decrease from T2 to T3 (p=.433). For the IMP-only condition, there was no significant main effect of time, $F_{(2, 24)}$=.595, p<.01, partial η^2 =.047. For the control condition, there was also no significant main effect of time, $F_{(2,26)}$=2.338, p=.117, partial η^2 =.152.

These results suggest that participating in the intervention regardless of condition significantly increased levels of organisational consequences, consequence severity, personal consequences, response efficacy, susceptibility, and response costs regardless of condition. There was only an observed effect of condition of response efficacy in which those exposed to the PMT intervention (IMP+PMT and PMT-only) had significant increase in their perceptions of response efficacy (although at different time points).

6.6 | DISCUSSION

This study examined the effectiveness of an intervention based on PMT and implementation intentions to increase employees' self-reported email security behaviour and objective phishing detection ability. The study found partial support for hypothesis 1; that those exposed to the motivational intervention (IMP+PMT and PMT-only condition) would have significantly higher performance at T2 and T3. Those exposed to PMT component only, and those exposed to a combined intervention had significantly better performance on the phishing detection task compared to the control after exposure to the intervention. Performance was sustained compared to control at T3 for those exposed to the combined intervention but not for the PMT only group. Further analyses revealed that these observed differences were for participants' overall accuracy and genuine precision detection.

Hypothesis 2 was not supported as those exposed to the combined intervention did not report more intentions to engage in email security behaviours (T2) or self-report engagement in the behaviours at 1-week follow-up (T3). The study found that participation in the intervention, regardless of condition, led to significant improvement in self-reported email security behaviour.

Hypothesis 3 posited that the PMT component would lead to greater improvement in performance for participants who had lower baseline performance scores. The study found no interaction between condition and whether participants had lower or higher baseline performance suggesting that the intervention did not lead to greater improvement for participants with lower baseline performance.

Hypothesis 4 was partially supported, the study found that there was significant improvement in some components of threat and coping appraisal perceptions regardless of condition (perceived severity, organisational consequences and personal consequences). Response efficacy was the only perception to significantly change as a result of the intervention in which the motivational intervention (IMP+PMT and PMT-only condition) had a significant increase in their perceptions of response efficacy.

The current study further broke down participants' performance to detection tasks. For those exposed to the PMT components, there were differences in participants' overall accuracy and in their genuine precision but not for phishing precision. This suggests that the intervention led participants to be more accurate overall in identifying phishing and genuine emails, and more precise in identifying genuine emails by having more correct detections than false negatives (thinking a phish is a real email) for genuine emails. However, there was no improvement in their precision for detecting phishing emails, suggesting that they did not have more correct detections compared to false positives (thinking a real email is a phish). This could be the result

of participants being overcautious and rating genuine emails as phishes leading to lower precision in phishing detection, therefore, no significant changes.

The study partially supports existing studies that have used training approaches to improve end-users phishing ability (Jansson & von Solms, 2011; Kumaraguru et al., 2009) which found improvements in reducing susceptibility to phishing emails. However, these have largely been "real-world" based where participants receive training following insecure behaviour (e.g. they click on a link on a simulated phishing attack by the organisation and are prompted with training); improvements at follow-up are thought to be reflective of the training they receive. An issue with "real-world" studies is that once participants have been told they behaved insecurely and are then given training, they may perceive that they are being monitored by their organisation which in itself has been shown to influence security behaviour (D'Arcy & Greene, 2014) therefore having a post-exposure expectancy effect and possibly inflating these studies findings. The current study demonstrated the benefits of a motivational program with training components in a lab-based setting on an email legitimacy task. Participants' role play activity was the same at all three-time points in which they were told to look for phishing emails therefore not introducing a bias at follow-up. Other studies adopting lab-based approaches and training programs for phishing have not found an effect on subsequent behaviour (Davinson & Sillence, 2010).

The study suggests that the combination of implementation intentions alongside the PMT intervention led to more sustained performance and heightened perceptions of response efficacy at T3 compared to those only receiving the PMT intervention. Those exposed to the PMT intervention in isolation had a significant reduction in their performance from T2 to T3 whereas for those who were exposed to implementation intentions-only, their performance remained stable compared to T2. For response efficacy, those exposed to the PMT component had significant increases in perceptions but at differing time points. The PMT-only group had a significant improvement from baseline at post-exposure whereas the combined intervention had a significant improvement from baseline at one-week follow-up. Similar to objective performance, the group difference at T3 was only between the combined intervention and control group. The motivational component of the intervention improves objective performance and makes individuals believe that the behaviour is effective. Supplementing this with implementation intentions leads to sustainable effects at follow-up on objective performance and response efficacy beliefs.

Research has suggested that, although motivated, people fail to enact behaviour due to poor self-regulation strategies (Abraham et al., 1998). Existing research (Vishwanath, 2015) has argued that phishing detection education may only work in the short-term as they fail to address

users email habits and as such, users fall back into their existing email routines. Implementation intentions help to bolster the effects of motivational interventions by helping people to enact the behaviour (Chatzisarantis et al., 2010; Hagger et al., 2012; Milne et al., 2002; Prestwich et al., 2008). The participants in the current study identified critical situations where they perceived they would be unlikely to behave securely in emails and then identified plans to help them deal with these situations. There were no observed differences in self-report email security behaviour across conditions but the sustained performance and heightened response efficacy of those in the combined intervention may be due to the additive effects of the implementation intentions. People who form plans to help cope with situations are more likely to act in the intended way (Luszczynska & Schwarzer, 2003; Sniehotta, Schwarzer, Scholz, & Schüz, 2005). Critical situations help individuals identify situational cues that lead to poor behaviour, these cues were from situations that may lead employees to engage in habitual email behaviours but they may have also enhanced employees' ability to identify deception indicators in emails and their beliefs in the effectiveness of checking that emails are genuine before clicking on links. So although they may not have led to enhanced self-report security behaviour the implementation intentions may have helped to sustain the effects of the PMT component and one aspect of their coping assessment (response efficacy).

The use of the volitional help sheet also allowed commonly chosen critical situations and goal-directed responses to be explored. The critical situations allowed an understanding of frequently faced barriers to checking email authenticity and the goal-directed responses indicated frequently chosen strategies to help deal with barriers to checking email authenticity. These findings are useful for businesses to understand how best to support their employees in preventing phishing emails as the goal-directed responses help to reduce habitual clicking of links in emails and thus, reducing the likelihood of a security breach occurring from a phishing email.

The PMT intervention aimed to increase levels of self-efficacy and response efficacy and reduce levels of response costs as the previous study found these to influence intentions to engage in email security behaviour. Response efficacy was the only construct that showed a significant change as a result of the motivational interventions, suggesting that the response efficacy manipulation was effective in changing employees' perceptions of the efficacy of email behaviours (being cautious with links and attachments in emails). This is somewhat supportive of studies that have used fear appeals and found changes in response efficacy following exposure (Johnston & Warkentin, 2010, 2015).

A large body of literature focussing on fear appeals manipulations focuses on severity and susceptibility (Boss et al., 2015; Jenkins et al., 2013; Johnston & Warkentin, 2010, 2015). The

lack of manipulation of severity may account for the lack of change in threat appraisal (severity and susceptibility) and coping appraisal (response costs and self-efficacy) as it may have indirectly influenced levels of these constructs. The relationship between severity and security behaviours is unclear as some studies suggest it may have a direct role (Chenoweth et al., 2009; Gurung et al., 2009; Siponen et al., 2014; Vance et al., 2012) whereas others have indicated an indirect role (Herath & Rao, 2009b; Liang & Xue, 2010; Mwagwabi et al., 2014; Ng et al., 2009). An indirect role suggests that it may moderate the effects of other PMT constructs. The current study chose not to focus on severity as it was found not to relate directly or indirectly to intention in Chapter 5 and existing reviews of fear appeals have found that severity is often the most visible component of appeals and the least persuasive (Ruiter, Kessels, Peters, & Kok, 2014).

Furthermore, studies have suggested that threatening information should be used with caution in persuasive communications (Ruiter, Verplanken, Kok, & Werrij, 2003) and that personally-relevant information alone may be sufficient instead of vividly presenting severity information to promote behaviour (Brug & de Vries, 1999). Future research, therefore, needs to fully understand the role of severity and whether it is a necessary component of fear appeals in security.

The PMT intervention was primarily focused on self-efficacy however it did not lead to significant improvements in self-report self-efficacy compared to those who only received goal-setting or control. However, compared to control, the experimental conditions did have marginal increases in their levels of self-efficacy. This goes against existing studies that have designed PMT interventions which have led to increases in self-efficacy (Wirth et al., 2007). However, the lack of change could reflect that participants levels of perceived self-efficacy were high at baseline (combined mean= 3.85), which left little room for improvement. The current study used a 4-item measure of self-efficacy covering the main behaviour of interest. It may have been more beneficial to further break down the target behaviour and cover a range of the email security behaviours within the instrument to understand their self-efficacy in relation to other behaviours and allow more scope for potential change. This would be similar to the 32-item Computer Self-efficacy scale which covers many computer-related knowledge and skills (Murphy, Coover, & Owen, 1989). This would allow greater exploration of self-efficacy in relation to a range of email security behaviours and allow more scope for change.

6.6.1 | LIMITATIONS

The study found that participation in the intervention, regardless of condition, led to significant improvement in self-report email security behaviour. The lack of difference between conditions could reflect that those within the control group were exposed to phishing information in the

form of the email legitimacy task. While they were not given any feedback on their performance or exposed to any persuasive manipulations, simply participating and looking for deception indicators may have prompted awareness and motivated users to engage in more email security behaviours. To overcome this, an additional control group should have been included, who are not exposed to the email legitimacy task, to explore whether engagement in these tasks also promotes greater awareness and to help isolate the potential effects of the intervention.

The main limitation of the current study was the lack of effective standardisation of the phishing tests, although efforts were made to control for such effects during data analyses, a much more effective approach would be to randomise the test items across participants and conditions in which the task difficulty would be balanced out.

6.6.2 | FUTURE RESEARCH

Experience was another factor that influenced the behaviour within the survey. The current study required participants to reflect on security experiences they may have encountered, however a more effective approach may have been to simulate a security breach to participants such as a desktop simulation of what could happen if they get malware onto their computer and shown how to recover, this would also enhance self-efficacy as past experiences is one of its sources.

The training aspects of the programme could be improved by being more interactive. Research has shown games to be effective for improving participants' phishing detection ability (Arachchilage, Love, & Scott, 2012; Sheng & Magnien, 2007). Interactivity could also be added to the motivational components as interactive PMT interventions have been shown to enhance their effectiveness (Vance et al., 2013).

The present study acted as a pre-cursor to dissemination within an organisation and demonstrated some promising findings, however it was lab-based and further work is required to improve the potential behaviour change implications of the programme. Future research could evaluate it within the employment setting, where it could be disseminated across a larger sample and explore its effects over a longer period of time.

CHAPTER 7: OVERALL DISCUSSION

This discussion considers the findings from the four research studies reported in this thesis and highlights contributions to the understanding and promotion of security behaviour in the workplace. The work is summarised in relation to the original research questions and objectives. The discussion will reflect on the literature discussed in Chapter 2 and consider how the work documented in this thesis has added to the knowledge of security behaviour and security behaviour change interventions. The implications of these findings will be discussed both in terms of the intervention and in the wider context of organisational behavioural security. Limitations of this research will also be presented. Furthermore, recommendations for research, as well as practice, will be suggested, and finally, considerations for future research will be explored.

7.1 | RESEARCH QUESTIONS

Two research questions were devised based on existing behavioural information security research with the aim to develop and evaluate an intervention to improve the security behaviour of employees. These questions were explored using a mixed-method approach across four organisational studies:

1. What influences and prevents different security behaviours in the workplace?
2. Does a theoretically-grounded intervention using motivational and volitional approaches lead to and sustain security behaviour change?

7.2 | RESEARCH OBJECTIVES

The specific objectives of thesis were to:

- examine internal and environmental factors that motivate the different behaviours contributing to information security compliance (Study 1 & Study 3, Chapter 3 & 5);
- identify barriers to security behaviours and consider them within the organisational context (Study 1, Chapter 3);
- develop a qualitatively-driven framework to explain how factors influence information security behaviours (Study 1, Chapter 3);
- understand how employees appraise the sensitivity of work information by developing and validating a scale to measure this (Study 2, Chapter 4);

- explore an extended PMT-model (driven by the qualitative work and existing literature) to identify factors that influence three specific anti-malware behaviours (Study 3, Chapter 5);
- use the findings from the extended model to inform the motivational component of a behaviour change intervention (Study 3 & 4, Chapter 5 & 6);
- assess the feasibility of an intervention that combines motivational and volitional components to promote anti-malware behaviour (Study 3 & 4, Chapter 5 & 6).

7.3 | WHAT INFLUENCES AND PREVENTS DIFFERENT SECURITY BEHAVIOUR IN THE WORKPLACE?

The first research question aimed to understand what motivates and prevents security behaviours in the workplace by understanding the psychological principles behind employees' motivations to undertake protective security actions. An over-reliance on an IS policy compliance paradigm has led to a limited understanding of what motivates individual security behaviours. This question aimed to identify key determinants of security behaviours using a mixed-methods approach accumulating in evidence to design the final intervention.

7.3.1 | STUDY 1 (CHAPTER 3)

Chapter 3 utilised framework analysis to analyse interviews with employees from two organisations to develop a qualitatively-driven framework to explain information security behaviours. The interviews explored factors from PMT and the TPB on behaviours that contribute to IS policy compliance. The analysis allowed an exploration of components from these models but also for new themes to emerge that were not accounted for from these a priori models. The analysis indicated that there were seven themes pertinent to how information security behaviours are influenced: Response Evaluation (response costs, perceived benefits and response efficacy), Threat Evaluation (threat models, severity, information sensitivity appraisal, and susceptibility), Knowledge (of security risks and protective actions), Experience (of security breaches and work experience), Security Responsibility, and Personal and Work Boundaries. The findings suggest that these differ by security behaviour and by the nature of the behaviour (i.e. on- and offline). An additional theme of security behaviour suggested three forms of security hygiene informed by protective behaviours and security citizenship. Levels of psychological ownership and organisational citizenship behaviour did not differ between organisations. Some of the findings were consistent with previous research, such as security responsibility, which had been previously suggested by Dourish et al. (2004) who found that individuals delegate responsibility onto one of four sources: technology, individuals, organisations and institutions.

The findings led to the development of a thematic framework of security behaviour; the framework consisted mainly of internal factors suggesting that environmental factors may play less of a role in driving employees' security behaviour. TPB (attitude and social pressures) components were not found to play a role in security behaviours so were not incorporated in the final framework. This framework was modified to an extended-PMT model based on findings from the qualitative study and the literature review, and explored in more depth in Chapter 5.

The findings provided greater clarity to existing literature as an important finding of this study was that these influencing factors played differing roles for security behaviours. PMT was an adequate theory to study security behaviour but its components (threat and coping) may have differing influence depending on the security behaviour and security threat of interest. In threat evaluation, susceptibility perceptions were found to differ, with online security threats perceived as more likely than offline threats. Severity perceptions were found to divide into four groups of consequences: technology, personal, organisational, and third parties. Within response evaluation, response costs findings was supportive of existing research discussing the impact of costly security in the workplace (Beautement et al., 2009). The study suggested that employees consider cognitive, monetary and productivity costs but do not view all security behaviours to be equally costly. For example, they considered passwords to have high costs but locking the computer to have minimal costs. Response efficacy perceptions were found to be limited and a potential barrier to security behaviour since employees do not receive feedback or information regarding their security actions and the effectiveness of these efforts.

A key finding was personal and work boundaries and its role in risky behaviour. Moreover, the role of previous job experience and security breach experiences was found to impact on current employees' security behaviour. Another important finding was the support of the role of information sensitivity appraisal in line with existing research (Adams & Sasse, 1999). However there is lack of quantitative studies exploring its link to security behaviour and tools to measure it. This highlighted the need to explore its role quantitatively and design a scale to measure this.

The study emphasised the limitations of using a compliance approach to understand security behaviour as the findings indicated that factors may play differing roles, a finding that was also confirmed in chapter 5 for anti-malware behaviours.

7.3.2 | STUDY 2 (CHAPTER 4)
Study 2 validated a new measure of information sensitivity in the workplace, confirming its relationship to security behaviour and assessed differences in sensitivity appraisal of different information types that employees may be exposed to in the workplace. The content, discriminant and criterion-related validity and reliability were assessed. A key contribution was

that the scale was found to comprise of five subscales; Privacy, Worth, Consequences, Low proximity interest by others and High proximity interest by others. The WISA scale, alongside its five subscales was found to have strong factorial validity that was confirmed across 8 target information types. The scale was found to have strong content validity and good criterion-related validity as it was found to significantly predict security behaviour. Finally, the scale was found to have adequate discriminant validity as 3 of the 5 aspects of the WISA scale were found to be unrelated to organisational citizenship behaviour. Of the information types, financial information was found to have the highest ratings for sensitivity followed by health and HR. They were also found to be the highest for 3 of the 5 sensitivity subscales, in particular, privacy, worth and consequences. Information about individuals (e.g. personal, health and lifestyle) was considered to be significantly of interest to employees' high proximity interest groups (i.e. family and friends) in comparison to organisational-focussed information. For low proximity interest, the opposite effect was apparent with organisational-focussed information (e.g. IP, day to day, commercial) perceived to be of interest to low proximity groups (i.e. criminals, fellow employees & business competitors). Finally, the findings indicated that the more an individual works with an information type did not mean they rated the information any more sensitive than employees who did not work with the information.

The study contributed a new scale to measure information sensitivity to be used in a workplace setting with components to understand what constitutes information sensitivity. The study also showed that sensitivity appraisal was able to predict a range of security behaviours including passwords, secure Wi-Fi usage, physical security and avoiding security risks. This demonstrates the potential role of information sensitivity appraisal as a determinant of protective actions in the workplace.

The study also shed further light on how employees evaluate the sensitivity of workplace information. The qualitative study and the study by Adams and Sasse (1999) indicated that employees consider information about individuals as more sensitive than commercially sensitive company information. Moreover, study 3 was in line with this as health, financial and HR information were considered most sensitive but the study suggested that employees do consider some forms of organisational information to be sensitive, particularly those pertaining to intellectual property. However, their appraisal process for the sensitivity evaluation for this form of information differs compared to that relating to living individuals. Overall, the study contributes five components to understanding how employees appraise the sensitivity of information.

7.3.3 | STUDY 3 (CHAPTER 5)

Study 3 confirmed that security behaviours are influenced by different factors by assessing an extended-PMT model based on findings from existing research and the qualitative study. Three anti-malware behaviours were explored: scanning USB sticks with anti-malware software (AMS security), installing software updates (SU security), and not clicking on suspicious links in emails (ES Security). The threat appraisal (severity and susceptibility) and coping appraisal (response costs, self-efficacy and response efficacy) of the original PMT model were explored. The model was extended to further include psychological ownership, security breach experience, organisational citizenship behaviour, responsibility and WISA.

Revising PMT using regression analyses allowed additional factors to be added to the model to provide greater insight into the influencers of anti-malware behaviours and to identify which factors can explain more variance in the target behaviour. For AMS security it was found that self-efficacy, response efficacy, response costs, WISA (consequences) and responsibility significantly predicted motivations to scan USB sticks for malware. For SU security it was found that, response efficacy, response costs, susceptibility and responsibility significantly predicted motivations to install software updates when prompted by devices. Finally, for ES security it was found that, self-efficacy, response costs, susceptibility and security breach experience at work were found to significantly predicted motivations to not click on links in suspicious emails. Response efficacy was partially supported for one of the two analyses. All revised models were found to be a good fit to the sampled data for four of the five fit indices using SEM.

Response costs were one of the only factors to relate to all three anti-malware behaviours. Employees who perceive that anti-malware behaviours have low costs (such as productivity, effort and time) are more likely to intend to perform the behaviours, suggesting that (high) costs are a potential barrier to security behaviour. These findings are in line with other research (Beautement et al., 2009; Chenoweth et al., 2009; Liang & Xue, 2010) and the qualitative study that found response costs prevented some security behaviours.

Response efficacy was also shown to relate to all three behaviours. Understanding the effectiveness of security actions is a key influencer of motivation to follow anti-malware security. Response efficacy has been regarded as one of the worst predictors of compliance and IS misuse in the workplace (Sommestad et al., 2014). Response efficacy is important for driving security behaviour; if employees understand the effectiveness of anti-malware behaviours for reducing security threats, they are more likely to undertake security actions. This finding is consistent with the qualitative study that also found that response efficacy was a barrier inhibiting security behaviours. The lack of support for response efficacy in IS policy research is

due to the abstraction issue of requiring employees to evaluate the effectiveness of overall information security efforts, rather than focusing on specific behaviours. When investigating specific behaviours, response efficacy is a key driver such as anti-malware behaviours as studied in this thesis. Study 1 and study 3 showed that low response efficacy is a barrier to security behaviour while study 4 showed that this barrier to security behaviour can be removed through a motivational intervention to increase perceptions of response efficacy. This effect can also be sustained at 1-week follow-up through a combined intervention with implementation intentions. The combined findings from study 1, 3 and 4 demonstrate that response efficacy is a barrier to security behaviour uptake, a key driver of motivation to perform three anti-malware behaviours and can be enhanced through motivational interventions and sustained through implementation intentions. Response efficacy is, therefore, an important factor of security behaviour.

Self-efficacy was shown to be the strongest predictor for two of the behaviours but did not relate to the software update behaviour, suggesting that employees' beliefs in their capabilities are not important for all behaviours. The importance of self-efficacy is well-documented in security research and, study 3 suggested that for some behaviours that require little input from the user (such as responding to dialog boxes to install updates), it plays little role compared to other factors. The qualitative study did not find self-efficacy to be important which was attributed to the difficulties of investigating the construct qualitatively. However, study 3 showed that it plays a significant determining role for some behaviours that require input and skill from the user.

Perceptions of the severity of consequences arising from malware were not found to relate to any of the behaviours. This does not support a wealth of research that suggests it has a key role in security behaviour. This finding was also consistent across its four components that were explored in relation to the behaviours that were driven from the qualitative study. Susceptibility, on the other hand, had a complicated role. It was a significant predictor of software update intention and the cookie acceptance task, but a significant negative predictor for the email security behaviour. The findings suggest that threat evaluation may not play as important a role as coping evaluation for security behaviours specifically - anti-malware behaviour.

Study 1 suggested that employees appraise the sensitivity of the information they work with and use this judgement to assess whether it needs protection. In study 2, this was further explored by developing the WISA scale, which has been shown predict a range of security behaviours. Study 3 further explored its role for anti-malware behaviours and found that one component predicted the AMS behaviour (WISA – consequences). This suggests that the information

sensitivity appraisal may be more important for some security behaviours (e.g. access control) than other protective behaviours (e.g. anti-malware).

Responsibility, a theme that emerged from the qualitative study, was found to be important for anti-malware. Individuals with higher perceptions of personal responsibility for security had greater motivation to undertake anti-malware actions (AMS and SU). A sense of personal responsibility supports the qualitative study and existing research exploring personal responsibility in consumers (Boehmer et al., 2015; LaRose, Rifon, & Enbody, 2008). The thesis thus showed the importance of a sense of personal responsibility for security behaviour in the workplace setting.

Psychological ownership and OCB were investigated as two potentially important factors that may influence security behaviour but had received little attention in previous literature. Study 1 explored potential differences in the factors between the two recruited companies and found no significant differences in levels between employees. Study 3 sought to explore their direct influence on anti-malware behaviours and found they did not significantly predict any of these.

Taken together, the three studies address the research question by identifying a number of factors that influence and prevent a range of security behaviours to develop an extended-PMT framework. A specific factor was then explored in-depth (information sensitivity) and the extended model was investigated with a specific subset of behaviours (i.e. anti-malware), to identify their key determinants.

7.4 | DOES A THEORETICALLY-GROUNDED INTERVENTION USING MOTIVATIONAL AND VOLITIONAL APPROACHES LEAD TO AND SUSTAIN SECURITY BEHAVIOUR CHANGE?

The second research question aimed to evaluate the effectiveness of an intervention to improve anti-malware behaviour. A lack of theory-based interventions with experimental validation has led to a limited understanding of how to promote and sustain behaviour change for security in the workplace. Study 4 sought to design, deliver and evaluate an intervention with motivational and volitional components.

7.4.1 | STUDY 4 (CHAPTER 6)

This study tested the intervention to increase the email security behaviour of employees in relation to malware mitigation. The motivational component of the intervention was driven by the findings of study 3 and the volitional component aimed to translate motivation into actual behaviour change through the use of implementation intentions. The motivational component primarily focussed on improving self-efficacy but also utilised security breach experience at work, susceptibility, response costs and response efficacy. The study looked at the effects of the

intervention on improving performance on an email legitimacy task, self-reported email and secondary security behaviour and enhancing levels of threat and response evaluation.

The study found that those exposed to the motivational intervention either alone or in combination with implementation intentions had significantly better task performance compared to the control group post-exposure. The combined intervention had sustained performance compared to control at 1-week follow-up but there was a significant reduction in performance for the motivational-only group. This suggests that the motivational intervention alongside the goal setting lead to sustained performance at 1-week follow-up compared to a control group. Further analyses revealed that these observed differences were for participants' overall accuracy in detecting genuine and phishing emails and approaching significance for participants' genuine precision detection ability but no effect on phishing precision ability. The study found no effect of the intervention on self-reported email security behaviour. The study found that there was significant improvement in some components of threat and coping appraisal perceptions regardless of condition. Response efficacy was the only factor to significantly change as a result of the intervention in which the combined and motivational-only group had a significant increase in their perceptions of response efficacy.

Furthermore, there was no self-reported change in any other threat or coping appraisal constructs. Other research using fear appeals has found changes in severity, susceptibility, self-efficacy and response efficacy (Johnston & Warkentin, 2010, 2015). However, these studies were exploring different behaviours (e.g. data backups and password theft), which may suggest that motivational behaviour change approaches may be more appropriate for some behaviours than others.

The study supports existing research using self-efficacy based principles to enhance security behaviour (Shillair et al., 2015; Waddell et al., 2014), and anti-phishing training (Kumaraguru et al., 2009; Sheng & Magnien, 2007). However, this is the first study to demonstrate the effects of supplementing motivational interventions with volitional strategies to promote security behaviour and found they helped sustain behaviour change at 1-week follow-up. This effect is supportive of other research in non-security domains that has bridged the intention-behaviour gap with implementation intentions (Chatzisarantis et al., 2010; Hagger et al., 2012; Milne et al., 2002; Prestwich et al., 2008).

However, the study found an increase in self-reported email behaviour and secondary security behaviours across time points independent of condition. The intervention was only successful in changing objective performance due to the limitations of self-report measures. The lack of a specific effect on self-reported behaviour is supportive of other phishing training studies that have found that intervention exposure, regardless of condition manipulation, leads to greater

intentions and self-report (Davinson & Sillence, 2010). This is line with the self-prophecy effect in which, simply asking individuals whether they intend to act in a desirable way is enough to increase the likelihood that they will (Sprott, Spangenberg, & Fisher, 2003). This highlights the importance of combining objective and subjective reports of behaviour.

Overall, the study demonstrates promising findings for combining motivational and volitional approaches to changing security behaviour. However, the study did not find a change in self-reported email security behaviour, enhancing threat and coping appraisal (except response efficacy) or additional effects on secondary security behaviour. There were only changes in performance on an email legitimacy task; the objective behavioural measure. Objective performance measures are considered a more reliable source of actual behavioural measures than self-report measures (Bommer, Johnson, Rich, Podsakoff, & MacKenzie, 1995) as they are not subject to social desirability bias.

In relation to the second research question, the study demonstrated the benefits of grounding the intervention design in findings from the target population and based on behaviour change best practice. The study also benefitted from adopting a RCT design to evaluate the effectiveness of the intervention, highlighting the benefits of using best practice to inform the design, delivery and evaluation of behavioural information security efforts. The study is also one of the first to focus on email security behaviour change to prevent malware; most existing approaches largely focus on detecting phishing emails to preventing accidental information disclosure.

7.5 | THESIS IMPLICATIONS

This thesis has designed and tested a motivational and volitional intervention based on the findings from studies with the target population. This resulted in an intervention that is short, low-cost and easy to disseminate. The implications of this thesis are far reaching and discussed in respect to research and practice.

7.5.1 | RESEARCH

As outlined in Chapter 2, existing research has largely conceptualised and addressed security behaviour in the workplace as "compliance with the IS policy". This thesis has shown that specific security behaviours are motivated by different factors and that behaviours need to be studied separately. The findings of the qualitative study resulted in an extended PMT-model that can be used to study security behaviour. Here, the extended model was examined for anti-malware behaviours in which it was shown that factors played differing roles. The results from Chapter 5 have led to revised models that can be used to promote the specific anti-malware behaviours. Research would benefit from focussing on specific security behaviours in an employment sample rather than using a compliance paradigm; this would provide the greatest benefit to the behavioural information security domain. This is only the start as the influencers

219

of each behaviour need to be explored independently and their relationships to behaviours understood prior to intervention - a process illustrated in this thesis.

The thesis showed the benefit of a theory-based intervention evaluated with experimental methodologies. The approach outlined in this thesis, based on best practice from behaviour change literature, would provide a useful basis for other longitudinal projects exploring behaviour change for security.

Threat evaluation is comprised of severity and susceptibility perceptions. The thesis provided greater insight into threat evaluation and found a complicated role. Chapter 3 showed that susceptibility perceptions are different depending on whether there was an online or offline threat. This is important to acknowledge when exploring online and offline security behaviours as information security practice in the workplace relies on both types of behaviours. As indicated by the qualitative data, employees perceive offline threats to be less likely and more opportunistic so it is important to acknowledge this distinction. Susceptibility was found to drive three behaviours (the software update behaviour, email security behaviour and cookie acceptance task) rather than severity of consequences. The qualitative study suggested that severity perceptions fall into different domains, and this factorial structure of severity was validated and further explored in Chapter 5. It found that employees consider organisational, personal, productivity and general consequence severity. None of these components were found to relate to anti-malware behaviours, suggesting that fear of the consequences of malware threats plays little role in driving behaviours but rather it is the perceived likelihood of getting malware that is more important. However, research may benefit from further exploring severity components with other security threats and behaviours.

The thesis showed the benefits of a motivational and volitional intervention. Implementation intentions and goal setting for bridging the intention-behaviour gap has been relatively understudied in security. The findings provide promising results for their utility in driving security behaviour so more focus is needed on volitional behaviour change.

The thesis also added to the growing body of research that extends or combines existing behavioural models in security (e.g. Herath & Rao, 2009a, 2009b; Ifinedo, 2011). The current study highlights the need for behavioural models that are specific to security. PMT was found to be useful in guiding the qualitative study and its findings. However, the threat appraisal component was found to have differing effects on security behaviour. In particular, severity was found not to relate to anti-malware behaviour and susceptibility was found to have significant relationships but with opposing effects. This highlights the need to validate behavioural models and modify them according to the behaviour and population under investigation.

7.5.2 | PRACTICE

The thesis showed response efficacy plays an important role in security behaviour and is a potential barrier to behaviour but can be improved through motivational interventions. These combined finding suggests a number of implications for information security practice.

More work is needed on improving the feedback link between behaviour and result. The thesis achieved this by emphasising the effectiveness of an anti-malware behaviour and providing participants with feedback on their performance. However, some practical implications could improve this feedback link. Feedback and/or positive reinforcement needs to be provided to users on their security behaviour. Systems sometimes provide information on their employees' reactive behaviour (e.g. weak password or non-updated system) but more attention needs to be given to providing feedback on their proactive security. In doing so, employees' perceptions of response efficacy may increase. Furthermore, management in organisations need to provide employees with feedback on their information security efforts; this could be tied in with employees' performance appraisal process or a regular report on their security behaviour. Presently, information security behaviours are given little attention in employees' job performance.

Perceived responsibility is also important for driving behaviour; organisations could focus on empowering responsibility in employees. Research has shown the benefits of enhancing responsibility perceptions in end-users (Boehmer et al., 2015; Shillair et al., 2015). Communicating to employees their personal responsibility and shared responsibilities for security actions may, therefore, help to enhance security behaviour.

The findings of the thesis indicated that for anti-malware behaviours, a focus on coping appraisal may be more appropriate rather than threat appraisal. Coping appraisal components were more consistently related to the behaviours. Efforts may, therefore, benefit from focussing more on equipping users with a sense of ability (self-efficacy), understanding of effectiveness (response efficacy) and reducing the perceived costs associated with security (response costs). Presently, attention is often given to fear appeals or scare tactics by highlighting all the losses associated with a risk, but the findings of the thesis suggest that for anti-malware behaviours, a focus on coping appraisal may be more appropriate.

It is important to consider the costly nature of security. While the qualitative study suggested that not all behaviours are perceived to be costly by employees, the survey indicated that high response costs will inhibit anti-malware behaviours. Attempts should be made to understand costs (such as effort and productivity) associated with specific security behaviours and, where possible, diminishing the cost for the employees through better system design, more usable policies or communicating the benefits vs. the costs towards the employee.

7.5.3 | PROCEDURE FOR INFORMATION SECURITY INTERVENTIONS IN THE WORKPLACE

Organisations need to move away from considering IS policy compliance as the basis of their employees' behaviour. Instead, organisations should consider the important subset of behaviours in their policy, and target these appropriately in intervention efforts by considering what motivates and prevents them. The multi-stage process adopted in this thesis can also be used in organisational IS practice. Below is a recommended process for identifying specific security behaviours, modifying interventions and evaluating their utility in the workplace. This process should be followed by intervention designers to further develop interventions in the workplace.
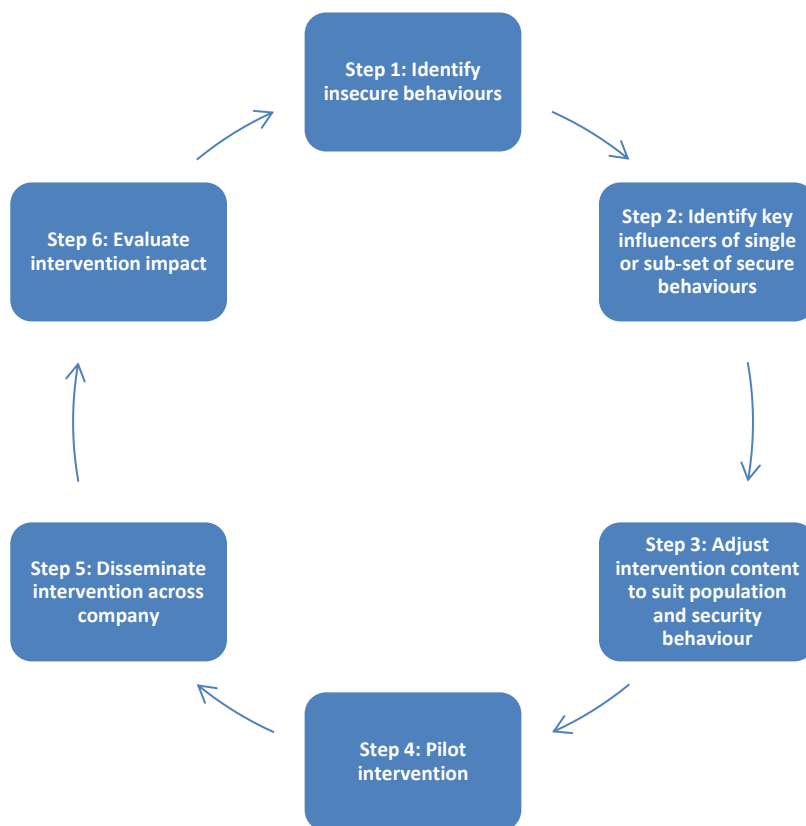
Figure 35. Process chart for security behaviour interventions in the workplace

Baseline measures

First, create user profiles for baseline security behaviour for all staff from objective and self-report measures where possible. This is to be used for identifying users requiring security intervention and to evaluate intervention success.

Step 1: Identify insecure behaviours

Prior to intervention, it is necessary to identify specific problematic behaviours within the organisation and measure this appropriately. Where possible these should be identified using objective data from systems such password logs. However, organisations could also gather data from their organisations using surveys or interviews to identify poorly performed security behaviours.

Step 2: Identify key influencers of secure behaviours

On identifying the specific security behaviours of interest, the extended-PMT model can be used to identify the key influencers of the behaviour. This can be achieved by surveying a portion of the workplace and matching participant data with objective or self-reports of their security behaviour.

Step 3: Adjust intervention content to suit population and security behaviour

The key influencers identified from step 2 can be targeted in a motivational intervention, focussing on those that influence the behaviour the most. If the behaviour is habitual and open to volitional control, implementation intentions can be used to help translate intentions into actual behaviour. If the behaviour is not habitual, the motivational intervention can be used in isolation.

Step 4: Pilot intervention

Upon development of the intervention, it then needs to be piloted with employees to assess whether it leads to behaviour change. Conduct a formative evaluation of the intervention with target users through evaluation of the content, objectives and ease of use of the intervention.

Step 5: Disseminate intervention across company

Identify users from profiles who currently do not engage in desired behaviours and randomly allocate to conditions in step 6.

Step 6: Evaluate intervention impact

Conduct a summative evaluation of the intervention by assessing the extent to which behaviour has changed as a result of the intervention. This can be best assessed by adopting principles of RCTs to evaluate the effectiveness of the intervention with an experimental and control conditions. The control condition could be a waiting list of users who will receive the intervention following evaluation. The use of RCT will identify whether a change in behaviour results from the intervention; this is achieved through comparison to baseline behaviour (from

user profiles). Effective evaluation will measure behaviour at multiple time points that include immediately after exposure to the intervention and at a follow-up interval (e.g. 1 month later)

On completion, continually monitor and gain feedback on the intervention to identify lessons learnt for future interventions and then repeat the process for other security behaviours.

7.6 | LIMITATIONS

The thesis has contributed novel and useful findings but some limitations need to be acknowledged. The final intervention acted as a feasibility study however its final sample was relatively small and would benefit from further testing with a larger sample. This should not detract from the significant results in the study with the target population.

Within behavioural information security, there is a lack of validated instruments for a number of constructs investigated in this thesis. Where possible, the self-report measures of the thesis were taken from existing studies or adapted from existing tools in other domains such as health. It should be recognised that these adapted instruments have not undergone validity assessment for security but were assessed for reliability. Validity is important as it legitimises the content of the tools ensuring that what is perceived to be measured is actually being measured. Attempts were made to overcome this limitation by using previously validated instruments from non-security domains but caution should be taken as these may not be entirely appropriate for non-health domains such as security.

The thesis relied on self-report measures of security behaviour in study 3 and study 4. Self-report measures are open to social desirability bias; individuals may report what they think they should be doing rather than their actual behaviour. The intervention may have raised individuals' awareness of what they should be doing, rather than creating an actual change in their behaviour. The lack of significant result for self-report email security behaviour may have resulted from this as there was an increase in all participants regardless of condition. The intervention tried to overcome issues of self-report by including an objective performance task, in which behaviour change was actually observed. Study 3 relied on self-report measures on behaviour as objective measures were not available. Future research would benefit from approaches such as that by Workman et al. (2008) who used computer logs as indicators of actual behaviour. Methods such as these remove limitations of self-report bias and allow more precise measurement of the influence of determinants on behaviour (rather than relying on intention as a proximate indicator).

7.7 | FUTURE RESEARCH

This chapter has touched on some areas for future research, namely, investigating the complicated role of threat perception for different security threats and behaviours and more

focus on the role of volition in behaviour change efforts. However, there are additional directions that future research could take.

Chapter 3 identified factors that may influence security behaviour. However, not all factors were explored in later studies. Namely, personal and work boundaries were identified as a factor that may play a role in risky behaviour. Future research could explore this boundary in more depth with quantitative methods to explore whether weak boundaries are more correlated with risky behaviour.

Chapter 4 developed and validated the WISA scale driven by the findings of Chapter 3, and showed that it predicted a range of security behaviours. Chapter 5 showed that only one component of the scale was important for AMS security behaviours. Informed by Chapter 4, the scale had better predictive value for access control behaviour. Further exploration of the scale in relation to this form of security behaviour is needed as information sensitivity appraisal may be more important for behaviours that are more directly related to information control. Additionally, further validation of the scale is required to enhance its potential utility in the IS domain.

This thesis explored the extended-PMT framework for anti-malware behaviours; future research should explore the model for other security threats and behaviours. There is a lack of research systematically exploring specific security behaviours in an employment sample, so the current thesis provides a promising baseline for further research to examine the model's utility for other security threats.

Further work is also needed to explore factors longitudinally. This thesis demonstrated the benefits of exploring response efficacy qualitatively, then through regression analysis to identify its influence on behaviour, and using experimental manipulations to enhance the factor. More work needs to be done like this for other security behaviours and behavioural determinants.

Finally, the intervention could be further enhanced by incorporating other principles from behaviour change practice such as individually-tailored communications. In particular matching the intervention to an individual's stage of change is effective in helping participants transition through change and lead to more sustainable behaviour change (Velicer, Prochaska, & Redding, 2006). A participant's current stage of change has also been shown to moderate the effectiveness of implementation intentions with greater effectiveness for the preparation stage compared to pre-contemplation and contemplation stages (Armitage & Arden, 2008). Individually tailoring the intervention to the employee may therefore further enhance its effectiveness.

7.8 | FINAL CONCLUSION

This thesis has presented an understanding of what motivates and prevents security behaviour in the workplace. The main aim to develop and evaluate an intervention to improve the security behaviour of employees has been achieved. The influencers of security behaviour in the workplace were identified and then explored more specifically for three anti-malware behaviours. This has identified potential barriers to employees' uptake of protective security actions. Furthermore, a new scale has been developed that allows measurement of employees' information sensitivity appraisal. Implementation intentions have been successfully applied to supplement a motivational approach to improve and sustain performance on an email legitimacy task. In doing so, the thesis has highlighted the benefits of using volitional approaches to enhance security behaviour. Organisations are persistently targeted by security threats putting their employees and information assets at increasing risk; incorporating the findings from this thesis into future research and practice will help enhance the human defence of information security.

APPENDICES

8.1 | APPENDIX A: OCB SCALE

Please use the 7-point scale to indicate how often you engage in the following behaviours in your workplace. Please read each statement carefully, and then select the response from the rating scale.

	Never	Very Rarely	Rarely	Sometimes	Often	Very Often	Always
I attend functions that are not required but that help the organisational image	❍	❍	❍	❍	❍	❍	❍
I keep up with developments in the organisation	❍	❍	❍	❍	❍	❍	❍
I defend the organisation when other employees criticise it	❍	❍	❍	❍	❍	❍	❍
I show pride when representing the organisation in public	❍	❍	❍	❍	❍	❍	❍
I offer ideas to improve the functioning of the organisation	❍	❍	❍	❍	❍	❍	❍
I express loyalty toward the organisation	❍	❍	❍	❍	❍	❍	❍
I take action to protect the organisation from potential problems	❍	❍	❍	❍	❍	❍	❍
I demonstrate concern about the image of the organisation	❍	❍	❍	❍	❍	❍	❍

8.2 | APPENDIX B : PSYCHOLOGICAL OWNERSHIP ITEMS

Please use the 6-point scale to answer the following questions. Please read each statement carefully, and then select the response from the rating scale

	Strongly Disagree	Disagree	Somewhat disagree	Somewhat agree	Agree	Strongly Agree
I feel a high degree of ownership for the device	❍	❍	❍	❍	❍	❍
I feel a high degree of ownership for the data stored on the device	❍	❍	❍	❍	❍	❍
I feel as though the device is MINE	❍	❍	❍	❍	❍	❍
I feel as though the data on the device is MINE	❍	❍	❍	❍	❍	❍

8.3| APPENDIX C : SECURITY BEHAVIOURAL CATEGORIES AND EXAMPLE VIGNETTES

Category	Description	Vignette
Remote working	Actions for working on mobile devices and in external locations	Miles is a merchandiser for a large menswear store and constantly travels to other stores within the local area. One of the benefits of Miles's job is that he is given a company laptop as he is constantly mobile. Miles has a 15 year old daughter, who he lets use his laptop when he doesn't need it as his laptop is of much better quality than his daughter's PC. Mile's daughter uses the laptop for playing computer games, however she often disables the anti-virus software as it slows down her favourite game.
Removable media	Portable storage devices that can be connected to and removed from a computer (e.g. USB sticks)	Mary works as a Lecturer at the local university, she has an important presentation at a national conference in London, 300 miles away from her home. Due to the long train journey and therefore intermittent internet connection, Mary decides to store her work on a USB stick so that she can continue working on the train from her laptop. The documents stored on the device include assignment results, presentation notes and an excel document listing the names and addresses of the students enrolled on one of her classes. After exiting the train and arriving at the conference location, she realizes that she has lost the USB stick.
User access management	How access controls are allocated and managed e.g. passwords	Matthew is staying late to work on an important assignment which is due the next day, Matthew has limited security access to confidential information stored on a company password-protected server but he requires a certain document to finish this report. Normally, Matthew would have to get authorization from the information owner who accesses the file for Matthew but instead the owner gave Matthew their password to access the server so that he could do it himself.
Prevention of malicious software	Actions to prevent malicious software	The updates for the anti-virus on Laura's work computer are controlled by her organization; however she has to occasionally restart her computer to allow the updates to install. Laura is regularly prompted by the anti-virus software to restart the computer however Laura keeps postponing this task as she is too busy to wait for her computer to restart and for her to re-open the documents she was working on.
Breaches of security	Steps for recovering and reporting security incidences	Chris is about to go on a two weeks holiday from work and on his last day his computer starts acting strangely. For example, the cursor on his computer screen would start to move around on its own and new files would appear on his desktop. Chris only realizes that something peculiar is going on later that day, rather than reporting it to IT, he decides to switch off his computer and deal with the issue on his return.
Physical security	Strategies to physically protect infrastructures, information and information resources	Kimberley works as a secretary in a busy open plan office. Kimberley's work computer has access to a number of highly confidential documents. She is normally stationed at her desk however at lunch she leaves to have her break in the staff room. During this time, Kimberley leaves her computer unlocked.
Information control	Responsibility in protection, storage and processing of information	Lee is disposing of old records which contain sensitive information about clients. His office has two bins for disposing of waste: one for confidential waste and the other for general waste. The confidential waste bin is full so Lee puts the old records in the general waste bin.
Software & Systems	Software and system acquisition, installation and maintenance	Anna requires the latest photo editing software for one of her work tasks, the department has no budget to purchase any new software, however Anna knows a website where she can download an unofficial version of the software. Her work computer allows Anna to download and install it.
Acceptable usage	Appropriate usage of information systems, email and the internet	Beth is a call centre employee and during her work breaks she uses her work computer for personal use. She has just booked a holiday to Tenerife which required her to enter her personal information and credit card details.
Continuity planning	Outlines prevention and recovery from internal and external threats	Michelle's work computer is run by Windows Vista, however she prefers to use her own personal laptop which has Windows 8 installed as its operating system. She brings her laptop into work on a daily basis and does all her work tasks on her laptop. However, Michelle does not back up the data that is stored on her personal laptop.
Compliance with legislation	Compliance to legislation acts such as the Data Protection Act (1998)	Sam is a medical doctor and part of this job role requires him to write notes about patients during his sessions which contain sensitive and personal information that is covered under the DPA (1998). Sam often leaves his notes on his desk in his office. Whilst Sam has an office to himself, other staff such as the cleaners can gain access when required.

8.4 | APPENDIX D : FULL INTERVIEW GUIDE AND PROCEDURE

Interview opening:

- Focus of session explained to participant
- Participant provided with an information sheet and informed consent granted from participant
- Emphasize that participants responses will not be shared with their management/company

  Participant to complete demographic questionnaire

For each topic area for the policy categories:

- Provide description of category (e.g. for user access management - Businesses have a number of computer systems to store and process data which employees use. Users have to identify themselves with a user ID and a password to gain access. Employees may have restrictions on their user access to both computer and information)
- Present participant with vignette
- Ask participant to imagine, drawing on his or her own experience, how they would react in that scenario
- Optional questions
    - What advice would you give? / What should they (the character) be doing to protect themselves?

<Researcher to then go back to the topic area>

- Within your workplace, how do you maintain security when/with <topic area>
- Which security behaviours do you perform? / How do you ensure data security?
- What security behaviours do you not perform? / What do you find difficult to do?

For behaviours discussed by participants, the following elicitation questions were used:

Determinant	Example elicitation questions
Self-efficacy	If you want to perform these behaviours, how certain are you that you can?
Experiential Attitude	What do you like/dislike about these behaviours?
Instrumental Attitude	What are the advantages and disadvantages of performing these behaviours?
Social pressures	Who would encourage/ discourage you to perform these behaviours?
Response efficacy	How effective do you think these behaviours are in reducing threats and why?
Response cost	What are the costs in terms of monetary, time and effort in performing these behaviours?
Perceived susceptibility	How vulnerable to a threat are you by not performing these behaviours?
Perceived severity	What are the potential consequences of not performing these behaviours?

Closing questions

- Anything else that you feel you contribute to security that hasn't been discussed?
- What are the top three security behaviours you think are most important?

<Participant provided with debrief sheet and thanked for their participation>

8.5 | APPENDIX E: STUDY 2 – ORGANISATION SECTOR DEMOGRAPHICS
Table 50. Study 2: Organisational sectors from recruited sample

Organisational Sector	Percentage of participants from sector
Accountancy and business services	1%
Advertising, marketing and PR	2%
Armed forces and emergency services	1%
Banking, investment and insurance	0%
Charity and development work	1%
Creative arts	1%
Education	37%
Energy and utilities	1%
Engineering	2%
Government and public administration	3%
Health	12%
Hospitality	7%
Human resources and recruitment	2%
Information technology	5%
Legal services	1%
Manufacturing	1%
Media	2%
Property	0%
Retail	10%
Science	3%
Social care	2%
Sport and leisure	1%
Tourism	0%
Transport and logistics	0%
Telecommunications	1%
Research	1%
Other (Unclassified)	3%

Instructions

The following statements consider what you know about the availability of the information and how it is regulated.

Read each statement carefully and select the appropriate response. If you cannot answer the *question, please select the option 'don't know'.*

<information type>
- Personal information about other people (e.g. address, gender, date of birth, marital status)
- Health information about other people (e.g. physical and mental health history, weight, family medical history)
- Lifestyle information about other people (e.g. shopping habits, hobbies, interests)
- Financial information about other people (e.g. banking details, credit rating, loan history)
- Information about or relating to intellectual property (e.g. trade secrets, creative ideas that could lead to patents, copyrights, new products)
- Day-to-day business operation information (e.g. current customer & supplier details, quotes, purchase history, call records)
- Commercial business information (e.g. strategic plans, financial business data)
- Personnel / HR information (e.g. appraisal, disciplinary info, salary, sickness records)

I think <information type> is:

	Yes	No	I Don't Know
publicly available outside of my organisation	❍	❍	❍
access restricted by my organisation	❍	❍	❍
regulated by law	❍	❍	❍

8.7 | APPENDIX G: FINAL WISA SCALE

> **Instructions**
> The following statements are about different types of information that may be stored by your organisation.
>
> Read each statement carefully and please rate the extent to which you agree with the *statements using a rating scale from 'strongly disagree' to 'strongly agree'."*

<information type>
- Personal information about other people (e.g. address, gender, date of birth, marital status)
- Health information about other people (e.g. physical and mental health history, weight, family medical history)
- Lifestyle information about other people (e.g. shopping habits, hobbies, interests)
- Financial information about other people (e.g. banking details, credit rating, loan history)
- Information about or relating to intellectual property (e.g. trade secrets, creative ideas that could lead to patents, copyrights, new products)
- Day-to-day business operation information (e.g. current customer & supplier details, quotes, purchase history, call records)
- Commercial business information (e.g. strategic plans, financial business data)
- Personnel / HR information (e.g. appraisal, disciplinary info, salary, sickness records)

I think <information type> is...

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
secret	❍	❍	❍	❍	❍
private	❍	❍	❍	❍	❍
insignificant	❍	❍	❍	❍	❍
humiliating	❍	❍	❍	❍	❍
of interest to fellow employees	❍	❍	❍	❍	❍
privileged	❍	❍	❍	❍	❍
meaningless	❍	❍	❍	❍	❍
worthless	❍	❍	❍	❍	❍
of interest to business competitors	❍	❍	❍	❍	❍
of interest to criminals	❍	❍	❍	❍	❍
embarrassing	❍	❍	❍	❍	❍
discreditable	❍	❍	❍	❍	❍
confidential	❍	❍	❍	❍	❍
of interest to my family	❍	❍	❍	❍	❍
of interest to my friends	❍	❍	❍	❍	❍
restricted	❍	❍	❍	❍	❍
compromising	❍	❍	❍	❍	❍

8.8 | APPENDIX H: STORAGE AND PROCESSING OF INFORMATION

How regularly do you use a computer as part of your daily work tasks?

	Never	Rarely	Sometimes	Often	Always
Personal information about other people (e.g. address, gender, date of birth, marital status)	❍	❍	❍	❍	❍
Health information about other people (e.g. physical and mental health history, weight, family medical history)	❍	❍	❍	❍	❍
Lifestyle information about other people (e.g. shopping habits, hobbies, interests)	❍	❍	❍	❍	❍
Financial information about other people (e.g. banking details, credit rating, loan history)	❍	❍	❍	❍	❍
Information about or relating to intellectual property (e.g. trade secrets, creative ideas that could lead to patents, copyrights, new products)	❍	❍	❍	❍	❍
Day-to-day business operation information (e.g. current customer & supplier details, quotes, purchase history, call records)	❍	❍	❍	❍	❍
Commercial business information (e.g. strategic plans, financial business data)	❍	❍	❍	❍	❍
Personnel / HR information (e.g. appraisal, disciplinary info, salary, sickness records)	❍	❍	❍	❍	❍

8.9 | APPENDIX I: SECURITY BEHAVIOUR ITEMS

For the following questions think about how you behave within the workplace and rate how regularly you do the following behaviours

	Never	Rarely	Sometimes	Often	Always
I share passwords with other people at work	❍	❍	❍	❍	❍
I use complex passwords at work	❍	❍	❍	❍	❍
I use different passwords for different work accounts	❍	❍	❍	❍	❍
I personally run the security software including anti-virus, anti-spyware and firewalls at work	❍	❍	❍	❍	❍
I ensure I run the latest and official version of software (including operating system) at work	❍	❍	❍	❍	❍
I personally scan work devices for available software updates and install them at work	❍	❍	❍	❍	❍
I log out of websites when I finish at work	❍	❍	❍	❍	❍
I use trusted and secured connections, and devices (including Wi-Fi) when at work	❍	❍	❍	❍	❍
I use trusted and secure websites and services at work and connect securely	❍	❍	❍	❍	❍
I stay informed about security risks online and in the workplace	❍	❍	❍	❍	❍
I avoid security risks online and in the workplace	❍	❍	❍	❍	❍
I am aware of my physical surroundings when online at work	❍	❍	❍	❍	❍
I report suspicious or criminal activities in the workplace	❍	❍	❍	❍	❍
I personally back up data stored on my workplace devices	❍	❍	❍	❍	❍
I adjust account settings on websites that I use at work	❍	❍	❍	❍	❍
I lock my computer when I leave my workstation	❍	❍	❍	❍	❍

8.10 | APPENDIX J: DEMOGRAPHIC QUESTIONNAIRE

What is your gender?
○ Male
○ Female
○ Prefer not to say

What is your age?
_____

Do you have managerial responsibilities?
○ Yes
○ No
Are you responsible for data protection in your organisation?
○ Yes
○ No

How long have you worked for your company?
In years: _____
and months: _____

How long have you worked in your current position?
In years: _____
and months: _____

Is your organisation:
○ A micro enterprise (less than 10 staff)
○ A small enterprise (less than 50 staff)
○ A medium-sized enterprise (less than 250 staff)
○ A large organisation (more than 250 staff)

In what sector do you classify your main occupation?

- ⭕ Accountancy and business services
- ⭕ Advertising, marketing and PR
- ⭕ Armed forces and emergency services
- ⭕ Banking, investment and insurance
- ⭕ Charity and development work
- ⭕ Construction
- ⭕ Creative arts
- ⭕ Education
- ⭕ Energy and utilities
- ⭕ Engineering
- ⭕ Environment and agriculture
- ⭕ Fashion and design
- ⭕ Government and public administration
- ⭕ Health
- ⭕ Hospitality
- ⭕ Human resources and recruitment
- ⭕ Information technology
- ⭕ Legal services
- ⭕ Manufacturing
- ⭕ Media
- ⭕ Property
- ⭕ Publishing
- ⭕ Retail
- ⭕ Science
- ⭕ Social care
- ⭕ Sport and leisure
- ⭕ Tourism
- ⭕ Transport and logistics
- ⭕ Other (PLEASE STATE): _____

8.11 | APPENDIX K: STUDY 3 – ORGANISATION SECTOR DEMOGRAPHICS
Table 51. Study 3 - Organisational sectors from recruited sample

Organisational Sector	Percentage of participants from sector
Accountancy and business services	2.5%
Advertising, marketing and PR	.7%
Armed forces and emergency services	.2%
Banking, investment and insurance	.7%
Charity and development work	4.7%
Creative arts	.7%
Education	46.5%
Engineering	1.7%
Fashion and design	.2%
Government and public administration	1.7%
Health	6.5%
Hospitality	2.5%
Human resources and recruitment	1.0%
Information technology	7.2%
Legal services	.5%
Manufacturing	.5%
Media	.7%
Property	.2%
Retail	4.5%
Science	3.7%
Social care	1.2%
Sport and leisure	1.7%
Telecommunications	3.2%
Tourism	.2%
Transport and logistics	.2%
Other (Unclassified)	6.0%

8.12 | APPENDIX L: DEVICE USAGE IN THE WORKPLACE

Which of the following devices (personally-owned or company-owned) do you use MOST for work-related tasks? (SELECT ONE)

Work-related tasks are activities you may do on devices such as accessing emails, editing work documents, accessing company information etc.

○ Desktop PC
○ Laptop
○ Smartphone
○ Tablet
○ Other [please state]: _____

Is this device:

○ Company-owned
○ Personally-owned

What is the operating system for this device?

○ Microsoft Windows
○ Mac OS X
○ Linux
○ iOS
○ Android
○ Other [please state]: _____

8.13 | APPENDIX M: PERCEIVED SUSCEPTIBILITY AND SEVERITY ITEMS

Please answer the following questions using a rating scale of Strongly Disagree to Strongly Agree

Perceived Susceptibility	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
My work device is at risk of becoming infected with malware	❍	❍	❍	❍	❍
I am unlikely to infect my work device with malware in the future	❍	❍	❍	❍	❍
My chances of infecting my work device with malware in the future are high	❍	❍	❍	❍	❍
It is likely that my work device will become infected with malware	❍	❍	❍	❍	❍

Perceived Severity	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
If my work device were infected by *malware*… …the consequences would be severe					
…the consequences would be serious	❍	❍	❍	❍	❍
…the consequences would be significant	❍	❍	❍	❍	❍
…it would run significantly slower	❍	❍	❍	❍	❍
… my organisation's computer network could be severely disrupted	❍	❍	❍	❍	❍
…I could be severely disciplined	❍	❍	❍	❍	❍
…I would be seriously embarrassed	❍	❍	❍	❍	❍
…my personal information and data could be severely at risk	❍	❍	❍	❍	❍
…it could significantly reduce my productivity	❍	❍	❍	❍	❍
…there would severe complications for my organisation's service users/customers	❍	❍	❍	❍	❍
…it could lead to my organisation having severely dissatisfied service users/customers	❍	❍	❍	❍	❍
…there could be severe consequences to company data and files	❍	❍	❍	❍	❍
…the organisation's image could be seriously damaged	❍	❍	❍	❍	❍

8.14 | APPENDIX N: SECURITY RESPONSIBILITY ITEMS

The following question is about your opinions on who is responsible for certain activities in the workplace. Using the slider below and for each statement please indicate whose responsibility you feel it is to undertake the activity with a rating scale from 1 to 5. Scores closer to 1 indicate your company's responsibility whereas scores closer to 5 indicate your responsibility
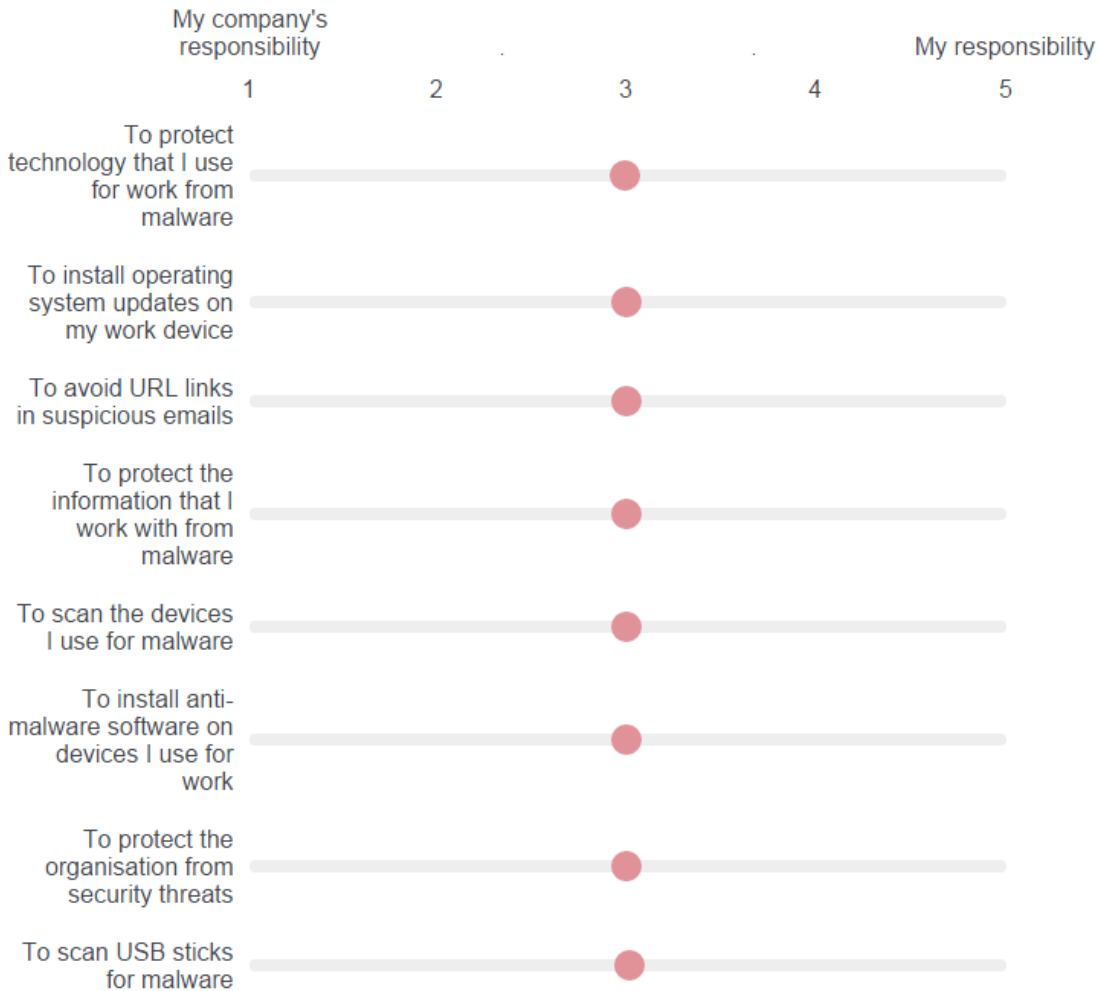
8.15 | APPENDIX O: PAST EXPERIENCE ITEMS

Please indicate whether or not you have ever experienced any of the following situations at HOME on your personally-owned devices (e.g. PC, laptop, mobile phone, tablet).

	Yes	No	I don't know	Not Applicable
My personal device has been infected by malicious software (e.g. viruses, Trojans, worms)	❍	❍	❍	❍
My financial information has been stolen from my computer	❍	❍	❍	❍
My personal account (e.g. email, social media) has been used by someone without my permission	❍	❍	❍	❍
My device resources (computer, internet, software, hardware) have been inaccessible/unusable because of computer security problems	❍	❍	❍	❍
I have been tricked into giving away my personal information online	❍	❍	❍	❍
Files on my personal device have been lost due to security problems	❍	❍	❍	❍

Please indicate whether or not you have ever experienced any of the following situations at WORK on your company-owned devices (e.g. PC, laptop, mobile phone, tablet).

	Yes	No	I don't know	Not Applicable
My work device has been infected by malicious software (e.g. viruses, trojans, worms)	❍	❍	❍	❍
Information has been stolen from my work device	❍	❍	❍	❍
My work account (e.g. email, computer logins) has been used by someone without my permission	❍	❍	❍	❍
My work device resources (computer, internet, software, hardware) have been inaccessible/unusable because of computer security problems	❍	❍	❍	❍
I have been tricked into giving away information about work online	❍	❍	❍	❍
Files on my work device have been lost due to security problems	❍	❍	❍	❍

8.16 | APPENDIX P: RESPONSE EFFICACY ITEMS

<Security behaviour> (Using the anti-malware software to scan suspect USB sticks for malware/ Installing software updates on my work device/ Not clicking on URL links in suspicious emails).....

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
...is effective in preventing problems for my organisation's service users/customers	○	○	○	○	○
...works in preventing malware	○	○	○	○	○
...reduces the likelihood of getting malware	○	○	○	○	○
...works in ensuring that my work device runs as efficiently as possible	○	○	○	○	○
...works in securing my organisation's data and files	○	○	○	○	○
...is effective in ensuring that I don't get embarrassed due to infecting my work device with malware	○	○	○	○	○
...is effective in protecting the organisation's network from the spreading of malware	○	○	○	○	○
...reduces the likelihood of my productivity getting affected by malware	○	○	○	○	○
...reduces my chances of being disciplined	○	○	○	○	○
...works in protecting the reputation of my organisation	○	○	○	○	○
...is effective in preventing malware	○	○	○	○	○
...reduces the likelihood of dissatisfied service users/customers for my organisation	○	○	○	○	○
...is effective in protecting my personal information and data	○	○	○	○	○

8.17 | APPENDIX Q: SELF-EFFICACY ITEMS

For the following questions, please indicate the extent to which you agree with the statements using a rating scale from strongly disagree to strongly agree

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I am discouraged from <security behaviour> because I feel unable to do so	○	○	○	○	○
I feel confident in my ability to <security behaviour>	○	○	○	○	○
It would not be difficult for me to <security behaviour>	○	○	○	○	○
<security behaviour> would be easy for me	○	○	○	○	○

8.18 | APPENDIX R: RESPONSE COSTS ITEMS

Using the anti-*malware software to scan suspect USB sticks for malware…*

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
...would slow my work device down	❍	❍	❍	❍	❍
...would reduce my productivity	❍	❍	❍	❍	❍
...can lead to non-malicious files being identified as infected with malware	❍	❍	❍	❍	❍
...would be time consuming	❍	❍	❍	❍	❍
...could lead to important files being destroyed	❍	❍	❍	❍	❍
...would require considerable effort	❍	❍	❍	❍	❍
...would have a considerable financial cost for me	❍	❍	❍	❍	❍

Installing software updates on my work device...

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
...could lead to important files being destroyed	❍	❍	❍	❍	❍
...would reduce my productivity	❍	❍	❍	❍	❍
...would slow my work device down	❍	❍	❍	❍	❍
...could lead to a less reliable or 'buggy' software version being installed	❍	❍	❍	❍	❍
...would require considerable effort	❍	❍	❍	❍	❍
...would be time consuming	❍	❍	❍	❍	❍

Not clicking on URL links in suspicious emails...

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
...would require considerable effort	❍	❍	❍	❍	❍
...would reduce my productivity	❍	❍	❍	❍	❍
...would slow my work device down	❍	❍	❍	❍	❍
...would be time consuming	❍	❍	❍	❍	❍

8.19 | APPENDIX S: PROTECTION MOTIVATION ITEMS

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Email security					
I intend to not click on URL links in suspicious emails	○	○	○	○	○
If I receive a suspicious email, I will not click on the URL links	○	○	○	○	○
I plan to not click on URL links in suspicious emails	○	○	○	○	○
SU security					
I intend to install software updates on my work device as soon as I am prompted to do so	○	○	○	○	○
If I was prompted to install software updates on my work device, I would do it immediately	○	○	○	○	○
I plan to install software updates on my work device as soon as I am prompted to do so	○	○	○	○	○
AMS security	○	○	○	○	○
I intend to use the anti-malware software to scan suspect USB sticks for malware	○	○	○	○	○
If I had a suspect USB stick, I would scan it for malware using the anti-malware software	○	○	○	○	○
I plan to use the anti-malware software to scan suspect USB sticks for malware	○	○	○	○	○

8.20 | APPENDIX T: IMPLICIT SECURITY TASK

Site Cookies

This cookie stores basic user information on your computer, potentially improving the browsing experience and helping us deliver more relevant information to you

Do you want to use this option?

ACCEPT   DON'T ACCEPT

8.21 | APPENDIX U: INSTRUCTIONS

SOFTWARE UPDATES SECTION

The following section is about software updates. Your operating system (e.g. windows, mac) may from time to time prompt you to install updates and this section is about your thoughts about these updates. These may appear on your device like this:
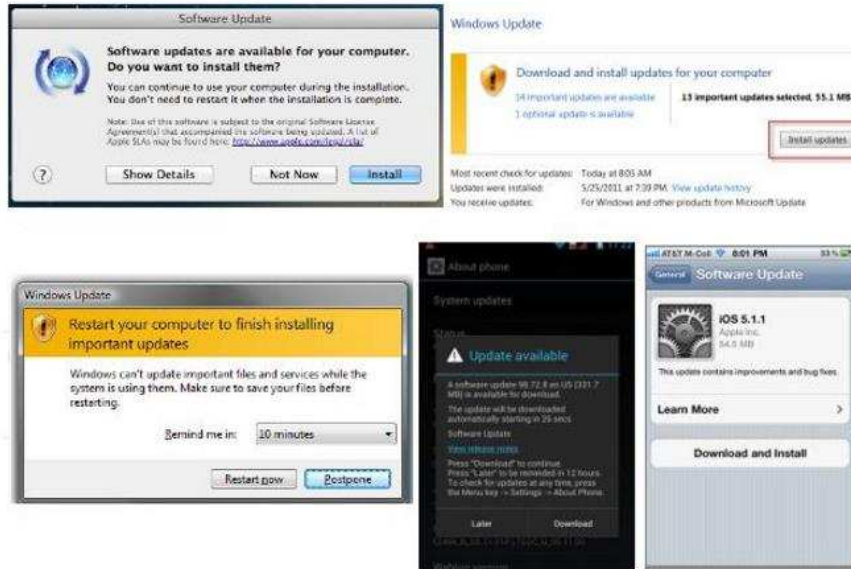
ANTI-MALWARE SOFTWARE & USB STICKS SECTION

KEY TERMS

Anti-malware software is security software such as an anti-virus which detects malicious software installed on your device. The pictures below represent examples of anti-malware software
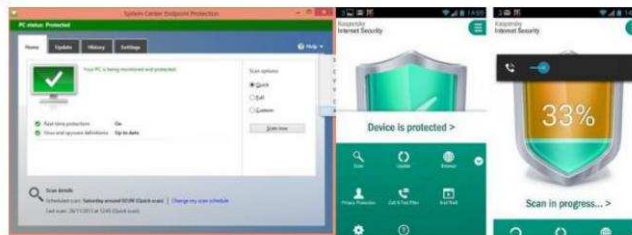
USB sticks also known as pen drives and flash drives are a form of removable media that allow you to store information and data

Suspect USB sticks - Here we are referring to USB sticks that you suspect of containing malware. For example, this may be due to the USB stick being used in someone else's machine, you may have been given it by a third party, found it or sent to you by an advertiser.

245

EMAIL USAGE SECTION

The following section is about using your work email and the security of the information you send and receive. Below are two examples of 'suspicious emails' that you may receive on your personal and work emails.

BARCLAYS

Dear Valued Customer,

For your security, Barclays Bank has safeguard your account when there is a possibility that someone other than you is attempting to Access your account from an unidentified location. You now need to verify your **Identity**.

To verify your **identity,** kindly follow the reference below and instantly re-activate your account.

https://bank.**barclays**.co.uk/olb/auth/verification/

Thank you for helping us to protect you.

Security Advisor
Barclays Bank PLC .

HM Revenue & Customs

Dear

We have detected that you have paid too much tax in the past, due to an official error. Therefore HMRC applied ESC B41 to issue a repayment for tax years which are now out of date under the strict statute.

Please follow the link below to reclaim your overpaid tax.
Document Reference: 60220848.

The security and confidentiality of your personal information is important for us. If you have any questions, please either call the toll-free customer service phone number.
Â© 2014, all rights reserved

8.22 | APPENDIX V: INTERCORRELATIONS BETWEEN VARIABLES

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
WISA Privacy (1)	-																										
WISA Consequences (2)	.086																										
WISA Worth (3)	.314**	-.341**																									
WISA Low proximity (4)	.079	.126**	.166**																								
WISA High proximity (5)	-.176**	.205**	-.249**	.183**																							
Perceived susceptibility (6)	-.070	.211**	-.218**	.021	.193**																						
PS Organisational (7)	.180**	.151**	.106*	.153**	.004	.074																					
Ps consequences (8)	.160**	.078	.128**	.084	-.044	.074	.480**																				
Ps personal (9)	.141**	.092	.053	.056	-.062	-.085	.506**	.376**																			
Ps Productivity (10)	.054	-.048	.126**	.139**	-.098*	-.113*	.302**	.271**	.180**																		
OCB (11)	.046	-.081	.154**	.230**	.061	.031	.163**	.125**	.110*	.121**																	
Personal security experience (12)	-.020	-.042	.016	-.007	.138**	-.016	-.038	-.028	.009	-.108*	-.040																
Work security experience (13)	-.016	.036	-.119*	-.075	.117*	.000	-.038	-.068	-.039	-.129**	-.197**	.302**															
Psych ownership – Data (14)	.054	-.042	.056	-.037	-.026	.013	-.187**	.035	-.033	.057	.132**	-.032	-.039														
Psych ownership – Tech (15)	.028	-.028	.008	.078	.038	.041	-.141**	-.010	-.106*	.053	.189**	.012	.043	.656**													
Responsibility (16)	.063	-.014	.046	.031	.030	.042	-.206**	-.085	.025	-.101*	.089	.027	-.047	.286**	.351**												
Self-efficacy (AMS) (17)	.014	-.180**	.173**	.116*	-.049	-.199**	-.098	-.027	.027	.012	.095	-.040	-.118*	.094	.167**	.288**											
Response efficacy (AMS) (18)	.137*	-.059	.075	.055	-.117*	-.090	.134*	.149**	.199**	.156**	-.009	-.209**	-.064	.117*	.068	.067	.282**										
Response costs (AMS) (19)	-.029	.270**	-.182**	-.011	.291**	.150**	.040	.082	.048	-.095	.064	.016	.065	-.053	.010	-.096	-.303**	-.186**									
Self-efficacy (ES) (20)	.069	-.213**	.272**	.109*	-.212**	-.233**	.067	.097	.078	.168**	.017	-.028	-.086	.005	-.118*	.012	.209**	.138*	-.185**								
Response efficacy (ES) (21)	.208**	-.003	.211**	.081	-.116*	-.142**	.205**	.143**	.181**	.251**	.141**	-.146**	-.106*	.062	.022	-.008	.159**	.506**	-.115*	.360**							
Response costs (ES) (22)	-.120*	.294**	-.295**	-.058	.250**	.254**	-.022	-.029	.031	-.119*	-.079	.041	.051	-.050	.046	-.003	-.179**	-.081	.299**	-.576**	-.300**						
Self-efficacy (SU) (23)	-.074	-.150**	.088	.058	-.054	-.117*	-.191**	-.091	-.090	.022	.039	-.021	.015	.125**	.183**	.245**	.463**	.191**	-.148**	.121*	.085	-.169**					
Response costs (SU) (24)	.102*	.145**	-.050	-.021	.092	.143**	.185**	.117*	.068	.096*	.008	-.023	-.025	-.117*	-.067	-.121*	-.264**	-.061	.389**	-.098	.017	.234**	-.398**				
Response efficacy (SU) (25)	.020	.022	.040	-.019	-.115*	-.057	.135**	-.002	.092	.087	.105*	-.135**	-.039	.050	.055	.083	.209**	.459**	-.183**	.070	.255**	-.042	.182**	-.294**			
AMS intention (26)	.030	-.022	.133*	.124*	-.048	-.070	-.050	-.050	.003	.018	.053	-.009	-.087	.095	.161**	.316**	.545**	.326**	-.348**	.155**	.165**	-.065	.254**	-.216**	.287**		
SU intention (27)	.012	.000	.049	.052	-.020	.084	-.019	.029	-.024	.069	.083	-.058	-.052	.177**	.159**	.231**	.204**	.170**	-.214**	.015	.029	.047	.256**	-.360**	.398**	.337**	
ES intention (28)	.083	-.179**	.254**	.026	-.206**	-.255**	.031	.100*	.033	.157**	.061	-.069	-.143**	.068	-.058	.016	.166**	.109	-.174**	.665**	.335**	-.520**	.114*	-.086	.024	.146**	-.009

Table 52 showing mean differences for response efficacy items for all behaviours and p values resulting from Bonferroni corrected repeated measures t tests

Response efficacy item			Mean Difference
...is effective in preventing problems for my organisation's service users/customers	AMS	SU	.408[***]
		ES	-.283[***]
	SE	AMS	-.408[***]
		ES	-.691[***]
	ES	AMS	.283[***]
		SU	.691[***]
...works in preventing malware	AMS	SU	.469[***]
		ES	-.328[***]
	SE	AMS	-.469[***]
		ES	-.797[***]
	ES	AMS	.328[***]
		SU	.797[***]
...reduces the likelihood of getting malware	AMS	SU	.402[***]
		ES	-.277[***]
	SE	AMS	-.402[***]
		ES	-.678[***]
	ES	AMS	.277[***]
		SU	.678[***]
...works in ensuring that my work device runs as efficiently as possible	AMS	SU	.051
		ES	-.373[***]
	SE	AMS	-.051
		ES	-.424[***]
	ES	AMS	.373[***]
		SU	.424[***]
...works in securing my organisation's data and files	AMS	SU	.318[***]
		ES	-.338[***]
	SE	AMS	-.318[***]
		ES	-.656[***]
	ES	AMS	.338[***]
		SU	.656[***]
...is effective in ensuring that I don't get embarrassed due to infecting my work device with malware	AMS	SU	.328[***]
		ES	-.550[***]
	SE	AMS	-.328[***]
		ES	-.878[***]
	ES	AMS	.550[***]
...is effective in protecting the organisation's network from the spreading of malware	AMS	SU	.280[***]
		ES	-.222[***]
	SE	AMS	-.280[***]

Response efficacy item			Mean Difference
		ES	-.502[***]
	ES	AMS	.222[***]
		SU	.502[***]
...reduces the likelihood of my productivity getting affected by malware	AMS	SU	.347[***]
		ES	-.325[*]
	SE	AMS	-.347[***]
		ES	-.672[***]
	ES	AMS	.325[***]
		SU	.672[***]
...reduces my chances of being disciplined	AMS	SU	.383[***]
		ES	-.196[**]
	SE	AMS	-.383[***]
		ES	-.579[***]
	ES	AMS	.196[**]
		SU	.579[***]
...works in protecting the reputation of my organisation	AMS	SU	.206[***]
		ES	-.267[***]
	SE	AMS	-.206[***]
		ES	-.473[***]
	ES	AMS	.267[***]
		SU	.473[***]
...is effective in preventing malware	AMS	SU	.415[***]
		ES	-.344[***]
	SE	AMS	-.415[***]
		ES	-.759[***]
	ES	AMS	.344[***]
		SU	.759[***]
...reduces the likelihood of dissatisfied service users/customers for my organisation	AMS	SU	.264[***]
		ES	-.228[***]
	SE	AMS	-.264[***]
		ES	-.492[***]
	ES	AMS	.228[***]
		SU	.492[***]
...is effective in protecting my personal information and data	AMS	SU	.280[***]
		ES	-.473[***]
	SE	AMS	-.280[***]
		ES	-.752[***]
	ES	AMS	.473[***]
		SU	.752[***]

*p<.05; **p<.01, ***p<.001

8.24 | APPENDIX X: RESPONSE COSTS PAIRWISE COMPARISONS

Table 53 showing AMS security mean differences for response cost rating for all items and p values resulting from Bonferroni corrected repeated measures t tests

	1	2	3	4	5	6	7
(1)...would slow my work device down	-	-.14**	.361***	.228***	-.194*	-.309***	-.630***
(2)...would reduce my productivity		-	.503***	.370***	-.052	-.167*	-.488***
(3)...can lead to non-malicious files being identified as infected with malware			-	-.133	-.556***	-.670***	-.991***
(4)..would be time consuming				-	-.423***	-.537***	-.858***
(5)...could lead to important files being destroyed					-	-.114	-.435***
(6)...would require considerable effort						-	-.321***
(7)...would have a considerable financial cost for me							-

*p<.05; **p<.01, ***p<.001

Table 54 showing SE security mean differences for response cost rating for all items and p values resulting from Bonferroni corrected repeated measures t tests

	1	2	3	4	5	6
(1)...could lead to important files being destroyed	-	-0.078	-.159*	-.422***	0.092	-.332***
(2)...would reduce my productivity		-	-0.081	-.344***	0.171	-.254***
(3)..would slow my work device down			-	-.263***	.251***	-.173**
(4)...could lead to a less reliable or 'buggy' software version being installed				-	.514***	0.09
(5)...would require considerable effort					-	-.424***
(6)...would be time consuming						-

*p<.05; **p<.01, ***p<.001

Table 55 showing ES security mean differences for response cost rating for all items and p values resulting from Bonferroni corrected repeated measures t tests

	1	2	3	4
(1)... would require considerable effort		-.1078	-.131*	-.061
(2)... would reduce my productivity		-	-.023	.047
(3)..would slow my work device down			-	.070
(4)... would be time consuming				-

*p<.05; **p<.01, ***p<.001

WELCOME TO THE COMPUTER HUB

The aim of this hub is to provide you with information so that you can protect yourself and your information when using your computer and the internet.

COMPUTER SECURITY

The personal information that is stored on our computers, mobile phones, tablets etc. is vulnerable to the many cyber criminals that wish to source, collect and use our information for financial gain.

The likelihood of a breach to our personal information is extremely high. In 2013 alone, Symantec reports that over 552 million identities were breached putting users' information directly into the hands of cyber criminals. This included their credit card data, birth dates, email addresses, passwords and medical records amongst other highly sensitive personal data.

Cyber criminals use a number of techniques to attempt to access our computers and information which often involve deceptive tactics to gain access without our knowledge. One particular tool at their disposal **is Malware** which will be the focus of the session today and in particular, how attackers use emails to try and get malware onto your computer.

Imagine receiving that message on your work computer

- You are ordered to pay a fine as your computer has been locked by the FBI and your computer files are held at ransom
- There is no way to access your files again, even if you pay the fine
- Of course, this software is not really the FBI but hackers who have installed the software on your computer and locked away your files
- This is known as ransomware; a nasty type of malware

Malware – What is it?

Malware is short for "malicious software" and is any kind of unwanted software that is installed onto your device without your adequate consent. Below are examples of Malware and what they can do to your computer:

- **Viruses** - alter the way your computer operates and replicates itself across your computer and any other computers on the same network "infecting" everything. Akin to a biological virus that makes you sick, they are persistent and keep you from functioning normally and are difficult to get rid of. Computer viruses slow your computer down, access your private information, spam your contacts, monitor your online behaviour and corrupt your data.

- **Trojans** – pretend to be real programs but trick you into loading the Trojan onto your computer. Once on your system it can execute a number of actions such as starting annoying pop-up windows to damage such as deleting and stealing files. Trojans also create backdoor access to give hackers access to your system.

- **Ransomware** - are a specific form of malware that holds your PC or files to ransom. The FBI ransom (as shown on the previous slide) is an example of this malware.

- **Keyloggers** – logs the keys struck on your keyboard without your knowledge. This allows hackers to steal your passwords and other confidential information.

How does malware get onto my computer?

There are many ways malware can get onto your computer, however today we will focus on "phishing emails" or "malicious spam". You will be familiar with getting these emails. They look real but are trying to trick you into giving away your personal information or tricking you into downloading malware.

- Malware can be hidden in these emails in two ways:

  1. **In the links within the email** – clicking on them takes you to websites where the malware will be downloaded simply by visiting the website

  2. **Hidden in attachments in the email** – downloading and opening the file is enough for it to infect your machine

Am I at risk?

– Employees are a major cause of security breaches in organisations. Organisations regularly experience security breaches, for example **81% of large organisations and 60% of small organisations experienced a security breach in the last year** (Price Waterhouse Coopers, 2014).

– Employees account for a large proportion of these breaches due to their insecure behaviour which includes clicking on links in suspicious emails. **If you are clicking on links in emails without checking the email is genuine first, then you are leaving your work computer open to be exploited by malware and you will help contribute to these high statistics.**

– In November 2014, 55% of all email sent were phishing emails and 41% of these contained malware links (Symantec). These statistics demonstrate the likelihood that **YOU** will receive malicious phishing emails, it is therefore important to check that all emails you receive are genuine before clicking on links and downloading attachments.

Security breach issues at work

- You may have experienced one of the following situations on your work computer before:
  - Your work computer infected by malware
  - Information stolen from your work computer
  - Your work account (e.g. email, computer logins) used by someone without your permission
  - Your computer resources (internet, software, hardware) inaccessible/unusable because of computer security problems
  - Tricked into giving away information about work online
  - Files on your work device lost due to security problems

Its important to remember these experiences and that by engaging in security behaviours will **significantly reduce** the chance of these happening again

PROTECTING AGAINST MALWARE PHISHING EMAILS

In this section, we will be outlining simple steps that you can take to help protect yourself and your company from malware
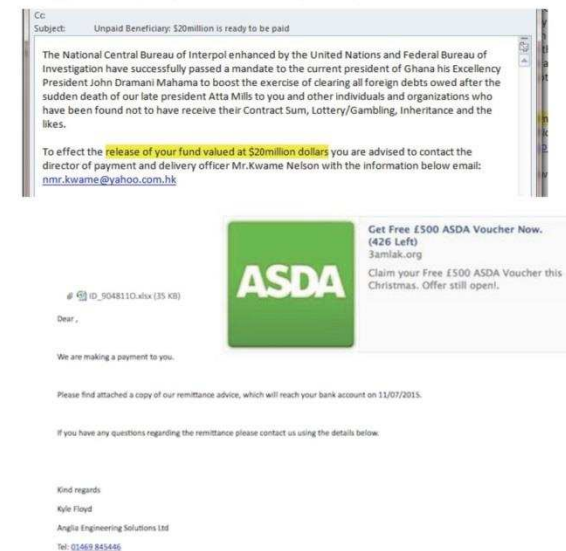
INSPECT THE EMAIL CONTENT – WATCH OUT FOR EMOTIONS

Attackers use emotional triggers to get you to react quickly

GREED

Phishing emails often provide a financial reward if you click on a link or provide your information. Emails which suggest that you have won something or are eligible for a refund should raise alarm bells.

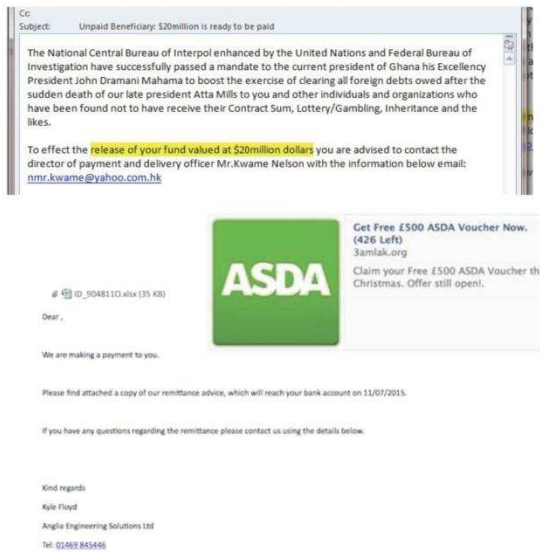**Remember.** If an email offers something that seems too good to be true, it probably is.

Cc:
Subject: Unpaid Beneficiary: $20million is ready to be paid

The National Central Bureau of Interpol enhanced by the United Nations and Federal Bureau of Investigation have successfully passed a mandate to the current president of Ghana his Excellency President John Dramani Mahama to boost the exercise of clearing all foreign debts owed after the sudden death of our late president Atta Mills to you and other individuals and organizations who have been found not to have receive their Contract Sum, Lottery/Gambling, Inheritance and the likes.

To effect the release of your fund valued at $20million dollars you are advised to contact the director of payment and delivery officer Mr.Kwame Nelson with the information below email: nmr.kwame@yahoo.com.hk

Get Free £500 ASDA Voucher Now. (426 Left)
3amlak.org

ASDA

Claim your Free £500 ASDA Voucher this Christmas. Offer still open!.

ID_904811O.xlsx (35 KB)

Dear ,

We are making a payment to you.

Please find attached a copy of our remittance advice, which will reach your bank account on 11/07/2015.

If you have any questions regarding the remittance please contact us using the details below.

Kind regards

Kyle Floyd

Anglia Engineering Solutions Ltd

Tel: 01469 845446

Inspect the email content – Watch out for emotions

Attackers use emotional triggers to get you to react quickly

Greed

Phishing emails often provide a financial reward if you click on a link or provide your information. Emails which suggest that you have won something or are eligible for a refund should raise alarm bells.

Remember. If an email offers something that seems too good to be true, it probably is.

Urgency

Attackers want to fluster you into clicking on a link, responding to an email or downloading an attachment by creating a sense of urgency

If there is a strict deadline in the email, then be suspicious. For example, "if you do not take these additional steps to keep your account safe then your account will be deactivated in 5 days"

256

CURIOSITY

Attackers know and exploit the fact that people are naturally curious. They will try to persuade you to download an attachment or click on a link to something that is exciting or intrigues us.

Example. If the email is suggesting that someone is trying to share you photos or files to entice you to looking at them

From: T-mobile <derekfb7@jaywire.org>
Sent: 10 April 2015 12:05
To: Lisa Thompson
Subject: T-Mobile MMS Service

T-Mobile_voice_835FABB73A60667C78FA.zip (67 KB)

This e-mail contains a voice message.
Download and listen to message in attached file.

Sender:
Mobile: +44702*******
Passcode: DBE480971B28

for Lisa Thompson
Subject: Look at this picture I took last night

I did take more which are uploaded here

http://mad3tech.gr/wp-includes/dex.php

FEAR

Scaring people into acting is a common tactic used in phishing emails.

Emails that threaten you with negative consequences or punishment should always be treated with caution. For example, suspending your account or suggesting you may get fined

NICE National Institute for Health and Care Excellence

Dear Lisa Thompson,

We have been sent a sample of your blood analysis for further research.
During the complete blood count (CBC) we have revealed that white bloody cells is very low, and unfortunately we have suspicion of a cancer.

Wite Blood cells	1200 Low
Hemoglobin	12 Normal
Platelets	19000 Low

We suggest you print out your CBC test results and interpretations in the attachment and visit your family doctor as soon as possible.

Subject: Latest Update - Tesco Bank Security Centre

Dear Customer,

We recently reviewed your accounts, and noticed irregular activities we would like to further verif

However, access to your accounts has been blocked due to possible errors detected.

You are requested to follow one simple step in order to restore

your online access and to review your statements.

Tesco online secure Login   http://new.indicana.com/i.htm

Cc:
Subject: SECURE TRUST BANK PLC has issued the claim against you and passed for consideration to HM Courts [DK6394\
Message   Warning.txt (592 B)

SECURE TRUST BANK PLC has issued the claim against you and passed for consideration to HM Courts [DK6394WTC]

SECURE TRUST BANK PLC,

Phillip Buckley

257

SMALL THINGS TO LOOK OUT FOR

You've got mail!

Not addressed to you
Emails that say "dear customer" or do not have your name in the body of the text should make you concerned that the email is not genuine

Email signatures
A lack of email signature or an overly ge~~neral~~ ~~signature may indicate~~ that something is wrong

Email tone
If the em~~ail~~ ~~is written in an unusual way for a~~ colleague. Consider t~~he way your company, friends~~ and colleagues talk so if it ~~seems out of character~~ for them, be suspicious of the rest of ~~the email~~

~~**Spelling a**~~nd grammar
~~If~~ you looked at a phishing email from 5 years ago, it would have been riddled with spelling and grammar mistakes. Attackers are a lot more sophisticated but it is still worth checking as it can be a sign that the email is not genuine.

Logos and look
Poor quality logos or lack of logos can often be a sign that it is fake

More sophisticated phishing emails will have this covered

ALWAYS LOOK AT THE FOLLOWING

SENDER ADDRESS

From: Apple iTunes <orders@tunes.co.uk>
Sent: 10 April 2015 16:34
To: Lisa Thompson
Subject: Your receipt No.111034281212

Look closely at the email address - here, it looks real but upon inspection the address only says "tunes" and not iTunes. Be careful though, attackers know how to work email clients so that the email will say it is coming from an official web address – this is called "email spoofing" and it is surprisingly easy for attackers to do. For example, the email below is the real email address for Netflix but attackers have spoofed the email so that it appears to be coming from them but in fact it is not.

From: NETFLIX <secure@netflix.co.uk>
Sent: 10 April 2015 12:48

We will now focus on the two main ways you can get malware from emails and how to avoid them
1. Downloading and opening attachments
2. Clicking on suspicious URLS

258

What are the benefits?

- Not clicking on links and not downloading attachments in suspicious emails is very important. You may feel that it requires more effort and time, and may affect your productivity and device efficiency.

- However, it only takes a few more seconds to check the email is genuine before clicking or downloading. You will be reassured that you are reducing the likelihood of getting malware by doing so.

- Being cautious with links and attachments in emails is a very important and effective way to prevent malware getting onto your work computer. This will protect your own personal information and data, reduce the likelihood of your productivity getting affected by malware and ensuring you don't get embarrassed for infecting your work device with malware.

- Finally, by being cautious with links and attachments in emails will help secure your organisation's data and files, prevent problems for your organisations service users/customers and protect the company's network from the spreading of malware.

Email Attachments

As a basic rule, never open any attachment to an email, unless you are expecting it

Attackers can hide malware in all common file types that you are likely to come into contact with at work including doc, pdfs, zip, xls

Simply downloading and opening the file is enough for the malware to infect your computer

Always check that the email is genuine, before downloading an attachment

Links

- You will regularly receive emails that contain links to websites so its very easy to just click on links without checking them first
- **Always check email links before clicking**

Hover over the link

Attackers will often mask web links. If you hover over a link without clicking on it, the actual web link will appear. For example, both these web links link to a fake Facebook website, but you wouldn't know that without hovering **(Give it a try!)**:
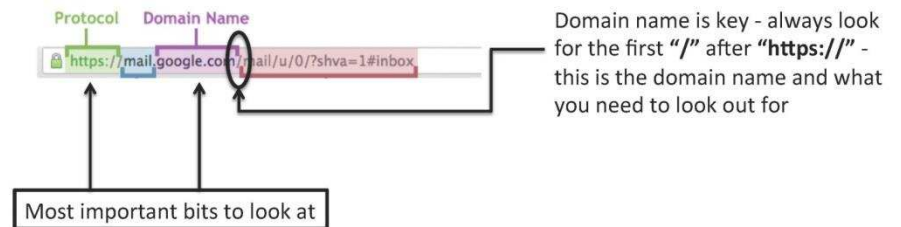
Click here
http://www.facebook.com/

Detecting a fake web link – how to know it's real

Attackers want their web links to look as real as possible so will make subtle changes to deceive people. Here we will teach you about checking the domain of the link to make sure it is legit

The "domain name" is the website which you want visit and can be difficult to identify on links as websites have many pages, however the simple rule below will help you find it.

Protocol   Domain Name

https://mail.google.com/mail/u/0/?shva=1#inbox

Domain name is key - always look for the first **"/"** after **"https://"** - this is the domain name and what you need to look out for

Most important bits to look at

260

HERE ARE SOME EXAMPLES

✅ https://www.facebook.com/jbrown/friends

Genuine website:
Facebook.com

❌ http://www.facebook.com.hyjjh1q.com/jbrown/friends

Fake website:
Hyjjh1q.com

❌ http://www.faceday.com/www.facebook.com/index.php?/jbrown/friends

Fake website:
faceday.com

Remember.

To find domain name. Always look for the first "/" after "http://", the domain name is before it/

https:// - sometimes web addresses start with http://, the addition of "**s**" indicates that the website is secure and you should check this when making a financial transaction

TEST

- Click on the link below for a test, can you identify which of these web links are fake and which ones are real?

- https://nupsych.qualtrics.com/SE/?SID=SV_6P5Vfetv8pn0BsF

Use a link scanner

If you are unsure whether the link is safe, **don't worry**. You can use a link scanner which will check if it safe by searching many anti-virus databases and let you know if it is unsafe. If you need to check a link, simply right click on the link and click on "copy hyperlink", then just paste it into the URL scanner website

Virustotal.com is free link scanner

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Dangers of short links

Short links and tiny URLs are shortened URLs (such as TinyURL, bit.ly) that allow users to take a link that is too long to fit in the confines of a twitter post and generates a short link that redirects you to the actual longer URL the user is linking to

For example, the link below

https://www.sophos.com/en-us/security-news-trends/best-practices/phishing.aspx

would be shortened to the following:

http://tinyurl.com/pwm2yp3

The new link looks nothing like the original link (even when hovering over it) so attackers use these services to trick users into visiting malicious websites. The use of this trick is seen more and more in phishing emails.

Fortunately there a number of websites you can learn the hidden path without visiting it.

Untiny.me – all you have to do is copy and paste the URL onto a website like this which will tell you the true web address. Phew!

RECAP

- Always check emails are genuine BEFORE clicking on attachments and links

- Remember that malware can embedded in most file types in attachments

- Check the domain on email links before clicking

- Un-shorten links that have been shortened

- Use a link scanner if you are uncertain

8.26 | APPENDIX Z: VOLITIONAL HELP SHEET

Participant Number:

Employees are more successful at checking if emails are genuine before clicking on links **if they identify situations in which they are tempted to not do so and pick strategies to overcome these situations.** We would like you to do this now. From the list, select up to 4 **"tempting situations"** (choose the ones in which you know you have the most difficulty when it comes to checking whether emails are genuine). Then use the list of **"strategies"** to decide what you will do to resist the tempting situation in the future. It is important that you make a link between the tempting situations and the strategies that you select: <u>Draw a line to link each tempting situation that you choose (on the left) with one strategy (on the right)</u>. You may choose the same strategy or different strategies to deal with the tempting situations that you select.

'Tempting situations'   ### 'Strategies'

If I am tempted to click on a link in an email without checking its genuine...	Then I will...
when I am interested in what is on the link	Remind myself that I am not saving much time by not checking if its real
when a colleague tells me to click on it	Seek out more information (e.g. from colleagues, IT, the internet) about the email
when it would disturb my work flow	Remember that not checking email authenticity contradicts the view I have of myself as a responsible person
when I have just started the working day	Remember that when I have not checked whether the email is real, I will become concerned about my computer security
when the email is from a colleague	Tell myself that I am capable of checking whether emails are genuine
when I am busy	Remind myself that I have a commitment to my organisation to protect its data
when the email is urgent	Rather than viewing checking emails as simply another rule to follow, I will see it as my opportunity to help protect data
when I might suffer negative consequences if I don't click on it	Make a concerted effort to ignore the urge/pressure to not check emails
when it's not labelled as spam by my email client	Try to avoid putting myself in that situation again in the future
when I have got lots of emails to get through	Try to control my impulses to click on links without checking if they are real first
when the email link looks real	Remind myself that I will have a more efficient and secure computer
when the email address from the sender looks real	Seek advice from others (e.g. colleagues, IT, those more experienced in computers) about how to avoid such situations in the future
when it has been addressed to me personally	Remind myself that people in my organisation will be supportive of me checking emails before clicking on links
when it's from a well-known company	Think about the embarrassment I will suffer if I cause a security breach at work
when it would require too much effort	Think about how irritated I will be if my computer is unusable due to malware
when I don't have enough time	Think about how if I check whether emails are genuine, it will prevent me from becoming a burden to my organisation/ IT department
when the email is from somebody that I trust	Remember that I could spread malware onto my friends and colleagues computers
when I need to as part of my job	Remind myself that I could get in trouble by my organisation/management for not checking whether emails are real
when the email message highlights a security issue	Remind myself that the government could fine my organisation up to £500, 000 for a security breach
when there is a financial reward for clicking	Tell myself that I am protecting my organisation from malware by taking extra steps to check if the email is real

8.27 | APPENDIX AA: EXAMPLE PHISHING EMAIL

From: Dropbox <no-reply@dropbox.com>
Sent: 11 April 2015 13:41
To: Lisa Thompson
Subject: Dropbox password reset

Hi there,

Someone recently requested a password change for your Dropbox account. If this was you, you can set a new password here:

Reset password

http://dropbox.magictime.fr/ passwordreset.htm

If you don't want to change your password or didn't request this, just ignore and delete this message.

To keep your account secure, please don't forward this email to anyone. See our Help Center for more security tips.

Thanks!
– The Dropbox Team

© 2015 Dropbox

8.28 | APPENDIX BB: EXAMPLE GENUINE EMAIL

From: npower <npoweronline@npower.com>
Sent: 11 April 2015 13:32
To: Lisa Thompson
Subject: Your bill is available online

Your account number: 156232258

Your statement is now ready to view

To view your statement simply log in to your online account or npower app, then click the Bills & Payments tab.

Log in to view your statement >

http://www.npower.com/login

First time viewing your statement online?
Please register for an online account using your account number 156232258. You'll then be able to log in to view your latest statement.

Avoid an estimated bill. Please provide us with an actual meter reading so we can make sure your account is up to date.

Ways to send your meter reading:

- Online via our website
- npower app for iPhone or Android
- Call us from a landline on - **0800 073 3000**
- Call us from a mobile on - **0330 100 3000**

Lines are open 8am to 8pm Monday to Friday and 8am to 6pm on Saturdays.
Calls may be monitored and recorded for training and security purposes.

Calling us on a 0800 number is normally free when you call from a landline but charges may vary if you use a mobile. Alternatively you can call us on 0330 100 3000 and it will cost you no more than 01 or 02 numbers from landlines or mobiles. If you get 'inclusive minutes' with your package, calls on a 0330 number will be part of these.
Please don't reply to this email
As this is an automated email, it's not managed. If you need more help please visit www.npower.com/customerservices where you'll find information and be able to contact us online or by phone.
There are a number of standards which cover levels of service expected of npower, your local electricity distribution company and your gas transportation company. Please visit www.npower.com/standards to view the latest document detailing the standards and the companies' performance against them.
Remember you can check your latest Terms & Conditions at any time at www.npower.com/terms
Like an overview to help you make the most of your energy supply? The Staying Connected booklets, produced by Consumer Focus, the independent body representing energy consumers, provide impartial advice and guidance. For more details just visit www.npower.com/focus

npower is a registered trademark and the trading name of
Npower Northern Limited (Registered No. 3432100) who also act as an agent for

8.29 | APPENDIX CC. EMAIL SECURITY BEHAVIOUR ITEMS

In the past 7 days, I have..

	Never	Rarely	Sometimes	Most of the Time	Always
...checked the sender's email address before opening attachments	○	○	○	○	○
...looked out for strong emotional tones in emails	○	○	○	○	○
...un-shortened reduced URLS (e.g. tinyURL, bit.ly) within emails before clicking on them	○	○	○	○	○
...checked an email is genuine before clicking on links from within it	○	○	○	○	○
...not clicked on links in suspicious emails	○	○	○	○	○
...checked that the website domain of links within emails is genuine before clicking on them	○	○	○	○	○
...hovered over links in emails to check if they are genuine	○	○	○	○	○
...checked an email is genuine before opening attachments	○	○	○	○	○
...not downloaded attachments in suspicious emails	○	○	○	○	○
...checked the sender's email address before clicking on links from within it	○	○	○	○	○

REFERENCES

Abraham, C., & Sheeran, P. (1994). Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection. Psychology and Health, 9(4), 253–272. http://doi.org/10.1080/08870449408407485

Abraham, C., Sheeran, P., & Johnston, M. (1998). From health beliefs to self-regulation: Theoretical advances in the psychology of action control. Psychology & Health, 13(4), 569–591. http://doi.org/10.1080/08870449808407420

ACMA. (2011). An overview of international cyber-security awareness raising and educational initiatives. Retrieved from http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf

Adams, A., & Sasse, M. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40–46. http://doi.org/10.1145/322796.322806

Adams, A., & Sasse, M. (2001). Privacy in multimedia communications: Protecting users, not just data. In People and Computers XV—Interaction without Frontiers (pp. 49–64). http://doi.org/10.1007/978-1-4471-0353-0_4

Adriaanse, M. a, de Ridder, D. T. D., & de Wit, J. B. F. (2009). Finding the critical cue: implementation intentions to change one's diet work best when tailored to personally relevant reasons for unhealthy eating. Personality and Social Psychology Bulletin, 35(1), 60–71. http://doi.org/10.1177/0146167208325612

Aiken, L., Gerend, M., Jackson, K., & Ranby, K. (2011). Handbook of Health Psychology. (J. Singer, A. Baum, & T. A. Revenson, Eds.)Handbook of Health Psychology (2nd ed.). Routledge. http://doi.org/10.4324/9780203804100

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. http://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. Journal of Applied Social Psychology, 32(4), 665–683. http://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security, 26(4), 276–289. http://doi.org/10.1016/j.cose.2006.11.004

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432–445. http://doi.org/10.1016/j.cose.2009.12.005

Anderson, C. A., & Jennings, D. L. (1980). When experiences of failure promote expectations of success: The impact of attribution failure to ineffective strategies1. Journal of Personality, 48(3), 393–407. http://doi.org/10.1111/j.1467-6494.1980.tb00841.x

Anderson, C., & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioural intentions. MIS Quarterly, 34(3), 613–643.

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. Journal of Applied Psychology, 76(5), 732–740. http://doi.org/10.1037/0021-

9010.76.5.732

Applegate, S. D. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, 18(1), 40–46. http://doi.org/10.1080/19393550802623214

Arachchilage, N., Love, S., & Scott, M. (2012). Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding "Phishing Attacks." International Journal for E-Learning Security, 2(2), 127–132.

Arden, M. A., & Armitage, C. J. (2012). A volitional help sheet to reduce binge drinking in students: A randomized exploratory trial. Alcohol and Alcoholism, 47(2), 156–159. http://doi.org/10.1093/alcalc/agr164

Armitage, C. J. (2006). Evidence that implementation intentions promote transitions between the stages of change. Journal of Consulting and Clinical Psychology, 74(1), 141–151. http://doi.org/10.1037/0022-006X.74.1.141

Armitage, C. J. (2007). Efficacy of a brief worksite intervention to reduce smoking: the roles of behavioral and implementation intentions. Journal of Occupational Health Psychology, 12(4), 376–390. http://doi.org/10.1037/1076-8998.12.4.376

Armitage, C. J. (2008). A volitional help sheet to encourage smoking cessation: a randomized exploratory trial. *Health Psychology: Official Journal of the Division of Health* Psychology, American Psychological Association, 27(5), 557–566. http://doi.org/10.1037/0278-6133.27.5.557

Armitage, C. J., & Arden, M. a. (2010). A volitional help sheet to increase physical activity in people with low socioeconomic status: A randomised exploratory trial. Psychology & Health, 25(10), 1129–1145. http://doi.org/10.1080/08870440903121638

Armitage, C. J., & Arden, M. A. (2008). How useful are the stages of change for targeting interventions? Randomized test of a brief intervention to reduce smoking. Health Psychology, 27(6), 789–798. http://doi.org/http://dx.doi.org/10.1037/0278-6133.27.6.789

Armitage, C. J., & Arden, M. A. (2012). A Volitional Help Sheet to Reduce Alcohol Consumption in the General Population: A Field Experiment. Prevention Science, 13(6), 635–643. http://doi.org/10.1007/s11121-012-0291-4

Armitage, C. J., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A meta-analytic review. British Journal of Social Psychology, 40(4), 471–499. http://doi.org/10.1348/014466601164939

Ashford, S., Edmunds, J., & French, D. P. (2010). What is the best way to change self-efficacy to promote lifestyle and recreational physical activity? A systematic review with meta-analysis. British Journal of Health Psychology, 15(2), 265–288. http://doi.org/10.1348/135910709X461752

Aurigemma, S., & Mattson, T. (2014). Do it OR ELSE ! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies. In AMCIS 2014 (pp. 1–12).

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices : A rational choice perspective. Journal of Organizational and End User Computing, 16(3), 22–40.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191–215. http://doi.org/10.1037//0033-295X.84.2.191

Bandura, A. (1982). Self-efficacy mechanism in human agency. American Psychologist, 37, 122–147.

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

Bandura, A. (1997). Self-efficacy: The Exercise of Control. W.H. Freeman, New York.

Bandura, A., Blanchard, E., & Ritter, B. (1969). Relative efficacy of desensitization and modeling approaches for inducing behavioral, affective, and attitudinal changes. Journal of Personality Social Psychology, 13(3), 173–199. http://doi.org/10.1037/h0028276

Bandura, A., Ross, D., & Ross, S. (1961). Transmission of aggression through imitation of aggressive models. Journal of Abnormal and Social Psychology, 63(3), 575–582. http://doi.org/10.1037/h0045925

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers and Security, 39, 145–159. http://doi.org/10.1016/j.cose.2013.05.006

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, 51(6), 1173–1182. http://doi.org/10.1037//0022-3514.51.6.1173

Barrick, M., & Mount, M. (1991). The Big Five personality dimensions and job performance: A meta-analysis. Personnel Psychology, 44(1), 1–26. http://doi.org/10.1111/j.1744-6570.1991.tb00688.x

Barter, C., & Renold, E. (1999). The use of vignettes in qualitative research. Social Research Update, 25(9), 1–6.

Bartsch, S., & Sasse, A. M. (2012). How Users Bypass Access Control - And Why: The Impact Of Authorization Problems On Individuals And The Organization. In European Conference on Information Systems (pp. 1–12).

Bauer, S., Bernroider, E., & Chudzikowski, K. (2013). End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study. In Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy (pp. 1–16).

Beautement, A., Sasse, M., & Wonham, M. (2009). The compliance budget: managing security behaviour in organisations. In In Proceedings of the 2008 workshop on New security paradigms (pp. 47–58). http://doi.org/10.1145/1595676.1595684

Becker, M. (1974). The Health Belief Model and Sick Role Behavior. Health Education & Behavior, 2(4), 409–419. http://doi.org/10.1177/109019817400200407

Becker, M., & Rosenstock, I. (1987). Comparing social learning theory and the health belief model. In Advances in Health Education and Promotion (pp. 245–9). Greenwich, CT: JAI Press.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 35(4), 1017–1042.

Bell, B. T., Toth, N., Little, L., & Smith, M. A. (2015). Planning to Save the Planet: Using an Online Intervention Based on Implementation Intentions to Change Adolescent Self-Reported Energy-Saving Behavior. Environment and Behavior, 1–24. http://doi.org/10.1177/0013916515583550

Blythe, J. M. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In Proceedings of CHItaly 2013 Doctoral Consortium (pp. 92–101). Retrieved from http://ceur-ws.org/Vol-1065/paper11.pdf

Blythe, J. M., & Coventry, L. (2012). Cyber Security Games: A New Line of Risk. In Entertainment Computing-ICEC 2012 (pp. 600–603). Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-33542-6_80

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 103–122). USENIX Association.

Blythe, M., Petrie, H., & Clark, J. A. (2011). F for Fake : Four Studies on How We Fall for Phish. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 3469–3478). ACM. http://doi.org/10.1145/1979442.1979459

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. Behaviour & Information Technology, 34(10), 1–14. http://doi.org/10.1080/0144929X.2015.1028448

Boer, H., & Seydel, E. (1996). Protection motivation theory. In M. Connor & P. Norman (Eds.), Predicting Health Behavior. Buckingham: Open University Press.

Bommer, W., Johnson, J., Rich, G., Podsakoff, P. M., & MacKenzie, S. B. (1995). On the interchangeability of objective and subjective measures of employee performance: A meta-analysis. Personnel Psyc, 48(3), 587–605. http://doi.org/10.1111/j.1744-6570.1995.tb01772.x

Borman, W., & Motowidlo, S. (1993). Expanding the criterion domain to include elements of contextual performance. In N. Schmitt & W. Borman (Eds.), Personnel Selection in organizations (pp. 71–98). San Francisco, CA: Jossey-Bass. http://doi.org/10.1037/12170-010

Borman, W., & Motowidlo, S. (1997). Task performance and contextual performance: The meaning for personnel selection research. Human Performance, 10(2), 99–109. http://doi.org/10.1207/s15327043hup1002_3

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear ? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Quarterly, 39(4), 837–864.

Bowerman, B., & O'Connell, R. (1990). Linear statistical models: An applied approach. Boston: PWS-kent.

Branley, D., Covey, J., & Hardey, M. (2014). Online Surveys: Investigating Social Media Use and Online Risk. In SAGE Research Methods Cases. SAGE Publications, Ltd. http://doi.org/10.4135/978144627305013514666

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. http://doi.org/10.1191/1478088706qp063oa

Brewster, S. E., Elliott, M. a., & Kelly, S. W. (2015). Evidence that implementation intentions reduce drivers' speeding behavior: Testing a new intervention to change driver behavior. Accident Analysis & Prevention, 74, 229–242. http://doi.org/10.1016/j.aap.2014.11.006

Brown, A. (1998). Organisational Culture (2nd editio). Pitman Publishing.

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641–651. http://doi.org/10.1002/acp.1014

Browne, M. W., & Cudeck, R. (1992). Alternative Ways of Assessing Model Fit. Sociological Methods & Research, 21(2), 230–258. http://doi.org/10.1177/0049124192021002005

Brug, J., & de Vries, H. (1999). Computer-tailored education. Special Issue of Patient Education and Counseling, 36(2), 99–205.

Buchanan, T., Paine, C., & Joinson, A. N. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. Journal of the American Society for Information Science and Technology, 58(2), 157–165.

http://doi.org/http://dx.doi.org/10.1002/asi.20459

Bui, L., Mullan, B., & McCaffery, K. (2013). Protection motivation theory and physical activity in the general population: A systematic literature review. Psychology, Health & Medicine, 18(5), 522–542. http://doi.org/13548506.2012.749354

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. In Computational Science and Engineering, 2009. *CSE'09. International* Conference on Computational Science and Engineering (Vol. 3, pp. 476–481). http://doi.org/10.1109/CSE.2009.484

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548.

Buller, D., & Burgoon, J. (1996). Interpersonal deception theory. Communication Theory, 6(3), 203–242. http://doi.org/10.1111/j.1468-2885.1996.tb00132.x

Burns, S., & Roberts, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. Crime Prevention and Community Safety, 15(1), 48–64. http://doi.org/10.1057/cpcs.2012.13

Cabinet Office. (2011). The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Carpenter, C. (2010). A meta-analysis of the effectiveness of health belief model variables in predicting behavior. Health Communication, 25(8), 661–669. http://doi.org/10.1080/10410236.2010.521906

Cerasoli, C., Nicklin, J., & Ford, M. (2014). Intrinsic motivation and extrinsic incentives jointly predict performance: A 40-year meta-analysis. Psychological Bulletin, 140(4), 1–29. http://doi.org/10.1037/a0035661

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security, 1(3), 18–41. http://doi.org/10.2307/3151312

Chatzisarantis, N. L. D., Hagger, M. S., & Wang, J. C. K. (2010). Evaluating the effects of implementation intention and self-concordance on behaviour. British Journal of Psychology, 101(4), 705–718. http://doi.org/10.1348/000712609X481796

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Computers in Human Behavior, 38, 220–228. http://doi.org/10.1016/j.chb.2014.05.043

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39, 447–459. http://doi.org/10.1016/j.cose.2013.09.009

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In Proceedings of the 42nd Hawaii International Conference on System Sciences (pp. 1–10). IEEE. http://doi.org/10.1109/hicss.2009.74

Chiasson, S., Forget, A., Stobert, E., Van Oorschot, P., & Biddle, R. (2009). Multiple password interference in text and click-based graphical passwords. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 500–511). http://doi.org/10.1145/1653662.1653722

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. Communications of the ACM, 42(2), 60–67. http://doi.org/10.1145/293411.293475

Clegg, S., & Hardy, C. (1999). Studying organization: theory and method. Sage Publications. http://doi.org/10.4135/9781446218556.n19

Computer Security Act. (1987). Advising users on computer systems technology. Retrieved from http://csrc.nist.gov/publications/nistbul/csl92-11.txt

Condly, S., Clark, R., & Stolovitch, H. (2003). The effects of incentives on workplace performance: A meta-analytic review of research studies. Performance Improvement Quarterly, 16(3), 46–63. http://doi.org/10.1111/j.1937-8327.2003.tb00287.x

Conner, M. (2014). Extending not retiring the theory of planned behaviour: a commentary on Sniehotta, Presseau and Araújo-Soares. Health Psychology Review, 9(2), 141–145. http://doi.org/10.1080/17437199.2014.899060

Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of Employee Security Behaviour: A Grounded Theory Approach. In IFIP Advances in Information and Communication Technology (pp. 283–296). Springer International Publishing. http://doi.org/10.1007/978-3-319-18467-8_19

Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. Computers & Education, 59(2), 661–686. http://doi.org/10.1016/j.compedu.2012.03.004

Coventry, L., Briggs, P., Blythe, J. M., & Tran, M. (2014). Using behavioural insights to *improve the public's use of cyber security* best practices. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

Craig, P., Dieppe, P., Macintyre, S., Michie, S., Nazareth, I., & Petticrew, M. (2009). Developing and evaluating complex interventions: an introduction to the new Medical Research Council guidance. In Evidence-based Public Health (Vol. 337, pp. 185–202). Oxford University Press. http://doi.org/10.1093/acprof:oso/9780199563623.003.012

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). Beyond Concern: Understanding Net Users' Attitudes about Online Privacy. In I. Vogelsang & B. M. Compaine (Eds.), Internet Upheaval: Raising Questions (pp. 47–70). Cambridge, MA, USA: MIT Press.

Crossler, R. E. (2010). Protection Motivation Theory : Understanding Determinants to Backing Up Personal Data. In 43rd Hawaii International Conference on System Sciences (pp. 1–10). IEEE. http://doi.org/10.1109/hicss.2010.311

Crossler, R. E., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. ACM SIGMIS Database, 45(4), 51–71. http://doi.org/10.1145/2691517.2691521

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory Bridging the Intention-Behavior Gap. Journal of Information Systems, 28(1), 209–226. http://doi.org/10.2308/isys-50704

Cyberstreetwise. (2015). Cyberstreetwise recommendations. Retrieved April 1, 2015, from https://www.cyberstreetwise.com/

D'Arcy, J., & Devaraj, S. (2012). Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. Decision Sciences, 43(6), 1091–1124. http://doi.org/10.1111/j.1540-5915.2012.00383.x

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of

employees' security compliance. Information Management & Computer Security, 22(5), 474–489. http://doi.org/10.1108/IMCS-08-2013-0057

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems, 20(6), 643–658. http://doi.org/10.1057/ejis.2011.23

D'Arcy, J., & Hovav, A. (2007). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. Journal of Information System Security, 3(2), 3–30.

D'Arcy, J., Hovav, A., & Galletta, D. (2008). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1), 79–98. http://doi.org/10.1287/isre.1070.0160

Dang-pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university : A Protection Motivation Theory approach. Computers & Security, 48, 281–297. http://doi.org/10.1016/j.cose.2014.11.002

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior, 26(6), 1739–1747. http://doi.org/10.1016/j.chb.2010.06.023

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. International Journal of Human-Computer Studies, 72(2), 154–168. http://doi.org/10.1016/j.ijhcs.2013.10.003

Davis, F. D., Bagozzi, R., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: a Comparison of Two Theoretical Models. Management Science, 35(8), 982–1003. http://doi.org/10.1287/mnsc.35.8.982

De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D., & Fischer, M. H. (2002). VIP. In Proceedings of the Working Conference on Advanced Visual Interfaces - *AVI '02* (pp. 316–323). New York, New York, USA: ACM Press. http://doi.org/10.1145/1556262.1556312

de Hoog, N., Stroebe, W., & de Wit, J. B. F. (2007). The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. Review of General Psychology, 11(3), 258–285. http://doi.org/10.1037/1089-2680.11.3.258

De Vet, E., Oenema, A., Sheeran, P., & Brug, J. (2009). Should implementation intentions interventions be implemented in obesity prevention: the impact of if-then plans on daily physical activity in Dutch adults. The International Journal of Behavioral Nutrition and Physical Activity, 6(11), 1–9. http://doi.org/10.1186/1479-5868-6-11

Deci, E., Koestner, R., & Ryan, R. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. Psychological Bulletin, 125(6), 627–668. http://doi.org/10.1037//0033-2909.125.6.627

Deci, E., & Ryan, R. M. (1985). The general causality orientations scale: Self-determination in personality. Journal of Research in Personality, 19(2), 109–134. http://doi.org/10.1016/0092-6566(85)90023-6

Dhamija, R., & Perrig, A. (2000). Déjà Vu: A User Study Using Images for Authentication. In In Proceedings of the 9th USENIX Security Symposium (pp. 45–48).

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems - *CHI '06* (p. 581). New York, New York, USA: ACM Press. http://doi.org/10.1145/1124772.1124861

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. Computers & Security, 20(8), 715–723. http://doi.org/10.1016/S0167-4048(01)00813-6

Dickman, S. J. (1990). Functional and dysfunctional impulsivity: personality and cognitive correlates. Journal of Personality and Social Psychology, 58(1), 95–102. http://doi.org/10.1037/0022-3514.58.1.95

Dillon, A., & Morris, M. (1996). User acceptance of information technology: Theories and models. Annual Review of Information Science and Technology, 31, 3–32.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. Information Systems Journal, 19(4), 391–412. http://doi.org/10.1111/j.1365-2575.2007.00289.x

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information System, 8(7), 386–408.

Dipboye, R. L. (1977). A critical review of Korman's self-consistency theory of work motivation and occupational choice. Organizational Behavior and Human Performance, 18(1), 108–126. http://doi.org/10.1016/0030-5073(77)90021-6

Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: The moving target. Computers & Security, 28(3), 189–198. http://doi.org/10.1016/j.cose.2008.11.007

Dolan, P. (2010). Influencing the financial behaviour of individuals: the mindspace way. In A. Oliver (Ed.), Behavioural Public Policy (pp. 191–215). Cambridge: Cambridge University Press. http://doi.org/10.1017/CBO9781107337190.009

Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. Personal and Ubiquitous Computing, 8(6), 391–401. http://doi.org/10.1007/s00779-004-0308-5

Downs, D. S., & Hausenblas, H. A. (2005). Elicitation studies and the theory of planned behavior: a systematic review of exercise beliefs. Psychology of Sport and Exercise, 6(1), 1–31. http://doi.org/10.1016/j.psychsport.2003.08.001

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit on - eCrime '07 (pp. 37–44). New York, New York, USA: ACM Press. http://doi.org/10.1145/1299015.1299019

Finch, J. (1987). The vignette technique in survey research. Sociology, 21(1), 105–114. http://doi.org/10.1177/0038038587021001008

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesleyle.

Fishbein, M., & Cappella, J. N. (2006). The role of theory in developing effective health communications. Journal of Communication, 56(1), 1–17. http://doi.org/10.1111/j.1460-2466.2006.00280.x

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web (pp. 657–666). http://doi.org/10.1145/1242572.1242661

Florêncio, D., Herley, C., & Oorschot, P. Van. (2014). Password Portfolios and the Finite-Effort User : Sustainably Managing Large Numbers of Accounts. In 23rd USENIX Security Symposium (pp. 575–590).

Floyd, D., Prentice-Dunn, S., & Rogers, R. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407–429.

http://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Ford, K., MaCallum, R., & Tait, M. (1986). The application of exploratory factor analysis in applied psychology: A critical review and analysis. Personnel Psychology, 39(2), 291–314. http://doi.org/10.1111/j.1744-6570.1986.tb00583.x

FTC. (2015). Data Security. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. IEEE Security and Privacy, 10(2), 40–49. http://doi.org/10.1109/MSP.2011.180

Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? Computer Fraud and Security, 2014(5), 12–18. http://doi.org/10.1016/S1361-3723(14)70491-9

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud and Security, 2009(2), 5–10. http://doi.org/10.1016/S1361-3723(09)70019-3

Gandy, O. (1993). The Panoptic Sort: A Political Economy of Personal Information. New York: Westview.

Getsafeonline.org. (2015). Spam & Scam email. Retrieved from https://www.getsafeonline.org/protecting-yourself/spam-and-scam-email/

Gibbs, J. (1975). Crime, punishment, and deterrence. New York: Elsevier.

Gliem, J., & Gliem, R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. In 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education.

Gollwitzer, P. M., & Oettingen, G. (2011). Planning promotes goal striving. Handbook of self-regulation: Research, theory, and applications (Vol. 2). New York: Guilford.

Gollwitzer, P. M., & Sheeran, P. (2006). Implementation Intentions and Goal Achievement: a Meta-Analysis of Effects and Processes. Advances in Experimental Social Psychology, 38, 69–119. http://doi.org/10.1016/s0065-2601(06)38002-1

Goo, J., Yim, M. S., & Kim, D. J. (2013). A path way to successful management of individual intention to security compliance: A role of organizational security climate. In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 2959–2968). http://doi.org/10.1109/HICSS.2013.51

Gov.uk. (2015). 10 Steps: Malware Prevention. Retrieved September 14, 2015, from https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-malware-prevention--11

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. Interacting with Computers, 23(3), 256–267. http://doi.org/10.1016/j.intcom.2011.03.007

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the internet. Group Decision and Negotiation, 13(2), 149–172. http://doi.org/10.1023/B:GRUP.0000021839.04093.5d

Gross, J., & Rosson, M. (2007). Looking for trouble: understanding end-user security management. In In Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology (p. 10). http://doi.org/10.1145/1234772.1234786

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against

spyware: an empirical investigation. Information Management & Computer Security, 17(3), 276–289. http://doi.org/10.1108/09685220910978112

Hackman, J., & Oldham, G. (1976). Motivation through the design of work: Test of a theory. Organizational Behavior and Human Performance, 16(2), 250–279. http://doi.org/10.1016/0030-5073(76)90016-7

Hagger, M. S., Chatzisarantis, N. L. D., & Biddle, S. J. (2002). A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables. Journal of Sport and Exercise Psychology, 24(1), 3–32. Retrieved from http://psycnet.apa.org/psycinfo/2002-12499-001

Hagger, M. S., Lonsdale, A., & Chatzisarantis, N. L. D. (2012). A theory-based intervention to reduce alcohol drinking in excess of guideline limits among undergraduate students. British Journal of Health Psychology, 17(1), 18–43. http://doi.org/10.1111/j.2044-8287.2010.02011.x

Hagger, M. S., & Luszczynska, A. (2014). Implementation intention and action planning interventions in health contexts: State of the research and proposals for the way forward. Applied Psychology: Health and Well-Being, 6(1), 1–47. http://doi.org/10.1111/aphw.12017

Hair, J., Anderson, R., Tatham, R., & Black, W. (2006). Multivariate Data Analysis. (5th, Ed.). Prentice Hall, Upper Saddle River.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. Social Science Research Network Journal. http://doi.org/10.2139/ssrn.2544742

Harrington, S., Anderson, C., & Agarwal, R. (2006). Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions. In Twenty-Seventh International Conference on Information Systems (pp. 1543–1562).

Harris, M., & Schaubroeck, J. (1988). A meta-analysis of self-supervisor, self-peer, and peer-supervisor ratings. Personnel Psychology, 41(1), 43–62. http://doi.org/10.1111/j.1744-6570.1988.tb00631.x

Harris, P. R. (1996). Sufficient grounds for optimism?: The relationship between perceived controllability and optimistic bias. Journal of Social and Clinical Psychology, 15(1), 9–52. http://doi.org/10.1521/jscp.1996.15.1.9

Hasher, L., & Zacks, R. (1979). Automatic and effortful processes in memory. Journal of Experimental Psychology: General, 108(3), 356–388.

Haynes, L., Service, O., Goldacre, B., & Torgerson, D. (2012). Test, Learn, Adapt: Developing Public Policy with Randomised Controlled Trials. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62529/TLA-1906126.pdf

Heckhausen, H., & Gollwitzer, P. (1987). Thought contents and cognitive functioning in motivational versus volitional states of mind. Motivation and Emotion, 11(2), 101–120. http://doi.org/10.1007/bf00992338

Henrich, J., Heine, S. J., & Norenzayan, A. (2010). The weirdest people in the world? Behavioral and Brain Sciences, 33(2-3), 61–83. http://doi.org/10.1017/S0140525X0999152X

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. Information Systems Journal, 24(1), 61–84. http://doi.org/10.1111/j.1365-2575.2012.00420.x

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165. http://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. http://doi.org/10.1057/ejis.2009.6

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. Journal of Management, 21(5), 967–988. http://doi.org/10.1016/0149-2063(95)90050-0

Hinkin, T. R. (1998). A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires. Organizational Research Methods, 1(1), 104–121. http://doi.org/10.1177/109442819800100106

Hodgkins, S., Sheeran, P., & Orbell, S. (1998). Prediction and intention in health-related behaviour: A metaanalytic review of protection motivation theory. Unpublished manuscript. University of Sheffield.

Hoe, S. (2008). Issues and procedures in adopting structural equation modeling technique. Journal of Applied Quantitative Methods, 3(1), 76–83.

Hogg, M. A., & Terry, D. J. (2000). Social identity and self-categorization processes in organizational contexts. Academy of Management Review, 25(1), 121–140. http://doi.org/10.5465/AMR.2000.2791606

Holland, R. W., Aarts, H., & Langendam, D. (2006). Breaking and creating habits on the working floor: A field-experiment on the power of implementation intentions. Journal of Experimental Social Psychology, 42(6), 776–783. http://doi.org/10.1016/j.jesp.2005.11.006

Holloway, A., & Watson, H. E. (2002). Role of self-efficacy and behaviour change. International Journal of Nursing Practice, 8(2), 106–115. http://doi.org/10.1046/j.1440-172x.2002.00352.x

Hu, L., & Bentler, P. (1995). Evaluating model fit. In R. Hoyle (Ed.), Structural equation modeling: Concepts, issues, and applications (pp. 76–99). US: Sage Publication.

Hughes, R. (1998). Considering the vignette technique and its application to a study of drug injecting and HIV risk and safer behaviour. Sociology of Health and Illness, 20(3), 381–400. http://doi.org/10.1111/1467-9566.00107

Hutchinson, S., & Wilson, H. S. (1992). Validity threats in scheduled semistructured research interviews. Nursing Research, 41(2), 117–119. http://doi.org/10.1097/00006199-199203000-00012

ICO. (2014). Data protection research. Retrieved September 1, 2015, from http://ico.org.uk/about_us/research/data_protection

ICO. (2015). Key definitions of the Data Protection Act. Retrieved September 1, 2015, from https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. http://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69–79. http://doi.org/10.1016/j.im.2013.10.001

Inglesant, P., & Sasse, M. (2010). The true cost of unusable password policies: password use in the wild. In In Proceedings of the SIGCHI Conference on Human Factors in Computing

Systems (pp. 383–392). http://doi.org/10.1145/1753326.1753384

Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In 2015 Symposium on Usable Privacy and Security (pp. 327–346). USENIX Association.

Irvine, C., Thompson, M., & Allen, K. (2005). Active Learning with the CyberCIEGE Video Game. In Federal Information *Systems Security Educators' Association Conference* (pp. 1–10).

Jagatic, T. N., Johnson, N. a., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100. http://doi.org/10.1145/1290958.1290968

James, L. a., & James, L. R. (1989). Integrating work environment perceptions: Explorations into the measurement of meaning. Journal of Applied Psychology, 74(5), 739–751. http://doi.org/10.1037/0021-9010.74.5.739

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 1–10. http://doi.org/10.1080/0144929X.2011.632650

Janz, N., & Becker, M. (1984). The Health Belief Model: a decade later. Health Education Quarterly, 11(1), 1–47. http://doi.org/10.1177/109019818401100101

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. Information Technology for Development, 20(2), 196–213. http://doi.org/10.1080/02681102.2013.814040

Jeske, D., Coventry, L., & Briggs, P. (2013). Nudging whom how : IT proficiency, impulse control and secure behaviour. In CHI Workshop on Personalizing Behavior Change Technologies 2014.

Johnson, P. E., Grazioli, S., Jamal, K., & Zualkernan, I. A. (1992). Success and failure in expert reasoning. Organizational Behavior and Human Decision Processes, 53(2), 173–203. http://doi.org/10.1016/0749-5978(92)90061-B

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behavior: An empircal study. MIS Quarterly, 34(3), 549–566.

Johnston, A. C., & Warkentin, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. Mis Quarterly, 39(1), 113–134.

Jones, C. J., Smith, H., & Llewellyn, C. (2014). Evaluating the effectiveness of health belief model interventions in improving adherence: a systematic review. Health Psychology Review, 8(3), 253–269. http://doi.org/10.1080/17437199.2013.802623

Jöreskog, K., & Sörbom, D. (1986). LISREL VI: Analysis of linear structural relationships by maximum likelihood, instrumental variables, and least squares methods, Users guide.

Kaiser, H. F. (1974). An index of factorial simplicity. Psychometrika, 39(1), 31–36. http://doi.org/10.1007/BF02291575

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). " My Data Just Goes Everywhere : " User Mental Models of the Internet and Implications for Privacy and Security. In 2015 Symposium on Usable Privacy and Security (pp. 39–52).

Karakasiliotis, A., Furnell, S., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. In The 7th Australian Information Warfare and Security Conference. Perth, Western Australia.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information

systems (IS) security training approaches. Journal of the Association for Information Systems, 12(8).

Karlsson, F., Astrom, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. Information and Computer Security, 23(3), 2056–4961. http://doi.org/10.1108/ics-05-2014-0033

Kasl, S. V., & Cobb, S. (1966). Health Behavior, Illness Behavior and Sick Role behavior. Archives of Environmental Health: An International Journal, 12(2), 246–266. http://doi.org/10.1080/00039896.1966.10664365

Kearney, W. D., & Kruger, H. A. (2013). Phishing and Organisational Learning. In IFIP Advances in Information and Communication Technology (pp. 379–390). http://doi.org/10.1007/978-3-642-39218-4_28

King, W. W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. Information & Management, 43(6), 740–755. http://doi.org/10.1016/j.im.2006.05.003

Kline, P. (1999). The handbook of psychological testing (2nd ed.). London: Routledge. http://doi.org/10.4324/9781315812274

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24–36. http://doi.org/10.1108/09685220610648355

Korman, A. K. (1970). Toward an hypothesis of work behavior. Journal of Applied Psychology, 54(1), 31–41. http://doi.org/10.1037/h0028656

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597–607. http://doi.org/10.1016/j.im.2003.08.001

Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. Decision Support Systems, 46(1), 254–264. http://doi.org/10.1016/j.dss.2008.06.010

Kumaraguru, P., Acquisti, A., & Cranor, L. F. (2006). Trust modelling for online transactions. In Proceedings of the 2006 International Conference on Privacy, Security and Trust Bridge the Gap Between PST Technologies and Business Services - *PST '06* (p. 1). New York, New York, USA: ACM Press. http://doi.org/10.1145/1501434.1501448

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish : A Real-World Evaluation of Anti-Phishing Training Categories and Subject Descriptors. In Proceedings of the 5th Symposium on Usable Privacy and Security - *SOUPS '09* (p. 12). http://doi.org/10.1145/1572532.1572536

Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security, 18(1), 4–13. http://doi.org/10.1108/09685221011035223

LaRose, R., Rifon, N. J. N., & Enbody, R. (2008). Promoting personal responsibility for internet safety. Communications of the ACM, 51(3), 71–76. http://doi.org/10.1145/1325555.1325569

Lebek, B., Uffen, J., Breitner, M., Neumann, M., & Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. In 2013 46th Hawaii International Conference on System Sciences (pp. 2978–2987). http://doi.org/10.1109/HICSS.2013.192

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, 37(12), 1049–1092. http://doi.org/10.1108/MRR-04-2013-0085

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology, 27(5), 445–454. http://doi.org/10.1080/01449290600879344

Lee, K., & Allen, N. J. (2002). Organizational citizenship behavior and workplace deviance: The role of affect and cognitions. Journal of Applied Psychology, 87(1), 131–142. http://doi.org/10.1037//0021-9010.87.1.131

Lee, Y., & Kozar, K. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. Information & Management, 45(2), 109–119. http://doi.org/10.1016/j.im.2008.01.002

Leventhal, H. (1993). Developmental aspects of health behaviour. In N. Krasnegor, L. Epstein, S. Johnson, & S. Yaffe (Eds.), Developmental aspects of health behaviour. New Jersey: Lawrence Erlbaum Associates.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Systems, 48(4), 635–645. http://doi.org/10.1016/j.dss.2009.12.005

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS Quarterly, 33(1), 71–90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective. Journal of the Association for Information Systems, 11(7), 394–413.

Little, L., Briggs, P., & Coventry, L. (2011). Who knows about me?: an analysis of age-related disclosure preferences. In Proceedings of the 25th BCS Conference (pp. 84–87).

Luszczynska, A., & Schwarzer, R. (2003). Planning and Self-Efficacy in the Adoption and Maintenance of Breast Self-Examination: A Longitudinal Study on Self-Regulatory Cognitions. Psychology & Health, 18(1), 93–108. http://doi.org/10.1080/0887044021000019358

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science, 35(4), 572–585. http://doi.org/10.1007/s11747-006-0003-3

MacKenzie, S. B., Podsakoff, P. M., & Ahearne, M. (1998). Some possible antecedents and consequences of in-role and extra-role salesperson performance. The Journal of Marketing, 62(3), 87–98. http://doi.org/10.2307/1251745

MacKenzie, S. B., Podsakoff, P. M., & Fetter, R. (1991). Organizational citizenship behavior and objective productivity as determinants of managerial evaluations of salespersons' performance. Organizational Behavior and Human Decision Processes, 50(1), 123–150. http://doi.org/10.1016/0749-5978(91)90037-T

Maddux, J. E. (1999). Expectancies and the social–cognitive perspective: Basic principles, processes, and variables. In How expectancies shape experience. (pp. 17–39). Washington: American Psychological Association. http://doi.org/10.1037/10332-001

Maddux, J. E., Brawley, L., & Boykin, A. (1995). Self-efficacy and healthy behavior: Prevention, promotion and detection. In Self-efficacy, adaptation, and adjustment: Theory, research and applpiation (pp. 173–201).

Maddux, J. E., & Lewis, J. (1995). Self-efficacy and adjustment: Basic principles and issues. In J. Maddux (Ed.), Self-efficacy, adaptation, and adjustment: Theory, research, and application (pp. 37–68). New York: Plenum.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems

Research, 15(4), 336–355. http://doi.org/10.1287/isre.1040.0032

Manstead, A. S. R., & Eekelen, S. A. M. (1998). Distinguishing Between Perceived Behavioral Control and Self-Efficacy in the Domain of Academic Achievement Intentions and Behaviors. Journal of Applied Social Psychology, 28(15), 1375–1392. http://doi.org/10.1111/j.1559-1816.1998.tb01682.x

Marsh, H., & Grayson, D. (1995). Latent variable models of multitrait-multimethod data. In R. Hoyle (Ed.), Structural equation modeling: Concepts, issues and applications (pp. 177–198). Thousand Oaks, CA: Sage.

McAfee. (2014). Phishing Deceives the Masses. Retrieved from http://www.mcafee.com/us/resources/reports/rp-phishing-quiz-assessment.pdf?snspd-0115

McBride, M., Carter, L., & Warkentin, M. (2012). The Role of Situational Factors and Personality on Cybersecurity Policy Violation. Retrieved from http://sites.duke.edu/ihss/files/2011/12/CyberSecurityResearchBrief-Final_mcbride-2012.pdf

McCrae, R. R., & Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. Journal of Personality and Social Psychology, 52(1), 81–90. http://doi.org/10.1037//0022-3514.52.1.81

McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J. (2011). Prospective prediction of health-related behaviours with the Theory of Planned Behaviour: a meta-analysis. Health Psychology Review, 5(2), 97–144. http://doi.org/10.1080/17437199.2010.521684

Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. Human Resource Management Review, 1(1), 61–89. http://doi.org/10.1016/1053-4822(91)90011-Z

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, Continuance, and Normative Commitment to the Organization: A Meta-analysis of Antecedents, Correlates, and Consequences. Journal of Vocational Behavior, 61(1), 20–52. http://doi.org/10.1006/jvbe.2001.1842

Michie, S., Dormandy, E., & Marteau, T. M. (2004). Increasing screening uptake amongst those intending to be screened: The use of action plans. Patient Education and Counseling, 55(2), 218–222. http://doi.org/10.1016/j.pec.2003.09.005

Michie, S., Johnston, M., Abraham, C., Lawton, R., Parker, D., & Walker, A. (2005). Making psychological theory useful for implementing evidence based practice: a consensus approach. Quality and Safety in Health Care, 14(1), 26–33.

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implementation Science, 6(1), 42. http://doi.org/10.1186/1748-5908-6-42

Microsoft. (2015). Updating software help. Retrieved from http://www.microsoft.com/security/portal/mmpc/help/updateFAQs.aspx

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: protection motivation theory and implementation intentions. British Journal of Health Psychology, 7(2), 163–184. http://doi.org/10.1348/135910702169420

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health Related Behaviour: A meta-analytic review of Protection Motivation Theory. Journal of Applied Social Psychology, 30(1), 106–143. http://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Mitnick, K. D. (2003). Are you the weak link? Harvard Business Review, 81(4), 18–20.

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element in Security. John Wiley & Sons, Ltd. http://doi.org/0471237124

Montaño, D. E., & Kasprzyk, D. (2008). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In K. Glanz, B. Rimer, & K. Viswanath (Eds.), Health behavior and health education: theory, research, and practice (4th Editio, pp. 67–96). Jossey Bass.

Moon, Y. (2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers. Journal of Consumer Research, 26(4), 323–339. http://doi.org/10.1086/209566

Morrow, P. (1993). The theory and measurement of work commitment. Greenwich, CT: JAI.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. Journal of Service Research, 15(1), 76–98. http://doi.org/10.1177/1094670511424924

Mowday, R. T., Porter, L. W., & Steers, R. M. (1982). Consequences of Employee Commitment, Turnover, and Absenteeism. In Employee–Organization Linkages (pp. 135–168). Elsevier. http://doi.org/10.1016/B978-0-12-509370-5.50010-1

Murphy, C., Coover, D., & Owen, S. (1989). Development and validation of the computer self-efficacy scale. Educational and Psychological Measurement, 49(4), 893–899.

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In Proceedings of the Annual Hawaii International Conference on System Sciences (pp. 3188–3197). http://doi.org/10.1109/HICSS.2014.396

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825. http://doi.org/10.1016/j.dss.2008.11.010

Ng, B.-Y., & Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. In PACIS 2005 Proceedings (pp. 234–247).

Nicholson, J., Coventry, L., & Briggs, P. (2013). Faces and Pictures: Understanding age differences in two types of graphical authentications. International Journal of Human-Computer Studies, 71(10), 958–966. http://doi.org/10.1016/j.ijhcs.2013.07.001

Norman, D. A. (2009). When security gets in the way. Interactions, 16(6), 60–63. http://doi.org/10.1145/1620693.1620708

Onwuegbuzie, A. J., Daniel, L. G., & Collins, K. M. T. (2009). A meta-validation model for assessing the score-validity of student teaching evaluations. Quality & Quantity, 43(2), 197–209. http://doi.org/10.1007/s11135-007-9112-4

Organ, D. (1988). Organizational citizenship behavior: The good soldier syndrome. Lexington, MA: Lexington Books. Retrieved from http://doi.apa.org/psycinfo/1988-97376-000

Ouellette, J. a., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. Psychological Bulletin, 124(1), 54–74. http://doi.org/10.1037/0033-2909.124.1.54

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees'behavior towards is security policy compliance. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (p. 156b–156b). http://doi.org/10.1109/HICSS.2007.206

Paré, G., Sicotte, C., & Jacques, H. (2006). The effects of creating psychological ownership on physicians' acceptance of clinical information systems. Journal of the American Medical Informatics Association, 13(2), 197–205. http://doi.org/10.1197/jamia.m1930

Parker, C., Baltes, B., Young, S., Huff, J., Altmann, R., Lacost, H., & Roberts, J. (2003). Relationship between pscyhological climate perceptions and work outcomes: A meta-analytic review. Journal of Organizational Behavior, 24(4), 389–416. http://doi.org/10.1002/job.198

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. Information Management & Computer Security, 22(4), 334–345. http://doi.org/10.1108/IMCS-10-2013-0078

Peeters, M., Montgomery, A., Bakker, A., & Schaufeli, W. (2005). Balancing Work and Home: How Job and Home Demands Are Related to Burnout. International Journal of Stress Management, 12(1), 43–61. http://doi.org/10.1037/1072-5245.12.1.43

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. MIS Quarterly, 31(4), 623–656.

Petty, R., & Cacioppo, J. (1986). The elaboration likelihood model of persuasion. http://doi.org/10.1007/978-1-4612-4964-1_1

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing, 19(1), 27–41. http://doi.org/10.1509/jppm.19.1.27.16941

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. Review of General Psychology, 7(1), 84–107. http://doi.org/10.1037/1089-2680.7.1.84

Pierce, W., & Cameron, J. (2003). Positive effects of rewards and performance standards on intrinsic motivation. The Psychological Record, 53(4).

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. Justice Quarterly, 13(3), 481–510. http://doi.org/10.1080/07418829600093061

Plotnikoff, R. C., Lippke, S., Trinh, L., Courneya, K. S., Birkett, N., & Sigal, R. J. (2010). Protection motivation theory and the prediction of physical activity among adults with type 1 or type 2 diabetes in a large population sample. British Journal of Health Psychology, 15(3), 643–661. http://doi.org/10.1348/135910709X478826

Podsakoff, N. P., Whiting, S., Podsakoff, P. M., & Blume, B. (2009). Individual-and organizational-level consequences of organizational citizenship behaviors: A meta-analysis. Journal of Applied Psychology, 94(1), 122–141. http://doi.org/10.1037/a0013079

Podsakoff, P. M., & MacKenzie, S. B. (1997). Impact of Organizational Citizenship Behavior on Organizational Performance: A Review and Suggestion for Future Research. Human Performance, 10(2), 133–151. http://doi.org/10.1207/s15327043hup1002_5

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903. http://doi.org/10.1037/0021-9010.88.5.879

Ponemon Institute. (2012). 2012 Cost of Cyber Crime Study: United States. Retrieved from http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6 .pdf

Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Global Analysis. Retrieved from http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

Posey, C., Roberts, T., & Lowry, P. (2011). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. In Proceedings of the Dewald Roode Workshop in Information Systems Security (pp. 1–51).

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., Courtney, J. F., & Behaviors, P. (2010). Insiders' Protection of Organizational Information Assets: A Multidimensional Scaling Study of Protection-Motivated Behaviors. In Proceedings of the Dewald Roode Workshop on IS Security Research (pp. 233–277). Waltham, Massachusetts, USA.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. International Journal of Human-Computer Studies, 71(12), 1133–1143. http://doi.org/10.1016/j.ijhcs.2013.09.002

Prestwich, A., Ayres, K., & Lawton, R. (2008). Crossing two types of implementation intentions with a protection motivation intervention for the reduction of saturated fat intake: A randomized trial. Social Science & Medicine, 67(10), 1550–1558. http://doi.org/10.1016/j.socscimed.2008.07.019

Prochaska, J., & DiClemnte, C. (1983). Stages and processes of self-change in smoking: toward an integrative model of change. Journal of Consulting and Clinical Psychology, 5(3), 390–395. http://doi.org/10.1037/0022-006x.51.3.390

Prochaska, J., Velicer, W., DiClemnte, C., & Fava, J. (1988). Measuring processes of change: applications to the cessation of smoking. Journal of Consulting and Clinical Psychology, 56(4), 520–528. http://doi.org/10.1037/0022-006x.56.4.520

Prochaska, J., Velicer, W., Rossi, J., Goldstein, M., Marcus, B., Rakowski, W., … Rossi, S. (1994). Stages of Change and Decisional Balalance for 12 Problem Behaviors. Health Psychology. http://doi.org/10.1037/0278-6133.13.1.39

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 34(4), 757–778.

PwC. (2012). Bring your own device: Agility through consistent delivery. Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf

PwC. (2015). 2015 Information Security Breaches Survey. Retrieved from http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Renold, E. (2002). Using vignettes in qualiative research. Building Research Capacity, 3, 3–5.

Rhee, H.-S. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816–826. http://doi.org/10.1016/j.cose.2009.05.008

Ritchie, J., & Spencer, L. (2002). Qualitative data analysis for applied policy research. In Analyzing qualitative data (pp. 173–194). Abingdon, UK: Taylor & Francis. http://doi.org/10.4324/9780203413081_chapter_9

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Information Management & Computer Security, 22(4), 393–406. http://doi.org/10.1108/IMCS-11-2013-0083

Rogers, E. (2010). Diffusion of innovations. New York: Free Press.

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 93–114. http://doi.org/10.1080/00223980.1975.9915803

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153–176). New York: Guilford Press.

Rogers, R. (1984). Changing health-related attitudes and behaviors: the role of preventative health psychology. In J. Harvey, J. Maddux, R. McGlynn, & C. Stoltenberg (Eds.), Social Perception in Clinical and Counseling Psychology (vol 2). Lubbock, TX: Texas Tech University Press.

Rosenstock, I., Strecher, V., & Becker, M. (1988). Social learning theory and the health belief model. Health Education & Behavior, 15(2), 175–183. http://doi.org/http://dx.doi.org/10.1177/109019818801500203

Ruiter, R., Kessels, L., Peters, G.-J., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. International Journal of Psychology, 49(2), 63–70. http://doi.org/10.1002/ijop.12042

Ruiter, R., Verplanken, B., Kok, G., & Werrij, M. Q. (2003). The role of coping appraisal in reactions to fear appeals: do we need threat information? Journal of Health Psychology, 8(4), 465–474. http://doi.org/10.1177/13591053030084006

Rutter, D. R., Steadman, L., & Quine, L. (2006). An implementation intentions intervention to increase uptake of mammography. *Annals of Behavioral Medicine : A Publication of the Society of Behavioral Medicine*, 32(2), 127–134. http://doi.org/10.1207/s15324796abm3202_10

Sans. (2015). Glossary of Security Terms - Z. Retrieved from http://www.sans.org/security-resources/glossary-of-terms/?pass=z

Schein, E. (1985). Organisational culture and leadership: A dynamic view (Jossey-Bas). San Francisco.

Schneider, B., Bowen, D., Ehrhart, M., & Holcombe, K. (2000). The climate for service: Evolution of a construct. In Handbook of organizational culture and climate. (pp. 21–36). Thousand Oaks, CA: Sage Publications.

Schneier, B. (2000). Secrets and Lies: Digital Security in a networked world. John Wiley & Sons Inc.

Schwarzer, R. (1992). Self-efficacy in the adoption and maintenance of health behaviors: Theoretical approaches and a new model. In R. Schwarzer (Ed.), Self-efficacy: Thought control of action (pp. 217–243). Washington, DC: Hemisphere.

Searle, A., Vedhara, K., Norman, P., Frost, A., & Harrad, R. (2000). Compliance with eye patching in children and its psychosocial effects: a qualitative application of protection motivation theory. Psychology, Health & Medicine, 5(1), 43–54. http://doi.org/10.1080/135485000105990

Seguin, C. A., & Ambrosio, A. (2002). Multicultural vignettes for teacher preparation. Multicultural Perspectives, 4(4), 10–16. http://doi.org/10.1207/s15327892mcp0404_3

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy & Marketing, 19(1), 62–73. http://doi.org/10.1509/jppm.19.1.62.16949

Sheeran, P. (2002). Intention — Behavior Relations : A Conceptual and Empirical Review. European Review of Social Psychology, 12(1), 1–36. http://doi.org/10.1080/14792772143000003

Sheeran, P., & Silverman, M. (2003). Evaluation of three interventions to promote workplace health and safety: Evidence for the utility of implementation intentions. Social Science and Medicine, 56(10), 2153–2163. http://doi.org/10.1016/S0277-9536(02)00220-4

Sheeran, P., Webb, T. L., & Gollwitzer, P. M. (2005). The interplay between goal intentions and implementation intentions. Personality and Social Psychology Bulletin, 31(1), 87–98. http://doi.org/10.1177/0146167204271308

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. S. (2010). Who falls for phish? In Proceedings of the 28th international conference on Human factors in computing systems - *CHI '10* (p. 373). New York, New York, USA: ACM Press. http://doi.org/10.1145/1753326.1753383

Sheng, S., & Magnien, B. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In Proceedings of SOUPS 2007, 88–99. http://doi.org/10.1145/1280680.1280692

Shepherd, M., Mejias, R., & Klein, G. (2014). A Longitudinal Study to Determine Non-technical Deterrence Effects of Severity and Communication of Internet Use Policy for Reducing Employee Internet Abuse. In 2014 47th Hawaii International Conference on System Sciences (pp. 3159–3168). IEEE. http://doi.org/10.1109/HICSS.2014.392

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior, 48, 199–207. http://doi.org/10.1016/j.chb.2015.01.046

Shropshire, J. D., Warkentin, M., & Johnston, A. C. (2010). Impact of Negative Message Framing on Security Adoption. Journal of Computer Information Systems, 51(1), 41–52.

Shropshire, J. D., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers and Security, 49, 177–191. http://doi.org/10.1016/j.cose.2015.01.002

Sillence, E., Briggs, P., Fishwick, L., & Harris, P. R. (2005). Guidelines for developing trust in health websites. In Special interest tracks and posters of the 14th international conference on World Wide Web WWW 05 (pp. 1026–1027). http://doi.org/10.1145/1062745.1062851

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224. http://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. Computer, 43(2), 64–71. http://doi.org/10.1109/MC.2010.35

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502.

Skår, S., Sniehotta, F. F., Molloy, G. J., Prestwich, A., & Araújo-Soares, V. (2011). Do brief online planning interventions increase physical activity amongst university students? A randomised controlled trial. Psychology & Health, 26(4), 399–417. http://doi.org/10.1080/08870440903456877

Skinner, B. (1938). The behavior of organisms: An experimental analysis. New York, Appleton-Century-Crofts.

Skinner, B., & Ferster, C. (1997). Schedules of reinforcement. Massachusetts: Copley Publishing Group.

Sniehotta, F. F., Presseau, J., & Araújo-Soares, V. (2014). Time to retire the theory of planned behaviour. Health Psychology Review, 8(1), 1–7. http://doi.org/10.1080/17437199.2013.869710

Sniehotta, F. F., Schwarzer, R., Scholz, U., & Schüz, B. (2005). Action planning and coping planning for long-term lifestyle change: Theory and assessment. European Journal of Social Psychology, 35(4), 565–576. http://doi.org/10.1002/ejsp.258

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security, 22(1), 42–75.

http://doi.org/10.1108/IMCS-08-2012-0045

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security, 23(2), 200–217. http://doi.org/10.1108/ics-04-2014-0025

Sophos. (2014). Security Threat Report 2014. Retrieved from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

Sprott, D., Spangenberg, E., & Fisher, R. (2003). The importance of normative beliefs to the self-prophecy effect. Journal of Applied Psychology, 88(3), 423–431. http://doi.org/10.1037/0021-9010.88.3.423

Sriramachandramurthy, R., Balasubramanian, S. K., & Hodis, M. A. (2009). Spyware and adware: how do internet users defend themselves? American Journal of Business, 24(2), 41–52. http://doi.org/10.1108/19355181200900010

Srivastava, A., & Thomson, S. (2009). Framework analysis: a qualitative methodology for applied policy research. Joaag. Retrieved from http://www.joaag.com/uploads/06_Research_Note_Srivastava_and_Thomson_4_2_.pdf

Stanton, J. M., & Mastrangelo, P. R. (2004). Behavioral information security: two end user survey studies of motivation and security practices. In Proceedings of the Tenth Americas Conference on Information Systems (pp. 1–7).

Stanton, J. M., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124–133. http://doi.org/10.1016/j.cose.2004.07.001

Stanton, J. M., Stam, K. R., Guzman, I., & Caledra, C. (2003). Examining the linkage between organizational commitment and information security. In *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483)* (Vol. 3, pp. 2501–2506). IEEE. http://doi.org/10.1109/ICSMC.2003.1244259

Sutton, S. (2001). Back to the drawing board? A review of applications of the transtheoretical model to substance use. Addiction, 96(1), 175–186. http://doi.org/10.1046/j.1360-0443.2001.96117513.x

Symantec. (2014). Malicious links: Spammers change malware delivery tactics. Retrieved from http://www.symantec.com/connect/blogs/malicious-links-spammers-change-malware-delivery-tactics

Symantec Corporation. (2015). 2015 Internet Security Threat Report. Retrieved from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Tari, F., Ozok, A. A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In Proceedings of the second symposium on Usable privacy and security - *SOUPS '06* (p. 56). New York, New York, USA: ACM Press. http://doi.org/10.1145/1143120.1143128

Taylor, D., Bury, M., Campling, N., Carter, S., Garfield, S., Newbould, J., & Rennie, T. (2006). A Review of the use of the Health Belief Model (HBM), the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB) and the Trans-Theoretical Model (TTM) to study and predict health related behaviour change.

Terry, D. (1993). Self-efficacy expectancies and the theory of reasoned action. In D. Terry, C. Gallois, & M. McCamish (Eds.), *The Theory of Reasoned Action: It"s Application to* AIDS-Preventive Behaviour. Oxford, UK: Pergamon. Terry.

Terry, D., & O'Leary, J. E. (1995). The theory of planned behaviour: The effects of perceived

behavioural control and self-efficacy. British Journal of Social Psychology, 34(2), 199–220. http://doi.org/10.1111/j.2044-8309.1995.tb01058.x

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472–484. http://doi.org/10.1016/j.cose.2005.05.002

Thompson, B. (2004). Exploratory and confirmatory factor analysis: Understanding concepts and applications. Washington: American Psychological Association. http://doi.org/10.1037/10694-000

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. Computer Fraud & Security, (10), 7–11. http://doi.org/10.1016/S1361-3723(06)70430-4

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. Information and Software Technology, 52(5), 463–479. http://doi.org/10.1016/j.infsof.2009.11.005

Valentine, T. (1998). An evaluation of the Passface personal authentication system.

van de Laar, K. E., & van der Bijl, J. J. (2001). Strategies enhancing self-efficacy in diabetes education: a review. Scholarly Inquiry for Nursing Practice, 15(3), 235–248.

Vance, A., Eargle, D., Ouimet, K., & Straub, D. (2013). Enhancing password security through interactive fear appeals: A web-based field experiment. Proceedings of the Annual Hawaii International Conference on System Sciences, 2988–2997. http://doi.org/10.1109/HICSS.2013.196

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190–198. http://doi.org/10.1016/j.im.2012.04.002

Vaniea, K. E., Rader, E., & Wash, R. (2014). Betrayed by updates: How negative experiences affect future security. Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14, 2671–2674. http://doi.org/10.1145/2556288.2557275

Velicer, W., Prochaska, J., & Redding, C. (2006). Tailored communications for smoking cessation: past successes and future directions *. Drug and Alcohol Review, 25(1), 49–57. http://doi.org/10.1080/09595230500459511

Vishwanath, A. (2015). Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack. Journal of Computer-Mediated Communication, 20(5), 570–584. http://doi.org/10.1111/jcc4.12126

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586. http://doi.org/10.1016/j.dss.2011.03.002

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. http://doi.org/10.1016/j.cose.2013.04.004

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191–198. http://doi.org/10.1016/j.cose.2004.01.012

Waddell, J. C., McLaughlin, C., LaRose, R., Rifon, N., & Wirth-Hawkins, C. (2014). Promoting Online Safety among Adolescents: Enhancing Coping Self-Efficacy and Protective Behaviors through Enactive Mastery. In Studies in Media and Communications (pp. 133–157). http://doi.org/10.1108/S2050-206020140000008021

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. Journal of Information Privacy & Security, 9(4), 52–79. http://doi.org/10.1080/15536548.2013.10845690

Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). An Exploration of the Design Features of Phishing Attacks. In R. Rao & S. Upadhyaya (Eds.), Handbooks in Information Systems (Vol. 4).

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. IEEE Transactions on Professional Communication, 55(4), 345–362. http://doi.org/10.1109/TPC.2012.2208392

Wash, R., Rader, E., Vaniea, K., & Rizor, M. (2014). Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences. In Proc. 10th Symposium on Usable Privacy and Security (SOUPS) (pp. 89–104).

Wason, K., Polonsky, M., & Hyman, M. (2002). Designing vignette studies in marketing. Australasian Marketing Journal (AMJ), 10(3), 41–58. http://doi.org/10.1016/s1441-3582(02)70157-2

Webb, T. L., & Sheeran, P. (2004). Identifying good opportunities to act: Implementation intentions and cue discrimination. European Journal of Social Psychology, 34(4), 407–419. http://doi.org/10.1002/ejsp.205

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. Psychological Bulletin, 132(2), 249–268. http://doi.org/10.1037/0033-2909.132.2.249

Weible, R. (1993). Privacy and data: an empirical study of the influence of types of data and situational context upon privacy perceptions. Mississippi State University.

Weinstein, N. D. (1980). Unrealistic optimism about future life events. Journal of Personality and Social Psychology, 39(5), 806–820. http://doi.org/10.1037//0022-3514.39.5.806

Weinstein, N. D. (2000). Perceived probability, perceived severity, and health-protective behavior. Health Psychology : Official Journal of the Division of Health Psychology, American Psychological Association, 19(1), 65–74. http://doi.org/10.1037/0278-6133.19.1.65

Weinstein, N. D., Rothman, a J., & Sutton, S. R. (1998). Stage theories of health behavior: conceptual and methodological issues. Health Psychology : Official Journal of the Division of Health Psychology, American Psychological Association, 17(3), 290–9. http://doi.org/10.1037//0278-6133.17.3.290

Weinstein, N. D., & Sandman, P. M. (1992). A model of the precaution adoption process: Evidence from home radon testing. Health Psychology, 11(3), 170–180. http://doi.org/10.1037//0278-6133.11.3.170

West, R. (2008). The psychology of security. Communications of the ACM, 51(4), 34–40. http://doi.org/10.1145/1330311.1330320

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. International Journal of Information Management, 24(1), 43–57. http://doi.org/10.1016/j.ijinfomgt.2003.12.003

Whitten, A., & Tygar, J. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63(1-2), 102–127. http://doi.org/10.1016/j.ijhcs.2005.04.010

Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J.-C. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces - *AVI '06* (p. 177). New York, New York, USA: ACM Press. http://doi.org/10.1145/1133265.1133303

Williams, D. M., Anderson, E. S., & Winett, R. A. (2005). A review of the outcome expectancy construct in physical activity research. Annals of Behavioral Medicine, 29(1), 70–79. http://doi.org/10.1207/s15324796abm2901_10

Williams, L. J. (1991). Job Satisfaction and Organizational Commitment as Predictors of Organizational Citizenship and In-Role Behaviors. Journal of Management, 17(3), 601–617. http://doi.org/10.1177/014920639101700305

Wirth, C., Rifon, N., LaRose, R., & Lewis, M. (2007). Promoting teenage online safety with an i-safety intervention: enhancing self-efficacy and protective behaviors. In Annual Meeting of the International Communication Association: Montreal, Quebec, Canada. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.9763&rep=rep1&type=pdf

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communications Monographs, 59(4), 329–349. http://doi.org/10.1080/03637759209376276

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. Health Education & Behavior, 27(5), 591-615. http://doi.org/10.1177/109019810002700506

Witte, K., Cmaeron, K., McKeon, J., & Berkowitz, J. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. Journal of Health Communication, 4(1), 317–341. http://doi.org/10.1080/108107396127988

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. In Proceedings of the Twenty--Sixth International Conference on Information Systems (pp. 367–380).

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799–2816. http://doi.org/10.1016/j.chb.2008.04.005

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. Cyber*psychology & Behavior : The Impact of the Internet, Multimedia and Virtual Reality* on Behavior and Society, 11(5), 615–7. http://doi.org/10.1089/cpb.2007.0208

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330–340. http://doi.org/10.1108/09685220910993980

Zhang, L., & McDowell, W. C. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. Journal of Internet Commerce, 8(3-4), 180–197. http://doi.org/10.1080/15332860903467508

Zimmerman, R., & Vernberg, D. (1994). Models of Preventive Health Behavior: Comparison, Critique, and Meta-Analysis. Advances in Medical Sociology, 4, 45–67.

Zonealarm. (2013). USB Drives: Are You Plugging Malware into Your PC? Retrieved from http://www.zonealarm.com/blog/2013/11/usb-drives-are-you-plugging-malware-into-your-pc/

Zviran, M., & Haga, W. (1999). Password security: an empirical study. Journal of Management Information Systems, 15(4), 161–185.