The socio-organisational factors that shape guardianship experience of information security management in organisations

A thesis submitted for the degree of Doctor of Philosophy

by

Jason Johnstone

School of Social and Health Sciences,
Abertay University.

January, 2020

Declaration

Candidate's declarations:

I, Jason Johnstone, hereby certify that this thesis submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy (PhD), Abertay University, is wholly my own work unless otherwise referenced or acknowledged. This work has not been submitted for any other qualification at any other academic institution.

Signed…..*Jason Johnstone……*

Date………30/06/2019……..

Supervisor's declaration:

I, Dr Stefano de Paoli hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy (PhD) in Abertay University and that the candidate is qualified to submit this thesis in application for that degree.

Signed …………*Stefano de Paoli*…...

Date………30/06/2019…………..

Certificate of Approval

I certify that this is a true and accurate version of the thesis approved by the examiners, and that all relevant ordinance regulations have been fulfilled.

Supervisor……*Stefano de Paoli*……………….

Date……………30/06/19…………………

Acknowledgements

The completion of this PhD thesis would not have been possible without the help and support of all my supervisors, Dr Stefano de Paoli, Dr Natalie Coull, and Dr Ian Ferguson. Dr Stefano de Paoli in particular, as my principal supervisor, has been nothing short of outstanding during the last 5 years. His support and unwavering patience proved an invaluable asset and I consider it an absolute privilege to have been under his guidance.

I would also like to thank Abertay University. I have now been at Abertay University for 10 years. As a student who struggled immensely throughout primary and secondary education due to learning issues, my life completely changed when I secured a place at Abertay University as a mature student. Over the next decade, all the staff members at Abertay University have supported me in becoming a fully-fledged researcher and I am proud to represent Abertay University.

I would also like to thank all my friends and family who have supported me throughout the duration of my PhD and I also wish to thank those who took part in this study; without their participation none of this would have been possible.

Again, to all those mentioned above, I am forever indebted to you. Thank you.

Abstract

To become more effective and efficient organisations are increasing their utilisation of information and information systems, which has made them more vulnerable to various kinds of attacks from cybercriminals; a major consequence of which are security breaches. Further, despite previous studies showing insecure behaviour as a major cause, information security if often viewed as a technical problem only, where socio-organisational factors are often overlooked. Therefore, the primary aim of this qualitative research is to investigate how socio-organisational factors influence security behaviour in organisations and to describe the experiences of guardians of information security management. In this context, guardians are defined as those actors who are responsible for protecting information in organisations. In total there were 86 in-depth interviews conducted with three groups of guardians: *security managers*, who experience guardianship by managing an organisation's information security; end users, who experience guardianship by using an organisation's security controls; and security testers, who experience guardianship by testing the level of information security in organisations via the practice of security testing. The emergent findings showed that the willingness and capability of end users towards protecting information in organisations was influenced by numerous socio-organisational factors connecting to: (1) the security behaviour of upper management; (2) the effective development and implementation of security policies; (3) the effective development and implementation of SETA programmes; (4) the effective use of monitoring and enforcement practices; and (5) the usability of technical security controls. In addition, the effectiveness of security managers towards managing end user security behaviour was influenced by upper management support for information security. Lastly, the findings showed that security testing comprised numerous sequential stages, which can be mapped using the universal crime script; where the goals and objectives for each stage, as well the required use of tools and tactics used by different security testers, were successfully mapped.

Table of Contents

List of Figures

1 Introduction

1.1 Background

To become more effective and efficient both public and private organisations are increasing their utilisation of information and information systems. Unfortunately, such advancements have simultaneously made organisations more vulnerable to various kinds of attack from cybercriminals. Thus, with increasing reliance upon information and information systems, managing information security has become a major concern for organisations. It should be highlighted, however, that defending organisations against cybercriminal attacks is not the only reason an organisation should exercise good information security. For example, should information be accidently deleted or disclosed to unauthorised persons, then that information would no longer be available to the organisation or its confidentiality compromised. Nevertheless, the focus of this paper will be on organisational efforts to defend against attacks from cybercriminals.

Arguably one of the greatest challenges in information security management is preventing security breaches. Schatz and Bashroush (2015, p. 2) defined a security breach as "a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed". The negative consequences of security breaches are numerous, including, but not limited to:

- *Operational costs*: The costs to the effectiveness and efficiency of the day-to-day operations and functioning of an organisation (Spanos and Angelis, 2016; Sutton, 2016).
- *Incident investigation*: The costs incurred for investigating a security breach, including forensic and consulting services (Caldwell, 2014; Dlamini et al, 2009).
- *Crisis management*: The costs incurred for managing a security breach such as hiring PR consultants and informing customers that information has been lost or stolen. This also includes credit monitoring and the reissuing of cards if necessary (Caldwell, 2014; Sutton, 2016).

- *Legal and regulatory sanctions*: The costs incurred from any fines and sanctions that may be imposed by legal and/or regulatory bodies (Caldwell, 2014; Dlamini et al, 2009).
- *Opportunity costs*: The costs incurred through loss of business because of reputational damage, such as changes in customer purchasing and failure to secure potential business with other organisations (Berezin et al, 2012; Dlamini et al, 2009).

In response to such potentially devastating consequences, security researchers and practitioners have argued we must drastically improve the protection of information in organisations (Chang and Lin, 2007; Furnell and Clarke, 2012). Indeed, studies suggest that the information security market is rapidly growing (Posey et al, 2014) and organisations are reportedly increasing their overall spending on information security, with worldwide spending forecasted to reach $124bn (approx. £98bn) in 2019 (Gartner Inc., 2018).

Importantly however, increased spending on information security will not guarantee that information is adequately protected in organisations. A major challenge of previous years (both for research and practice) was information security is often viewed as a technical problem, where many organisations tried to manage information security largely through purchasing and implementing technical security controls (Kayworth and Whitten, 2010; Metalidou et al, 2014). While technology is undoubtedly important and helps to address various security risks, security experts have argued technology alone will not properly address the problem of security breaches (Ifinedo, 2014; Soomro et al, 2016; Willison and Backhouse, 2006).

For example, previous studies have shown that a major cause for security breaches are the insecure behaviours of end users (often referred to as ‘the insider threat’), whose actions or inactions reduces the level of protection of information in organisations (Ifinedo, 2014). Therefore, security researchers and practitioners have argued in order to properly address the problem of security breaches we must understand how various socio-organisational factors (often referred to as ‘human factors’) influence security behaviour in organisations alongside technical factors (Furnell and Clarke, 2012; Werlinger et al, 2009).

Yet, despite this acknowledgement, research into socio-organisational factors of information security management is currently lacking. Furthermore, previous research has tended to be quantitative, where security researchers have utilised models, theories, and concepts drawn from computer-science related disciplines (Stahl et al, 2012; Bauer et al, 2017; Alshaikh et al, 2018). Hence, Posey et al (2014, p. 551) have argued "to understand the effects of user behavior on information security, researchers and practitioners must incorporate behavioral frameworks from disciplines outside of computer science and electrical engineering that examine human perceptions, beliefs, motivations, and behaviors".

Therefore, the present study seeks to contribute towards addressing the problem of security breaches in organisations through conducting a phenomenology-inspired investigation into the socio-organisational factors that influence the managing of information security in organisations. This study is concerned with the problem of understanding how socio-organisational factors influence security behaviour in organisations to help improve the protection of information and help to prevent or reduce the likelihood of security breaches. This study draws upon two dominant theories within criminology – the Routine Activity Approach and the Rational Choice Perspective – to investigate the experiences of three groups of social actors referred to as *guardians*. Guardians are those members of an organisation who have the protection of information as part of their job role (a full discussion of guardianship will be presented in chapter 3). Their experiences of the following six areas of information security management will be investigated: (1) upper management support, (2) information security policies, (3) security education, training, and awareness (SETA) programmes, (4) monitoring and enforcement practices, (5) usability of technical security controls, and (6) security testing.

1.2 Research Aims and Objectives

The primary aim of this research is to investigate how socio-organisational factors influence the level of protection of information in organisations and to describe the experiences of three groups of guardians towards information security management in organisations. The concept of guardianship connects with the Routine Activity Approach in criminology which states *crime events* are comprised of: (1) a likely offender, (2) a suitable target, and (3) the absence of capable guardians. Therefore, the primary aim of this research is to understand how socio-organisational factors shape the experiences of guardians of information security management to help improve the level of guardianship of information in organisations, which may in turn help organisations better manage information security and prevent security breaches.

The following are the three main research objectives for the present study:

- To identify, present, and discuss the socio-organisational factors of information security management which may influence security behaviour in organisations.
- To further develop the concept of guardianship and to describe the experiences of guardians of protecting information in organisations.
- To investigate how socio-organisational factors shape the experiences of guardians of protecting information in organisations.

1.3 Research Questions

The main research question for this study is:

- RQ: How do socio-organisational factors shape guardianship experience of protecting information in organisations?

As mentioned, this study includes three groups of guardians who experience information security management. Therefore, there are three sets of sub research questions that will be asked in this study.

The first group of guardians are *security managers*, who experience guardianship by managing an organisation's information security (e.g., through the development and implementation of security controls). Therefore, the following sub research questions relating to security managers are:

- SRQ1: What are security managers’ experiences of managing information security in organisations?
- SRQ2: How do socio-organisational factors shape security managers experiences of managing information security in organisations?

The second group of guardians are *end users*, who experience guardianship by using an organisation’s security controls (e.g., using technical security controls, reading security policies, completing security education, training, and awareness programmes, and having their security behaviour monitored and enforced). Therefore, the following sub research questions relating to end users are:

- SRQ3: What are end user’s experiences of security controls in organisations?
- SRQ4: How do socio-organisational factors shape their experiences of security controls in organisations?

The third group of guardians are *security testers*, who experience guardianship by testing an organisation’s information security (e.g., through conducting network-based and physical-based penetration testing). Therefore, the following sub research questions relating to security testers are:

- SRQ5: What are security testers’ experiences of security testing in organisations?
- SRQ6: How do socio-organisational factors shape their experiences of security testing?

1.4 Thesis Structure

This thesis is structured into 9 chapters. The remaining chapters are structured as follows. *Chapter 2* provides an extensive review of previous research into various socio-organisational factors which influence the security behaviour of end users in organisations. In addition, there will be a review of previous research on the practice of network-based and physical-based penetration testing. *Chapter 3* outlines the theoretical framework for this study. The theoretical framework was developed in accordance with the Routine Activity Approach and the Rational Choice Perspective. Therefore, both theories will be presented and discussed, including how each have been incorporated for use in this study. *Chapter 4* provides an overview of the methodology and research methods used in this study. This includes a discussion of research paradigm, research strategy, research design, sampling design, and data collection and analysis. *Chapter 5* presents the findings from interviews with security managers about their experiences of information security management. *Chapter 6* presents the findings from interviews with end users about their experiences of information security management. *Chapter 7* presents the findings from interviews with security testers about their experiences of information security management. *Chapter 8* provides a critical discussion and synthesis of the findings with previous studies to answer the research question. Finally, *Chapter 9* provides a conclusion to the study and highlights research contributions, implications for theory, the limitations of this study, and future research.

2 Literature Review

2.1 Introduction

This chapter presents a critical review of the literature in numerous areas of information security management. The chapter begins by discussing what information security management involves and introduces the notion of the insider threat to organisations, namely the insecure behaviour of end users. Following this, five areas of the literature relating to end user security behaviour will be discussed, including: (1) upper management support, (2) information security policies, (3) security education, training, and awareness (SETA) programmes, (4) monitoring and enforcement practices, and (5) usability of technical security controls. The chapter then closes with a discussion of the practice of security testing and how this may help organisations better understand how to protect information against attacks from cybercriminals.

2.2 Information security management

Information security management is generally described as protecting organisational information against unauthorised access, usage, disclosure, modification, disruption, and/or destruction to achieve the security goals of confidentiality, integrity, and availability (Rhodes-Ousley, 2014; Sutton, 2016; Taylor et al, 2013). For example, Sutton (2016, p. 7) argued the information assets of organisations “must be kept confidential, so that only authorised people may have access to them; their integrity must be protected, so that only authorised people may change them; and they must be available when required by those who have a need to access them”.

To achieve confidentiality, integrity, and availability of information, organisations primarily develop and implement various security controls (von Solms and Niekerk, 2013). Security controls are generally categorised into technical (or logical), physical, and administrative security controls. Technical controls refer to the hardware and software features that protect information. Examples include firewalls, intrusion detection/prevention systems, access lists, and encryption. Physical controls refer to the means and devices used to control physical access to information. Examples include perimeter fencing, security guards, secure entry, and closed-circuit television

(CCTV). Lastly, administrative security controls refer to the controls used to directly manage the security behaviour of employees. Examples include information security policies, security education, training, and awareness (SETA) programmes, and incident management/recovery (Keung, 2013; Rhodes-Ousley, 2014; Wright, 1994).

As explained in the introduction chapter, due to information security management involving both technical and non-technical aspects, security experts have argued organisations must ensure to develop and implement security controls from all three categories rather than focusing on one category (Ashenden, 2008; Chang and Ho, 2006; Furnell and Clarke, 2012; Soomro, Shah, and Ahmed, 2016; Werlinger et al, 2009). Otherwise organisations will not fully protect information against cybercriminal attacks. For example, Ashenden (2008) argued failure to be properly managed information security (i.e., consider both technical and non-technical aspects) may result in organisations overlooking certain security controls and/or selecting incorrect security controls for development and implementation, which wastes organisational resources and leaves information vulnerable to attack.

To ensure security controls are properly selected, security experts recommend organisations utilise an *information security strategy* to guide information security management activities (Beebe and Rao, 2010; Blakey et al, 2001; Taylor et al, 2013). Beebe and Rao (2010) argued the *risk management approach* to be one of the most successful and widely used information security strategies used by organisations to help manage information security. They described the risk management approach as comprising the following stages: (1) the identification and evaluation of organisational information assets; (2) the identification of any threats to, and vulnerabilities of, information assets; (3) the completion of risk analysis to determine the levels of risk to information assets; and (4) the selection of appropriate security controls to mitigate the identified risks. Importantly, Beebe and Rao (2010, p. 331) stated the “decisions surrounding which risks to mitigate, to what extent, what types of countermeasures to employ, and at what cost, are strategic in nature. This collective set of decisions constitutes the strategy”.

Of initial relevance here is stage 2, the process of identifying threats to information assets, as this will impact the later stages of the risk management approach, namely risk analysis and the selection of appropriate security controls (Beebe and Rao, 2010; Rhodes-Ousley, 2014). Thus, the next section introduces and briefly discusses internal threats to information in organisations.

2.2.1 Internal threats to information in organisations

In information security management, threats are divided into two main sources: human and non-human threats (such as earthquakes and other 'acts of God'). This study will only discuss human threats to organisations. Further, human threats (also referred to as threat actors) can be divided into external and internal threats (Hashem et al, 2015; Cheng et al, 2017). Of obvious relevance here are internal threats to organisations.

When discussing internal threats to organisations, previous studies generally use the terms *insider* or *insider threat*. An insider is generally described as an employee (past or present) that has privileged access to an organisation's information (Predd et al, 2008; Nurse et al, 2014). Importantly, the use of the terms insider and insider threat do not denote malicious activity conducted by an employee against an organisation. Security researchers typically distinguish between two main types of insiders. The first type is the *malicious insider*, where the insider uses their privileged access to intentionally cause a negative impact against the confidentiality, integrity, and/or availability of organisational information. It is understood that a malicious insider will seek to exploit their privileged access for some inappropriate gain, whether it be money related or for purposes of revenge and so on (Hashem, 2015; Nurse et al, 2014).

The second type is the *non-malicious insider*, who through action or inaction causes harm or increases the chances of future harm to the confidentiality, integrity, and/or availability of organisational information (Nurse et al, 2014). In this study, only non-malicious insiders will be discussed, malicious insiders will not be discussed. The focus toward non-malicious insiders (i.e., end users) is because they are often described as the weakest link in information security management, where their insecure behaviour puts organisations and information at increased risk from malicious external and internal threats actors (Abawajy, 2014; Bunker, 2012; Furnell and Clarke, 2012; Orshesky, 2003). For example, Abawajy (2014) posited a large proportion of security breaches originate from inside organisations due to the insecure behaviour of end users, such as writing down and sharing passwords and/or opening unknown e-mails and attachments. These behaviours potentially expose organisations to deliberate attacks from threat actors such as malicious hackers and jeopardise the level of security surrounding information in organisations.

Therefore, the next several sections of this chapter will explore the security behaviour of end users and the different areas of information security management which may influence whether they behave securely in organisations and ultimately keep information safe.

Following extensive reading of the relevant literature in information security management, there emerged a total of five areas that were considered important relating to information security management and the managing of end user security behaviour. In other words, five areas were identified during the reading of the relevant literature which were deemed the most important areas connected to the security behaviour of end users in organisations, and therefore will form the basis of the main areas of interest in the current paper. The main focus areas identified were: (1) upper management support, (2) information security policies, (3) security education, training, and awareness (SETA) programmes, (4) monitoring and enforcement practices, and (5) usability of technical security controls. Each of these areas will now be presented and critically discussed.

2.3 Upper management support in information security management

Within information security management literature, upper management support is often described as one of the most important factors when managing information security in organisations (Ashenden, 2008; Choi et al, 2008; Hu et al, 2012; Kajava et al, 2006; Kankanhalli et al, 2003; Leach, 2003; Merhi and Ahluwalia, 2015; Puhakainen and Siponen, 2010; Siponen et al, 2007; von Solms and von Solms, 2004b). Following an analysis of the literature, there were two main reasons for this: (1) upper management influence the amount of organisational resources that are allocated to security managers for the managing of information security (Ashenden, 2008; Choi et al, 2008; Gaunt, 2000; Kankanhalli et al, 2003; Knapp et al, 2006a; Merhi and Ahluwalia, 2016; Willison and Backhouse, 2006); and (2) the expectations and observed behaviour of upper management influences the security behaviour of end users (Bulgurcu et al, 2010; Hu et al, 2012; Pahnila et al, 2007; Siponen et al, 2014). Therefore, both aspects of upper management support in information security management will now be critically discussed.

2.3.1 Allocation of organisational resources for information security management

Although not directly relating to the security behaviour of end users, it is argued in this study that proper allocation of organisational resources to security managers for the development and implementation of security controls is an important factor when determining the reasons why end users might behave insecurely. For example, if security managers do not have enough organisational resources, then this will greatly impact their ability to develop and implement effective security controls, which includes those security controls purposefully designed to manage end user security behaviour – hence, the increased likelihood for insecure behaviour of end users.

Indeed, many security researchers and practitioners have claimed that one of the ways upper management influence security behaviour in organisations is through the allocation of organisational resources to ensure the proper development and implementation of security controls (Gaunt, 2000; Kankanhalli et al, 2003; Kajava et al, 2006; Knapp et al, 2006a; Merhi and Ahluwalia, 2016; Wood, 1997). For example, Kajava et al (2006, p. 1520) argued "The key component of information security work is the visible support and engagement of senior management. In practical terms, this commitment involves allocating necessary funding to information security work".

Similarly, Kankanhalli et al (2003) investigated various security efforts in small and medium-sized organisations. They argued organisations which have support from upper management were more likely to have financial and technical resources made available for managing information security. Their findings showed that upper management support had a positive influence on the overall levels of ‘preventative efforts’ within organisations.

However, despite the acknowledgement from security experts that upper management support is essential towards ensuring enough organisational resources are allocated, there is some evidence to suggest that many security managers do not receive their support. For example, Knapp et al (2006a) reported that in two surveys where *Certified Information System Security Professionals* (CISSPs) ranked a list of 25 ‘critical information security issues’, the top-ranked issue in both surveys was gaining upper management support for information security management. Some of the responses they received in the surveys included:

- “Management frequently does little but pay lip service to security; it is viewed as a cost and a hindrance, not a critical business component.” (*quoted in* Knapp et al, 2006a, p. 52)
- “Top management is not serious about security; otherwise they would commit the funds necessary to accomplish real results.” (*quoted in* Knapp et al, 2006a, p. 52)

Thus, Knapp et al (2006a, p. 57) concluded that “Perhaps an organization’s overall security health can be accurately predicted by asking a single question: Does top management consider security important?”

According to Kankanhalli et al (2003), upper management support towards information security may be lacking because (a) upper management think security risks towards information are low, (b) upper management do not understand the value of developing and implementing certain security controls due to the difficulty in evaluating the benefits, and (c) upper management may lack understanding about the range of security controls available to protect information (especially non-technical security controls).

Werlinger et al (2009) similarly argued a lack of upper management support may be caused by the perceived high costs of developing and implementing security controls and a lack of understanding of the consequences of failing to protect information.

Overall, it appears that despite upper management support being recognised by some as an important factor in information security management, there is some evidence to suggest that upper management are failing to provide their support to security managers. Importantly, the studies described above are few and somewhat dated, therefore further investigation into this area of upper management support is much needed. Moreover, having more of an understanding as to the reasons why upper management might fail to provide their support would also be very helpful to security managers when trying to improve the levels of support from upper management.

Therefore, this study significantly contributes towards addressing the problem of upper management support by looking at the ways in which upper management influence the level of organisational resources allocated to security managers, and the possible reasons behind their failure to provide their support (should this be the case).

2.3.2 Influencing social norms towards protecting information

In addition to making sure enough organisational resources are allocated to security managers for developing and implementing security controls, many security researchers have described upper management support as an important factor because the expectations and observed behaviour of upper management influences the security behaviour of end users (Bulgurcu et al, 2010; Hu et al, 2012; Pahnila et al, 2007; Siponen et al, 2014).

Most studies that have investigated this aspect of upper management support have utilised the concept *social norms* (also referred to as subjective norms, normative beliefs, or social pressures) to better understand how the security behaviour of upper management influences that of end users. According to Herath and Rao (2009a, p. 158), social norms are “the belief as to whether or not a significant person wants the individual to perform the behavior in question … the individual's behavior is influenced by what the relevant others expect her/him to do”. Further, individuals are described as influenced by both messages about expectations as well as the observed behaviour of the significant person.

In the context of information security management, this suggests that if end users believe that significant persons, such as peers, immediate supervisors, security managers, and upper management, expect end users to behave securely and demonstrate good security behaviour, then end users are more likely to behave securely themselves (Hu et al, 2012).

It is important to note, while there have been numerous studies which have supported the idea that social norms influence end user security behaviour, most have only investigated how the expectations of peers, immediate supervisors, and security managers influence end user security behaviour, and therefore have tended to exclude the expectations of upper management (e.g., Cox, 2012; Dinev and Hu, 2007; Hazari et al, 2008; Ifinedo, 2012; 2014; Safa et al, 2015). Consequently, there were fewer studies to review which have looked at whether upper management behaviour can likewise influence social norms; which highlights the importance of improving our understanding in this area. Nevertheless, those studies which included upper management behaviour produced some interesting findings that are worth discussing.

For example, Pahnila et al (2007) found that the expectations of upper management (what they termed ‘social pressures’) towards end users complying with security policies of organisations (which outline security behaviours end users must perform to keep information safe), influenced the overall intentions of end users’ to comply. Thus, Pahnila et al concluded that security practitioners should attempt to utilise the fact that social pressures from upper management towards security policy compliance may help improve compliance rates, and ultimately the protection of information in organisations.

Hu et al (2012) similarly investigated whether upper management influenced end user intentions to comply with security policies. They argued various cognitive beliefs of end users, such as attitudes and normative beliefs (i.e., social norms) are influenced by the observed behaviour of upper management. Their findings showed upper management significantly influenced the cognitive beliefs of end users towards information security and their intentions to comply with security policies.

Importantly, while some studies have supported the influence of upper management behaviour towards that of end users, there are some mixed findings in this area, where some studies have argued against any positive influence from upper management (Herath and Rao, 2009b). For example, Herath and Rao (2009b) found that while expectations from peers and immediate supervisors did influence end user security behaviour, those relating to upper management did not. Interestingly, Herath and Rao did highlight that this may have been caused by end users in their study not being aware of upper management's expectations towards information security.

Consequently, there is still some debate about whether the expectations and observed behaviour of upper management can indeed positively influence the behaviour of end users alongside those of peers, immediate supervisors, and security managers. Part of the problem surrounding this debate is a lack of research on upper management behaviour. As mentioned, much of the studies which have investigated the influence of social norms in information security management have only in recent years begun to include the expectations and observed behaviour of upper management.

In addition, while some studies have shown that if end users consider upper management to take security seriously they too are more likely to take it seriously, they have not yet properly investigated how end users come to learn upper management's expectations towards security behaviour. Indeed, one of the major studies conducted in this area by Hu et al (2012, p. 648) acknowledged that "the nature and effectiveness of communication from top management to employees was not examined". Therefore, they recommended future studies investigate the "different styles and channels of communication used by top management in shaping employee beliefs … and ultimately changing the level of compliance towards information security policies".

Lastly, most of previous studies which have investigated upper management support have tended to be quantitative. While there is nothing inherently wrong with taking a quantitative approach, perhaps a more in-depth exploration towards both security managers and end users experiences of upper management support would reveal important insights into how upper management support influences their security behaviour. Therefore, this study helps towards filling this research gap by investigating how upper management support influences the security behaviour of end users towards protecting information in organisations.

2.4 Information security policies

Although the insecure behaviour of end users, such as non-compliance with information security policies (hereafter security policies), is becoming a major research interest within information security management, most previous studies have tended to focus their attention on various factors beyond security policies when discussing non-compliance; rather than investigating how security policies themselves operate as a security control toward managing security behaviour in organisations.

For instance, when investigating non-compliance with security policies, researchers have investigated whether factors relating to end users such as social norms towards complying with security policies influences compliance rates (as described in the previous section on upper management) or whether a lack of security awareness or lack of perceived severity and certainty of punishment for non-compliance influences compliance rates (as will be discussed in later sections on SETA programmes and monitoring and enforcement practices). While this research is very important, and SETA programmes and monitoring and enforcement practices are arguably essential when managing information security, this approach to understanding non-compliance with security policies overlooks the fact that security policies are essentially a security control akin to SETA programmes and monitoring and enforcement practices. In other words, the fundamental purpose of security policies is to directly influence factors such as end user attitudes, social norms, perceived risk of punishment, and so on, surrounding the protecting of information, which then positively influences end user security behaviour; the same way SETA programmes and monitoring and enforcement practices purposefully influence end user security behaviour.

The importance of understanding this aspect of security policies cannot be overstated, for it is argued in this study that part of the reasons why end users might behave insecurely and demonstrate non-compliance with security policies may be due to factors directly relating to security policies, rather than because of factors directly relating to end users, which then requires the presence of additional security controls such as SETA programmes and monitoring and enforcement practices (although they will normally be developed and implemented to support security policies anyway).

Therefore, this next section discusses (1) what are security policies and how do they manage security behaviour, (2) previous studies which support the use of security policies, and (3) criticism towards the effectiveness of security policies as a security control.

2.4.1 What are security policies?

Within information security management literature, security researchers and practitioners have described security policies as an essential security control for managing information security in organisations (David, 2002; Flowerday and Tuyikeze, 2016; Hone and Eloff, 2002; von Solms and von Solms, 2004a; Soomro et al, 2016; Wood, 1995). Indeed, Hone and Eloff (2002, p. 402) argued, while there are various security controls that need to be developed and implemented within organisations, “the singularly most important of these controls is the information security policy”. However, despite this, not all organisations have security policies in place. For example, in 2018 the Department of Digital, Culture, Media and Sport carried out a survey of UK-based businesses and charities across the UK and found that only around a third of businesses (33%) and charities (36%) had a formal security policy which covered various security risks to information (Department of Digital, Culture, Media and Sport, 2019). Importantly, such low numbers may have be influenced by the sector within which an organisation was situated. For example, the survey showed that organisations within the finance or insurance sector had a higher percentage of adoption of security policies (66%, vs. 33% of all businesses), as did the healthcare sector (60%) (Department of Digital, Culture, Media and Sport, 2019).

According to Thomson and von Solms (2005, p. 71), the primary purpose of any organisational policy, whether relating to information security management or not, “is to influence and determine decisions, actions and other issues, by specifying what behaviour is acceptable and what behaviour is unacceptable”. Thus, in the context of information security management, the primary purpose of security policies is to define the specific roles and responsibilities of employees in relation to information security to enable a uniform and coherent approach to managing the protection of information in organisations (Doherty et al, 2009). Furthermore, Flowerday and Tuyikeze (2016, p. 170) argued the purpose of security policies are “to differentiate between employee behaviours that are either permitted or prohibited, as well as the consequent sanctions if the forbidden behaviours take place.”

Thus, in general, we can understand that security policies are an important security control when managing the security behaviour of end users because they define (1) the organisation’s security goals and objectives and the need to protect information, (2) the roles and responsibilities of end users towards protecting information, (3) the appropriate and inappropriate uses of information and information systems, and (4) the punishments for non-compliance with security policies (Doherty et al, 2009; Hone and Eloff, 2002; Flowerday and Tuyikeze, 2016; Kirlappos et al, 2013).

2.4.2 Previous studies supporting the use of security policies

As mentioned above, previous studies investigating non-compliance with security policies have tended to focus on various causal factors beyond the development and implementation of security policies when explaining why end users may or may not be compliant. Therefore, there were limited studies which have investigated the direct influence of security policies on end user security behaviour or those factors directly relating to security policies which may influence their effectiveness towards managing end user security behaviour. However, of those studies found there were some interesting findings worth discussing.

Most previous studies which have investigated the direct influence of security policies on end user security behaviour have tended to use *Theory of Planned Behaviour* (or some modified version) (e.g., Pahnila et al, 2007; Siponen et al, 2014; Safa et al, 2015). Theory of Planned Behaviour states a person's behaviour can be predicted by their intentions to perform a given behaviour. Behavioural intentions are described as encompassing the motivational factors that influence a behaviour and indicate how much a person is willing to perform it. In addition, theory of planned behaviour describes three determinants of a person's intentions to perform a behaviour. The first is a person's *attitude* toward the behaviour, which refers to whether the person has a favourable or unfavourable evaluation of the behaviour. Next is a social factor called *subjective norm*, which refers to a person's perceived social pressure to perform or not to perform the behaviour (as discussed in the last section on upper management support). Lastly, is *perceived behavioural control*, which refers to the perceived level of difficulty of performing the behaviour (Ajzen and Madden, 1986; Beck and Ajzen, 1991; Fishbein and Ajzen, 1970). Overall, Beck and Ajzen (1991, p. 287) posit "As a general rule, the more favorable the attitude and subjective norm with respect to a behavior, and the greater the perceived behavioral control, the stronger should be an individual's intention to perform the behavior under consideration".

In the context of information security management, this suggests that end user attitudes, social norms, and perceived behavioural control towards performing certain security behaviours, such as those outlined in security policies, will influence whether they have strong intentions towards performing them. There have been a few studies which have used Theory of Planned Behaviour and which have shown how security policies directly influence behavioural intentions towards protecting information and/or how factors relating to security policy development and implementation may influence the effectiveness of security policies.

For example, Pahnila et al (2007) conducted a study which utilised both the constructs of attitude and social norms towards compliance with security policies. Their findings showed that end user attitudes and normative beliefs towards complying with security policies positively influenced end user intentions towards compliance. However, more importantly, they also argued that *facilitating conditions* surrounding security policies are important because they determined whether end users developed a positive attitude towards complying with security policies. They argued if end users lack appropriate facilitating conditions, such as time to familiarise themselves with security policies, or they do not have quick and easy access to security policies, or they do not understand security policies, then end users are unlikely to develop positive attitudes, which would then influence their level of intention towards compliance.

A later study by Siponen et al (2014) also found that compliance behaviour is partly dependent upon factors relating to security policies. Their findings showed that end user attitudes towards compliance, normative belief towards compliance (a.k.a. subjective norms), and self-efficacy towards compliance (a proxy for perceived behavioural control), positively influenced end user intentions towards complying with security policies. Hence, they recommended security policies be made clear, concise, and easy-to-understand to ensure end users develop a positive attitude towards compliance. Again, this highlights how a positive attitude towards a security policy is also influenced by factors relating to security policy development and implementation.

In addition to studies which have investigated how factors relating to security policies influence end user compliance, are those studies which have investigated how security policies directly influence end user security behaviour. In other words, they have investigated how security policies themselves influence end user attitudes towards behaving securely, rather than investigating how attitudes towards security policies determines compliance.

For example, Safa et al (2015) investigated whether end user attitude, social norms, and perceived behavioural control influenced end user intentions to perform ‘conscious care behaviours’ in relation to information and information systems. Safa et al (2015, p. 66) described conscious care behaviours as when “users think about the consequences of their actions in terms of information security”. They also investigated whether *security awareness* influenced end user attitudes towards performing conscious care behaviours; whether *security policies* influenced end user subjective norms towards performing conscious care behaviours; and lastly, whether *experience and involvement* influenced perceived behavioural control towards performing conscious care behaviours. Thus, in this instance, Safa et al were looking at how security policies influence social norms as opposed to attitudes (as attitudes were investigated in relation to security awareness). Their findings showed that while attitudes and subjective norms influenced conscious care behaviour, these were in turn influenced by security awareness and security policies respectively.

Again, of major importance here is that security policies were found by Safa et al to influence end user subjective norms towards behaving securely when handling sensitive information, rather than subjective norms influencing behaviour in relation to security policies. Safa et al (2015, p. 75) explained their findings as being caused by security policies which "create a mandatory condition for staff to perform in a proper manner to safeguard the information assets". Thus, their findings showed that security policies can be used directly as an effective security control to influence the subjective norms of end users towards protecting information in organisations.

2.4.3 Criticism towards using security policies as a security control

Despite the many claims of security researchers and practitioners that a security policy is an essential security control, many more have questioned whether they are actually effective at managing security behaviour in organisations (Baskerville and Siponen, 2002; Doherty and Fulford, 2005; Doherty et al, 2009; 2011; Fulford and Doherty, 2003; Goel et al, 2010; Hone and Eloff, 2002b; Hong et al, 2006; Karyda et al, 2005; Kirlappos et al, 2013; Knapp et al, 2009). For example, Karyda et al (2005) argued despite the development and implementation of security policies being common practice in organisations, too often do they fail to achieve the goal of improved security behaviour. Similarly, Doherty et al (2009, p. 451) argued "the persistently high incidence of security breaches … may suggest that the information security policy is not always delivering the goods".

A major study in the debate surrounding the effectiveness of security policies was conducted by Doherty and Fulford (2005), who distributed security questionnaires designed to explore various aspects of developing and implementing security policies, and their subsequent impact on security breaches. Their results showed no statistically significant associations between the existence of security policies and the incidence and severity of any of the eight types of security breaches they assessed. Thus, they remarked “it came as something of a surprise … to find almost no statistically significant relationships between the adoption of information security policies and the incidence or severity of security breaches” (Doherty and Fulford, 2005, p. 34). Interestingly, Doherty and Fulford argued their findings may be caused by ineffective development and implementation of security policies (what they referred to as ‘dead documents’) rather than the accurate measurement of an ineffective security control. Thus, they questioned whether the apparent failure of security policies to help manage security behaviour in organisations was due to organisations experiencing problems during development and implementation.

Elsewhere in the literature, there is some evidence to support their argument. For example, Hone and Eloff (2002) claimed most end users in organisations do not fully understand security policies because they are too long, too technical, or they have not been tailored to the everyday tasks that end users are likely to perform, and so they do not consider information security to be relevant to their job role. Thus, Hone and Eloff (2002, p. 14) argued in most organisations “the information security policy appears to be totally ineffective and is not achieving its aim of explaining the need and concepts of information security to the users”.

Similarly, Doherty et al (2009) argued that many organisations fail to tailor security policies to the unique organisational environments in which they will be implemented. To support their argument, they investigated the development of security policies in universities and found that “there was absolutely no evidence of any University explicitly tailoring specific policy issues to take account of the knowledge intensive context in which their policies will be applied” (Doherty et al, 2009, p. 455). These findings were repeated several years later by Doherty et al (2011) who showed again that security policies were often written in a generic and predictable manner, with very little contextual tailoring.

Lastly, some studies have even suggested that many organisations are failing to make end users aware of the existence of security policies, which means the effectiveness in terms of influencing their security behaviour will be greatly reduced (Fulford and Doherty, 2003; Hone and Eloff, 2002a; Whitman, 2004). For example, a study conducted by Fulford and Doherty (2003) which investigated the dissemination practices in large UK-based organisations found that only 76% of the surveyed organisations had a security policy in place. Moreover, they found of those 76% the majority were not properly disseminating security policies, which meant end users were largely unaware of their existence.

Importantly, the problem of organisations failing to effectively develop and implement security policies is exacerbated by a severe lack of research in this area. As mentioned above, most research on non-compliance with security policies investigates factors beyond security policies, which overlooks the possibility that some end users might not comply with security policies due to factors connected to the security policy itself. For example, Stahl et al (2012, p. 89) argued while there is widespread agreement toward security policies being one of the most influential security controls that organisations can develop and implement, "it is extremely difficult to assess whether there is any truth behind this received wisdom as there have been few empirical contributions … into the behaviour and impact of information security policies".

In addition, while there are some publications offering recommendations to organisations on how to develop security policies, these have tended to focus more on the *contents* rather than the *form* of security policies (Baskerville and Siponen, 2002; Flowerday and Tuyikeze, 2016; Goel et al, 2010). For example, Goel et al (2010) argued while there has been much discussion on what to include in security policies, there has been very little discussion on how to properly write security policies. They described this is problematic for many organisations because "two policies with the same basic content can have vastly different impacts on the organization based on their form." (Goel et al, 2010, p. 282). Thus, they argued towards more research being conducted on how to effectively develop security policies.

Lastly, there is also a lack of qualitative research being conducted on security policies and how they influence end user security behaviour. For example, Karyda et al (2005) argued most studies that have investigated security policies have mostly used quantitative methods, where little research has been conducted based on qualitative methods. Karlsson et al (2017, p. 268) similarly argued "there exists practitioner-oriented literature … However, this literature focuses on the design process and product guidelines without reflecting on the end products' usefulness from an employee's perspective".

Therefore, this study significantly contributes towards improving our understanding of security policy development and implementation, and the influence security policies have on end user security behaviour, through conducting an in-depth qualitative study which investigates both the experiences of security managers in developing and implementing security policies (with a particular focus on the form of security policies), and the experiences of end users of security policies and how these influence their security behaviour.

2.5 Security education, training, and awareness (SETA) programmes

According to security researchers and practitioners, while it is incredibly important for organisations to ensure that all end users are aware of security policies, end users must also be aware of various security threats and vulnerabilities in information security, and be provided with any security training and/or education necessary to perform their job roles effectively and securely (Alshaikh et al, 2018; Abawajy, 2014; Alzamil, 2012; Chan and Mubarek, 2012; Bada et al, 2015; Eminagaoglu et al, 2009). For example, Alzamil et al (2012, p. 39) argued SETA programmes enhance security behaviour in organisations by improving end users' awareness of the need to protect information from various threats, and through developing skills and knowledge so they can perform their jobs roles more securely. Hence, SETA programmes can be understood as building upon and supporting the foundations laid down during the development and implementation of security policies and which further improve end user security behaviour in organisations.

However, much like security policies, not all organisations have SETA programmes in place. For example, the *UK Cyber Security Breaches Survey* (Department of Digital, Culture, Media and Sport, 2019) found that just under a third of businesses (27%) and charities (29%) had employees who attended internal or external training programmes in the previous 12 months. Importantly, this was again potentially influenced by the sector within which the organisation was situated. For example, there were several sectors which stood out as being more likely to train and/or educate their employees. These included finance or insurance-based organisations (56%, vs. 27% overall), information or communications-based organisations (45%), and healthcare-based organisation (45%).

Due to the importance placed upon developing and implementing SETA programmes in organisations, the remainder of this section discusses (1) the three learning levels of SETA programmes, (2) previous studies which support the use of SETA programmes, and (3) criticism towards the effectiveness of SETA programmes as a security control.

2.5.1 The three learning levels of SETA programmes

Security researchers and practitioners tend to describe SETA programmes as comprising three learning levels which generally correspond to three different security concepts; that is, security education, security training, and security awareness (Dominquez et al, 2010; Hansche, 2001a; 2001b; Katsikas, 2000; Maqousi et al, 2013; Peltier, 2005; von Solms and von Solms, 2009; Wilson and Hash, 2003). Therefore, it is important to discuss what each learning level or security concept represents and how each influences end user security behaviour in organisations.

According to Dominguez et al (2010), the concept of security awareness refers to when organisations try to motivate end users towards behaving securely. The purpose of a security awareness programme is simply to focus the attention of end users on the need to protect information and to motivate them to perform security actions (Dominguez et al, 2010; Hansche, 2001a; Katsikas, 2000; Kruger and Kearney, 2008; Wilson and Hash, 2003). For example, Kruger and Kearney (2008, p. 255) argued "the goal of such an awareness programme would be to increase awareness of the importance of information systems security and the possible negative effects of a security breach or failure”.

Supporting security awareness is security training, which refers to when organisations teach end users the required skills that will enable them to perform their job roles securely (Amankwa et al, 2014; Manke and Winkler, 2012). In other words, security training instructs end users on how to perform certain security actions to defend organisations against the security threats identified as part of security awareness. For example, Peltier (2005, p. 37) argued security training is “the process that teaches a skill or the use of a required tool”. Therefore, security training programmes is usually more formal than security awareness because it is directed towards developing knowledge, skills, and abilities that improve job performance (Hansche, 2001a; Wilson and Hash, 2003).

Finally, the concept of security education, which refers to either the required expertise of security managers or the advanced learning of end users on information security (Katsikas, 2000; Peltier, 2005). For example, Peltier (2005, p. 37) described security education as “the specialized, in-depth schooling required to support the tools or as a career development process”. Therefore, in contrast to security training, security education is more in-depth, and while security training mostly utilises practical methods of delivery, security education tends to use more theoretical and instructional delivery methods. Security education may also be generic in nature while security training tends to be focused more on developing skills which are specific to end user job roles (Amankwa et al, 2014).

Importantly, security experts argue that all three learning levels are required to ensure end users behave securely and are properly able to protect information in organisations. Thus, while security education, security training, and security awareness are all described as distinct security concepts, in practice, all must be present to be effective at managing end user security behaviour (von Solms and von Solms, 2009; Thomson, 1999; Yanus and Shin, 2007). However, despite such claims, some have argued towards a major confusion within the literature over each of the three learning levels of SETA programmes, which has caused major problems for many organisations when trying to develop and implement SETA programmes (Amankwa et al, 2014; Hansch and Benenson, 2014; Tsohou et al, 2008).

For example, Tsohou et al (2008) described the existence of multiple definitions of security awareness as one of the major obstacles in information security management. They argued such differences of opinion were negatively impacting upon the ability of organisations to develop and implement effective SETA programmes; where ambiguity surrounding the concept of security awareness may cause organisations to place indistinct or unattainable goals and objectives for security awareness programmes.

In addition, Amankwa et al (2014) reviewed the literature on SETA programmes and found the differences between each learning level were not always made clear by security researchers and the different security concepts were often used interchangeably. The most common confusion related to the concept of security awareness. Amankwa et al (2014) stressed that each concept should not be confused with any other since they are stated to have different meanings, where the differences help organisations determine whether end users should be educated or trained on information security or when organisations should introduce various awareness programmes.

2.5.2 Previous studies supporting the use of SETA programmes

In contrast to those studies discussed in the previous section which investigated how security policies influence security behaviour and/or how factors relating to security policy development and implementation influence compliance, there have been many more studies which have investigated various factors relating to end user security behaviour and how SETA programmes can improve compliance (or improve security behaviour in general). Further, most of these studies have utilised either Protection Motivation Theory (PMT) or Theory of Planned Behaviour (TPB) (or a combination of PMT- and TPB-based constructs). Therefore, both Protection Motivation Theory and Theory of Planned Behaviour will now be discussed along with those studies which have utilised either theory when investigating end user security behaviour and the potential positive influence of SETA programmes.

2.5.2.1 Protection Motivation Theory-based studies

Protection Motivation Theory is structured around two cognitive processes: *threat-appraisal* and *coping-appraisal*. The threat-appraisal process evaluates a given threat that will occur due to some maladaptive behaviour. The primary constructs influencing threat-appraisal are *perceived threat severity* and *perceived threat vulnerability*. Perceived threat severity assesses how dangerous someone believes the threat would be to his or her own life while perceived threat vulnerability refers to how personally susceptible someone feels to a given threat (Floyd et al, 2000; Milne et al, 2000). The coping-appraisal process evaluates the ability of someone to cope with and avert the given threat. The constructs influencing coping-appraisal are two efficacy variables (*response efficacy* and *self-efficacy*) and *response cost*. Response efficacy concerns beliefs about whether the recommended coping response will be effective in reducing the threat. Self-efficacy concerns someone's belief about whether they can perform the recommended coping response. And response costs concern someone's belief about how costly performing the recommended response will be in terms of time and effort (Floyd et al, 2000; Milne et al, 2000).

In the context of information security management, we can understand why security researchers are attracted to Protection Motivation Theory. In general, the concepts of security awareness/security education (as described above) correspond well to the concept of threat appraisal, while the concept of security training corresponds well to the concept of coping appraisal, where both combined may help to improve end user security behaviour. Indeed, there are several studies which have supported the use of Protection Motivation Theory in understanding end user security behaviour (Herath and Rao, 2009a; Ifinedo, 2012; Pahnila et al, 2007; Siponen et al 2007; 2014).

For example, an early study by Siponen et al (2007) found that threat appraisal (single construct) and coping appraisal (comprising self-efficacy and response efficacy) positively influenced end user intentions towards complying with security policies.

Thus, they recommended that organisations make end users aware of information security threats and vulnerabilities and that measures be put in place to ensure end users can effectively perform various security tasks to protect information.

Importantly, many later studies using PMT have produced mixed finings. For example, studies by Herath and Rao (2009a) and Vance et al (2012) found that while perceived threat severity influenced end users’ concern towards security breaches, perceived threat vulnerability was not found to be significant. Further, while Herath and Rao (2009a) found both response efficacy and self-efficacy influenced end users’ intentions towards compliance, Vance et al (2012) found only self-efficacy had a positive influence on end users’ intentions to comply with security policies. Further still, a study by Ifinedo (2012) found the opposite, where perceived threat vulnerability influenced end user behaviour while perceived threat severity didn’t. Thus, findings surrounding the potential use of PMT towards explaining end user security behaviour are still inconclusive.

2.5.2.2 Theory of Planned Behaviour-based studies

As explained in the previous section on security policies, Theory of Planned Behaviour states that end user attitudes, social norms, and perceived behavioural control towards performing certain security behaviours will influence whether they have strong intentions towards performing them. Again, we can understand the attraction towards Theory of Planned Behaviour in relation to SETA programmes. The general idea is that end user attitudes and/or social norms are influenced by the learning levels of security awareness and security education, while end users’ perceived behavioural control will be influenced by the learning level of security training.

There have been numerous studies which have supported Theory of Planned Behaviour towards understanding end user security behaviour in relation to SETA programmes (Bulgurcu et al, 2010; Dinev and Hu, 2007; Hazari et al, 2008; Zhang et al, 2009). For example, Dinev and Hu (2007) investigated whether ‘technology awareness’ influenced the attitude of end users towards performing protective actions. They defined technology awareness as “a user’s raised consciousness of and interest in knowing about technological issues and strategies to deal with them" (Dinev and Hu, 2007, p. 391). They argued the more knowledgeable end users were about the problems and consequences of cyber-attacks and the ways to prevent them, the more likely they were to form a positive attitude towards protecting information, which will then motivate them to behave more securely. They also looked at whether ease-of-use of performing preventive behaviours influenced perceived behavioural control. They found that both technology awareness and ease-of-use influenced end user attitude and perceived behavioural control respectively, which in turn influenced end user behavioural intentions. Thus, Dinev and Hu argued SETA programmes which include both awareness of security threats and vulnerabilities as well as instruction on how to perform security actions can improve the security behaviour of end users in organisations.

In addition, Hazari et al (2008) investigated the security behaviour of end users who perform work related duties from home, either on a part-time or full-time basis. They referred to these end users as *Work Related Home Computing* (WRHC) users. They found WRHC user attitudes, subjective norms, and perceived behavioural control influenced their intentions towards behaving securely at home. Thus, Hazari et al (2008, p. 16) recommended that organisations "should offer technology related courses which include content… about information security issues, thereby giving them more confidence and a better attitude."

Lastly, Bulgurcu et al (2010) investigated whether end user attitudes, subjective norms, and self-efficacy (a proxy for perceived behavioural control) positively influenced end user intentions to comply with security policies. In addition, they investigated whether security awareness influenced end user attitudes towards compliance. Security awareness was argued to influence end user attitudes directly and indirectly via various 'outcome beliefs' towards compliance, such as the benefits and safety provided to organisations which comes from end user compliance, but also the costs to end users themselves for complying, such as work impediments. They found that attitude, subjective norms, and self-efficacy all influenced end user intentions towards compliance. More importantly, they found that security awareness directly and indirectly (via outcome beliefs) influenced end user attitudes towards compliance. Thus, they concluded because such outcome beliefs positively influenced end user attitudes towards compliance, security awareness programmes should be implemented to emphasize such outcome beliefs. Further, because self-efficacy influenced behavioural intentions, they argued organisations should provide security training programmes to ensure end users know how to perform certain security tasks to comply with security policies.

2.5.3 Criticism towards the use of SETA programmes as a security control

Much like security policies, many security scholars have questioned the effectiveness of SETA programmes to positively influence end user security behaviour. Indeed, studies have shown that end users often have very poor levels of security awareness and often lack the basic skills required to perform their job roles securely. For example, Albrechtsen (2007) investigated the views of end users towards information security management and found that the levels of security awareness in some organisations were inadequate. He found that many end users performed very few security actions, were not familiar with possible security threats and vulnerabilities, and were not aware of possible consequences of security breaches.

Similarly, Chan and Mubarek (2012) investigated the levels of security awareness of end users in Higher Education institutions and the results from their survey showed that only 24.7% knew the term phishing, 17.9% knew the term social engineering, and 65.9% knew what constituted a strong password. In addition, the results showed that 52.9% shared their passwords, 77.3% had left their computer unattended and unlocked, and 74% clicked on unknown links contained within emails. Thus, Chan and Mubarek (2012, p. 28) concluded “the results of the questionnaire were both alarming and surprising … The generally low levels of awareness were reflected in employee behaviors, whereby most employees have admitted to performing actions which could have negative consequences for the organization”.

While the above mentioned studies have shown that end users often lack security awareness and regularly perform behaviours which put organisations and information at increased risk; importantly, it is argued in this study that the above findings could perhaps be understood as the result of SETA programmes being poorly developed and implemented by organisations, rather than SETA programmes simply being an ineffective security control at managing end user security behaviour; much like the previous section argued towards the ineffectiveness of security policies. For example, Manke and Winkler (2012) argued despite previous studies providing numerous examples of where poor security behaviour has led to major impacts against the level of information security in organisations, it is not that SETA programmes are an inherently flawed security control, but that the development and implementation of SETA programmes in organisations vary greatly in both quantity and quality.

Indeed, some studies have shown that many organisations don’t even have SETA programmes in place, which obviously drastically reduces the level of awareness and ability of end users towards protecting information. For example, Rezgui and Marks (2008) investigated SETA programmes in Higher Education institutions and were surprised to find that security training was barely practiced. Rezgui and Marks (2008, p. 248) exclaimed, “Unfortunate but true, once hired … employees are expected to perform critical jobs with absolutely no training”.

Alzamil et al (2012) similarly investigated the levels of end user security awareness in in Saudi organisations. Their findings showed that when questioned about security awareness programmes, only 46.1% of security managers admitted to raising end user awareness about the importance of information security. Further, when questioning end users about their experiences of security training, only 37.7% described being admitted into security training programmes on information security. Importantly, Alzamil et al (2012, p. 49) concluded, “the lack of proper training and policies enforcements is a major cause of absence of information security awareness at the surveyed organizations”.

In addition to a lack of providing SETA programmes, others have argued SETA programmes are often of very low quality. For example, Valentine (2006, p. 17) argued many organisations adopt a one-size-fits-all approach when developing and implementing SETA programmes, where “every employee within an organization attends the same boiler-plate training session regardless of job function or knowledge level”. Valentine argued while such an approach might allow for large-scale improvements in security awareness, the outcome will often be less than adequate to properly protect information because organisations and the individuals within them are so incredibly varied.

Stewart and Lacey (2012) similarly argued that SETA programmes in organisations show little sign of innovation in the last few decades. They described how most SETA programmes are based upon the ‘The Broadcast Approach’, where the problem of insecure behaviour is caused by ‘a lack of facts’. Therefore, improvement in security behaviour require only the broadcast of those facts to end users. However, they argued having technical expertise in understanding security risks does not necessarily mean having expertise in communicating this to end users. Thus, they argued “technical specialists are venturing outside of their technical expertise when deciding what audiences will be told, how they will be told and how often they will be told” (Stewart and Lacey, 2012, p. 30).

The problems associated with developing and implementing effective SETA programmes are arguably exacerbated by an overall lack of research on how to develop and implement SETA programmes. Despite previous studies which have adopted PMT or TPB-based constructs to provide theoretical support for the use of SETA programmes, these studies have provided little insight into how to develop and implement SETA programmes in practice. This is important because while end user levels of understanding towards various security threats, vulnerabilities, and their abilities to perform various security actions are theoretically supported by those studies to have an influence on security behaviour, this does not mean to say that the simple existence of SETA programmes will automatically produce improvements in end users’ understanding of information security concepts/issues nor improvements in their capability to perform security tasks. In other words, not all SETA programmes are created equally. Thus, unless organisations are provided with concrete recommendations on how to develop and implement SETA programmes then end users may potentially continue to have low levels of security awareness and ability to perform certain security tasks, despite the existence of SETA programmes in organisations.

Furthermore, while there have been some studies which have shown improvements in end user security awareness following SETA programmes, along with useful recommendations for development and implementation (e.g., Albrechsten, 2007; Hagen and Albrechtsen, 2009; Shaw et al, 2009), most recommendations are from security practitioners which are unsupported by empirical research (e.g., Desman, 2003; Peltier, 2005; Valentine, 2006, Wilson and Hash, 2003; Vroom and von Solms, 2002). Thus, security researchers have argued towards more research being done on how to effectively develop and implement SETA programmes.

For example, Puhakainen and Siponen (2010) argued most recommendations for developing and implementing SETA programmes are largely atheoretical and anecdotal. Puhakainen and Siponen (2010, p. 758) stressed that "Empirical evidence is … important as it indicates whether the training and education approach works *in practice*, which is the ultimate goal of training. A training programme that does not work in practice is of limited value". Bauer et al (2017) similarly argued while the importance of having SETA programmes in organisations is now widely accepted, there appears to be no commonly agreed method of how to effectively develop and implement them. Lastly, in addition to an overall lack of research on SETA programmes, Abawayj (2014, p. 237) argued there has been very little research that looks at security awareness and security training effectiveness from the recipients' point of view.

Therefore, this study significantly contributes towards improving our understanding of SETA programmes through an in-depth qualitative investigation of the experiences of both security managers, who develop and implement SETA programmes in organisations, and end users, who take part in SETA programmes as part of their job role.

2.6 Monitoring and enforcement of security behaviour

Although having the support from upper management and developing and implementing security policies and SETA programmes are essential towards making sure end users are behaving securely and protecting information, many security researchers and practitioners have argued it is also important that organisations monitor whether end users are behaving securely and suitably punish them when they aren’t (Cheng et al, 2013; Darcy et al, 2008; David, 2002; Knapp and Ferante, 2012; Siponen et al, 2007; von Solms and von Solms, 2004b; Wood, 1997). For example, von Solms and von Solms (2004b) described the consequences of failing to monitor and enforce security behaviour as creating a false sense of security, where organisations will assume that because they have all the necessary security policies and SETA programmes in place, end users will behave securely; without ever realising if this is the case. Furthermore, some surveys indicate that a low percentage of organisations are monitoring end user security behaviour. For example, the *UK Cyber Security Breaches Survey* (Department of Digital, Culture, Media and Sport, 2019) found that only 40% of businesses and 33% of charities were monitoring end user security behaviour.

Therefore, this section discusses (1) what is monitoring and enforcement, (2) previous studies which support monitoring and enforcement practices, and (3) possible alternatives to the use of punishment in monitoring and enforcement practices.

2.6.1 What is monitoring and enforcement of security behaviour?

Security experts have argued that because performing security actions to protect information are mandatory, organisations must regularly monitor and enforce security behaviour (Boss et al, 2009; Kilman and Stamp, 2005). Thus, if following the monitoring of end users there is found to be insecure behaviour, such as non-compliance with security policies, then an organisation must enforce this by appropriately reacting to the transgressive behaviour. An organisation can enforce security behaviour through punishments such as an official reprimand, monetary penalty, job demotion, work suspension or even termination of employment (Knapp and Ferante, 2012).

Importantly, it should also be noted that the monitoring of security behaviour has been argued to have a secondary function. It also allows organisations to identify when end users are struggling to behave securely because of problems directly relating to security controls. For example, Sasse and Flechias (2005) argued end users often cannot perform certain security actions because (1) the technical controls are too difficult to use, (2) they haven't been properly trained, and (3) they are unaware that they are supposed to perform them. Therefore, monitoring their security behaviour enables organisations to become aware of such issues and to properly address them.

The importance of this cannot be overstated, as security experts make clear, the monitoring and enforcement of security behaviour should not take place until end users have been properly made aware of the security policies with which they must comply and are sufficiently trained on how to behave securely (Lowery, 2002; Sasse and Flechias, 2005). Otherwise end users may become even more frustrated and are likely to develop a negative attitude towards information security, which will further drive insecure behaviour (Kirlappos and Sasse, 2014).

2.6.2 Previous studies supporting monitoring and enforcement practices

Previous studies which have investigated the influence of monitoring and enforcement practices towards improving security behaviour have overwhelmingly been based upon the criminological theory *General Deterrence Theory* (GDT). The basic assumptions of GDT are, the greater the perceived certainty and perceived severity of punishments for certain behaviours, the more likely individuals are deterred from performing them. As Jacobs (2010, p. 487) stated, "The paradigm itself is simple and straightforward … Crime occurs when the expected rewards outweigh the anticipated risks, so increasing the risks, at least theoretically, will prevent most crimes in most circumstances".

Hence, in the context of information security management, GDT is mainly used to explain non-compliance with security policies as being the result of a lack of fear towards the monitoring of, and punishments for, non-compliance with security policies (D'Arcy and Herath, 2011; Knapp and Ferante, 2012). There have been numerous studies which have utilised GDT to investigate end user non-compliance; although these studies have tended to produce very mixed findings.

For example, an early study by Siponen et al (2007) found that sanctions influenced actual compliance with security policies, where they concluded organisations must ensure end users are made aware that their security behaviours are monitored and clearly state what the punishments will be for non-compliance.

However, studies by Darcy et al (2008) and Cheng et al (2013) found that while perceived severity of sanctions positively influenced security behaviour, perceived certainty of sanctions did not. In contrast, a study by Herath and Rao (2009a) found that only perceived certainty of sanctions positively influenced security behaviour. In fact, their study showed that perceived severity of sanctions had a significant and negative influence on security behaviour!

Lastly, there have been several studies which don't support punishment-based approaches at all (e.g., Pahnila et al, 2007; Siponen and Vance, 2010; Posey et al, 2011). Thus, security scholars have come to conclude that overall, extant research provides inconsistent and sometimes contradictory findings for general deterrence theory in the information security context (D'Arcy and Herath, 2011).

Another major issue with previous research into how monitoring and enforcement practices influence security behaviour is there has been little research into how monitoring and enforcement practices are managed in organisations and whether there are any challenges connected to using such an approach to manage security behaviour in organisations.

For example, Vroom and von Solms (2004) argued while it is important to monitor and enforce end user security behaviour, there is little evidence to suggest that this actually occurs in practice. Importantly, Vroom and von Solms stated that several practical obstacles may come into play when attempting to monitor and enforce security behaviour in organisations which may explain why this happens. For example, to properly monitor end user security behaviour would require large amounts of organisational resources and manpower, as well as numerous other factors which may play a disruptive role when monitoring and enforcing information security. Of course, a major problem with our understanding towards this is little research has been conducted on monitoring and enforcement practices in organisations. Only one study was found to have investigated monitoring and enforcement practices (Rezgui and Marks, 2008). Thus, much more research is needed in this area.

This is important because if organisations aren’t monitoring and enforcing security behaviour for whatever reason(s), then end users will not have the desired perceived certainty and perceived severity of punishment for non-compliance, which might also explain why so many end users are described as behaving insecurely in organisations. Thus, while GDT (and arguably common sense) may provide partial support towards the usefulness of monitoring and enforcement of security behaviour, in practice this may not be a suitable means of managing end user security behaviour. Therefore, this study significantly contributes towards improving our understanding of monitoring and enforcement practices in organisations through an in-depth social study of the experiences of security managers, who are tasked with conducting monitoring and enforcement practices, and end users, who regularly have their security behaviour monitored and enforced.

2.6.3 Possible alternatives to punishment-based approaches

In response to the inconsistent findings with previous studies based upon GDT, security researchers have investigated possible alternatives to punishment-based approaches (D’Arcy and Herath, 2011; Darcy and Devaraj, 2012). One of the major arguments in the literature surrounding monitoring and enforcement practices is that not everyone is susceptible to formal sanctions such as threats of punishment. Thus, security researchers have argued towards moving beyond formal sanctions towards the use of informal sanctions, such as those relating to the moral aspects of security behaviour (Darcy and Devaraj, 2012; Son, 2011; Vance and Siponen, 2012).

For example, a study by Son (2011) found that while neither perceived certainty and perceived severity of punishment influenced end user security behaviour, moral commitment was found to have a positive influence. Thus, they concluded that intrinsic motivations such as moral commitment could possibly explain end user compliance behaviour better than extrinsic motivations such as fear of punishment, where our understanding of end user security behaviour has perhaps been limited by a lack of attention to the intrinsic motivations surrounding security behaviour.

In addition, a study by Darcy and Devaraj (2012) found that informal sanctions such as moral beliefs were a significant determinant of end user intentions towards behaving securely and were more strongly associated than formal sanctions. Darcy and Devaraj (2012, p. 113) claimed that “anticipated feelings of social and self-disapproval are important considerations within the cost portion of the rational decision process involving technology misuse”. Again, they concluded that prior research that focused solely on formal sanctions were missing a key component of security behaviour.

It is Important to note however, that there are also studies which show moral beliefs or informal sanctions do not influence security behaviour. For example, Siponen et al (2007) and Vance and Siponen (2012) found informal sanctions do not influence security behaviour.

In addition to investigating how informal sanctions such as moral beliefs influence end user security behaviour, other studies have investigated the usefulness of reward-based approaches. For example, Bulgurcu et al (2010) argued rewards can also be used to improve compliance with security policies. Bulgurcu et al described rewards as tangible or intangible remuneration given to end users by their organisations in exchange for compliance with security policies. They found that rewards had a significant influence over end user perceptions of the benefits of compliance, which in turn influenced end users’ attitudes towards compliance.

Chen et el (2012) similarly argued rewards can be used by organisations to exert control over end user security behaviour through tangible (e.g., pay bonus and holidays) and intangible rewards (e.g., promotion, employee of the month). Their study showed that while punishments influenced compliance, rewards were also influential towards end user compliance. Thus, Chen et el (2012, p. 178) concluded that “managers would be wise to … also put reward schemes in place to help … foster a common favorable disposition to compliance”.

Again, it’s important to note that some security researchers have argued that using rewards will not improve security behaviour (e.g., Boss and Kirsch, 2007; Panila et al, 2007). Overall, however, the influence of moral beliefs and rewards is still under-researched and therefore more research into this area is much needed, given the lack of support for GDT. Hence, this study significantly contributes towards improving our understanding of monitoring and enforcement practices in organisations by also investigating how both moral beliefs connected to security behaviour and rewards schemes may help to improve security behaviour.

2.7 Usability of technical security controls

Although it is important to develop and implement security controls such as SETA programmes to ensure end users can perform various security actions and comply with security policies, it is also important to understand how factors relating to the design and configuration of various technical security controls can also influence whether end users can or cannot perform security actions. For example, security scholars have argued when trying to understand the reasons for end users behaving insecurely in organisations it is important to realise that another significant factor may be a lack of user friendly security technologies (Furnell, 2005; Furnell and Katsabas, 2006; Johnston et al, 2003; Kainda et al, 2010).

This is important to acknowledge because it implies that security controls such as security policies, SETA programmes, and monitoring and enforcement practices may not guarantee that end users will behave securely, if the technical security controls themselves are badly designed or unusable from the perspective of end users. When end users are unable to behave securely due to factors directly relating to technical security controls, they are generally deemed unusable. Thus, we have seen the emergence and increasing popularity of usable security research or *Human-Computer Interaction and Security* (HCI-S) research, which focuses on how to improve the usability of technical security controls from the perspective of end users. Therefore, this next section discusses: (1) what is usable security, (2) major research areas in usable security research, namely passwords and email encryption, and (3) criticism towards usable security research.

2.7.1 What is usable security?

The emergence of Human-Computer Interaction and Security (HCI-S) research is generally described as an offshoot from the earlier field of Human-Computer Integration research, which began as far back as the 1960s (Johnston et al, 2003; Kainda et al, 2010; Renaud and Flowerday, 2017). For example, Johnston et al (2003) stated that Human-Computer Interaction research focused on the interaction between one or more human users and one or more computers. Further, this interaction took place via human user interfaces which were purposefully designed to assist those human users in using the computer. They described a well-designed human user interface as one which assisted the human user in becoming proficient towards completing a variety of tasks, where they became overall satisfied with using the technology. However, in contrast, Johnston et al (2003, p. 276) stated “a poorly designed interface can frustrate the user and hinder the successful completion of tasks, resulting in aversion and scepticism towards using the specific technology in the future”. Thus, the overall purpose or goal of Human-Computer Interaction research was to improve the user friendliness of technology.

In the context of information security management, we can understand the overall purpose of HCI-S research as extending this mission to include security technology. For example, Johnston et al (2003, p. 278) argued “HCI-S deals with how the security features … can be made as user friendly and intuitive as possible. The easier a system is to use, the less likely the user will be to make a mistake or to try to bypass the security feature”. Importantly, to help improve the usability of security technology from the perspective of end users, usable security researchers have argued towards a design approach which puts end users at the centre of attention.

For example, Arbas et al (2004) argued towards a user-centred design approach which incorporated end users during the design process. They described various ways in which end users could be involved. For example, end users may be consulted at the beginning of the design process to determine their needs, referred to as 'requirements gathering', or end users could become deeply involved throughout the entire design process as 'design partners'. However much involved end users were in the design process, Arbas et al (2004) stressed that the overall purpose of the user-centred design approach was to make sure that end users were able to learn and make good use of the finished product with a minimum of effort.

Fidas et al (2010) similarly argued security technology designers must apply a user-centric approach, where end users are at the centre of the design process to achieve a common understanding between end users and technology designers towards how end users would likely use security technologies in practice, which would then ensure higher levels of usability upon completion. Thus, Fidas et al (2010, p. 112) argued "The objective is to reach a certain point in which the designers and the users share a common conceptual ground related to the developed system e.g. sharing a common mental model of using it".

2.7.2 Previous studies on usability of technical security controls

According to usable security researchers, there are two canonical areas in usable security research. These are user authentication (i.e., user logins and passwords) and email encryption (Fidas et al, 2010; Nurse et al, 2011; Payne and Edwards, 2008). Therefore, both areas will now be critically discussed.

2.7.2.1 The password problem

According to Payne and Edwards (2008), user logins and passwords have presented themselves as a major research interest because there is an innate tension between end users having a usable password (such as a short, memorable password used on many systems) and having a secure password (such as a long, complex password unique to each system). Thus, the problem of passwords is considered a leading problem and major research area in usable security research (Faith and Garfinkel, 2004; Fidas et al, 2010).

The wide interest surrounding passwords arguably began following the publication of the seminal paper *Users Are Not the Enemy* by Adams and Sasse in 1999, which presented the findings from a web-based questionnaire and in-depth interviews which investigated end user password behaviour. Adams and Sasse found that many end users were having to remember numerous passwords, use different passwords for different applications and systems, and/or were required to change their passwords regularly. Consequently, many end users demonstrated insecure behaviours, including the creation and use of weak passwords; writing passwords down; and sharing their passwords. Importantly, Adams and Sasse (1999) argued the main causes of such insecure behaviour was the lack of a user-centred design during development, where designers did not take into consideration the everyday work routines of end users. Thus, Adams and Sasse (1999, p. 45) concluded that "Unless security departments understand how the mechanisms they design are used in practice, there will remain the danger that mechanisms that look secure on paper will fail in practice".

We can understand then, that usable security is not just about making technical controls easy to use in and of themselves (e.g., focusing on designing nicely presented interfaces) but also acknowledging and understanding how the physical and social context surrounding the use of technical controls also influences their level of usability from the perspective of end users (Flechais et al, 2004). For example, Kirlappos et al (2013) argued the primary focus of end users is not performing secondary *security* tasks, rather it is performing primary *work* tasks. They argued security tasks are often treated as overheads by end users, and as a result end users are only willing to spend a limited amount of time and effort on security. Thus, when security tasks become too difficult they make end users consider non-compliance a viable course of action.

Beautement et al (2008) similarly described the 'compliance budget' of end users when performing security tasks. They argued decisions to behave securely are determined by the perceived costs and benefits of the security task in question. They highlighted that the perceived costs and benefits are centred on primary work tasks. Hence, when end users perform security tasks they do so only up until a certain point – normally when performing the security task begins to interfere with their primary work tasks – beyond which the costs are considered too great, where end users will become more likely to circumvent difficult technical security controls.

Considering the above studies which have highlighted the problems of end users creating and managing secure passwords, security researchers and practitioners have investigated possible solutions. For example, Payne and Edwards (2008) argued towards the use of *passphrases*, which use sequences of words which are easier to remember, and because they are longer than passwords they are more secure. They also argued for the use of *pass-algorithms*: An example is when an end user must type the next letter in the alphabet for each letter of their chosen password. Thus, the password 'BEL' would become 'CFM'. The major advantage of doing this is it jumbles normal words making them harder to guess but are still easy to remember. Further, even if you know the word you still won't know the algorithm used (Payne and Edwards, 2008).

In addition, Faith and Garfinkel (2004) argued towards the use of *graphical passwords* because end users will have a higher capacity for remembering images than words. Faith and Garfinkel (2004) also argued *biometrics* and hardware tokens represent possible alternatives to user authentication. Lastly, Stobert and Biddle (2014) argued things like *password managers*, which store and enter end users' passwords automatically for them, may help solve the password problem.

Whichever security solution is adopted to help alleviate the problems end users experience with passwords, the importance of improving the usability of passwords for end users cannot be overstated, due to the increasing number of passwords that end users have to remember and use as part of their everyday working lives. For example, Florencio and Herley (2007) conducted a large-scale study of password habits and they found that each end user had about 25 accounts that required passwords and each typed an average of 8 passwords per day. A later study by Stobert and Biddle (2014) found that the total number of accounts for end users was between 9 and 51 accounts, with a median of 27 accounts. Further, they showed that end users had between 2 and 20 unique passwords, with a median of 5 passwords.

2.7.2.2 The encryption problem

As mentioned above, the second major research area in usable security research is email encryption (Fidas et al, 2010; Nurse et al, 2011; Payne and Edwards, 2008). Major interest surrounding the problem of encryption arguably began with the publication of the seminal paper *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* by Whitten and Tygar in 1998. Whitten and Tygar (2005) argued that usable security will not be achieved through the design approach that is normally applied during the development process of other types of consumer software. They supported their argument via a usability assessment of a popular and 'well-designed' encryption software programme called *PGP 5.0*. When evaluating PGP 5.0's usability, they chose to use two separate evaluation methods: an analysis technique they referred to as 'cognitive walkthrough' (where they evaluated the software programme as if they were novice users) and a laboratory end user test.

Their findings relating to end user testing showed that despite 12 participants being well educated and experienced at using email, only one-third were able to use PGP 5.0 to correctly encrypt an email within the 90-minute timeframe. Furthermore, one-quarter accidentally exposed the secret they were meant to protect by sending an email they thought they had encrypted. Overall, Whitten and Tygar (2005, p. 699) concluded "All this failure is despite the fact that PGP 5.0 is attractive, with basic operations neatly represented by buttons with labels and icons, and pull-down menus for the rest".

While the study by Whitten and Tygar was published some time ago now, it appears things may not have improved much since. For example, Ruoti et al (2015) conducted a study on the usability of another popular and 'well-designed' encryption software programme called *Mailvelope*. They described Mailvelope as a modern PGP-based tool, which was highly rated on the Chrome Web Store (242 reviewers collectively gave it 4.6 out of 5 stars). They assessed the usability of Mailvelope by assigning 20 participants, who were grouped into 10 pairs, the task of exchanging encrypted emails. Their findings showed that only one pair were able to successfully complete the task using Mailvelope, while the remaining participants were unable to do so within the 1-hour time frame. Thus, Ruoti et al (2015) concluded that even after a decade and a half had passed, modern PGP-based tools are still unusable for the masses, where Johnny sadly hasn’t gotten any closer to encrypting his email using PGP.

2.7.3 Criticism toward HCI-S research

While the goal of improving the usability of security technologies is widely considered to be an important endeavour, there are those who question whether the goals of HCI-S research are simply too great and/or if HCI-S researchers overlook other contributing factors to the insecure behaviour of end users.

For example, Herley (2014) argued that improving the usability of security technology alone cannot solve the problem of insecure behaviour, as there are other organisational aspects which need to be addressed. Herley argued if end users are required to perform various security actions which consume their time and effort then there must be some form of compensation toward their remaining work load connected to their primary job role. In other words, it’s not solely a problem of making security technologies more usable for end users, rather its making organisations understand that performing security tasks consumes valuable time and effort and therefore the performance expectations of end users in relation to their primary job roles must be lowered, otherwise they will continue to bypass technical security controls to meet their targets. Thus, the overall conflict between performing security tasks and completing primary work tasks cannot be completely offset simply by making security technologies more usable (although this of course helps tremendously).

Kirlappos and Sasse (2014) similarly argued that in usable security research there is an implicit assumption that if end users can easily use technical security controls, they would be motivated to do so. However, simply making technical security controls more usable for end users will not in and of itself motivate end users to use them. Indeed, Kirlappos and Sasse (2014, p. 69) highlighted that “work by usability researchers … suggests that the assumption that ‘users want security, provided it’s not too difficult to use’ may be wide off the mark. Users look for efficiencies in their daily lives, and that means ‘the less I have to think about security, the better’”. In other words, it’s not enough to make technical security controls easier to use, as this alone will not necessarily provide the motivations for end users to use them. Thus, other security controls need to be in place in organisations to ensure end users are motivated to use them (e.g., security policies, SETA programmes, monitoring and enforcement practices).

Of course, this does not mean usable security research is not incredibly important towards understanding the insecure behaviour of end users. Indeed, this study argues usability aspects of technical security controls may prove an important factor when understanding security behaviour in organisations alongside that of security policies, SETA programmes, and monitoring and enforcement practices. Therefore, the present study includes usability aspects of technical security controls as a potentially important factor when investigating end users’ experiences of information security management in organisations.

Before moving on to discuss the practice of security testing it should be noted that, while the five areas discussed above are presented as being the most important areas of information security management, they should not be considered as disconnected from one another in the sense that an organisation may choose to spend resources in one or more area independently. Rather, good information security management necessitates that all these areas be properly considered by organisations, where each area receives sufficient attention; as a lack of attention in one area will impact upon the effectiveness of another area, due to the holistic nature of information security management (Bunker, 2012; Martins and Veiga, 2015).

For example, Goo et al (2013) argued that information security management should be conceived of as a holistic process that involves various ‘critical success factors’ which must be considered equally important, as each will determine and shape the effectiveness of other areas. Goo et al argued first, security managers must ensure the support of upper management is obtained because more organisational resources are likely to become available when upper management become involved. Next, security policies must be developed and implemented in order to transform the expectations of upper management into clear, specific, and measurable security goals and objectives for organisational members. Thereafter, an organisation must focus on developing and implementing SETA programmes which help organisational members comply with security policies by both reminding them of the potential consequences of insecure behaviour and teaching them the skills necessary to perform their job roles securely. Lastly, an organisation must monitor and enforce the security behaviour of end users to ensure there are good levels of compliance with security policies throughout the organisation.

Consequently, this stusy adopts a holistic approach to the managing of information security in organisations where each of the five areas that emerged from analysing the literature will be considered equally important towards ensuring the protection of information in organisations, where no single area is described as more or less important.

2.8 Security Testing

As explained in the introduction chapter, the primary focus of this study is on the security behaviour of end users. However, this last section will focus on the security behaviour of security testers. The reason for this change of focus is because it is argued in this study that understanding how external malicious threat actors operate might help improve our understanding of various socio-organisational factors of information security, which in turn may prove useful during the development and implementation of various security controls, as this will provide organisations and security managers insight into how attackers are likely to exploit certain vulnerabilities in information security, such as those caused by the insecure behaviour of end users.

Importantly however, security researchers have stated that despite such insight into the attack patterns of cybercriminals being incredibly useful towards managing information security, such insight is incredibly difficult to obtain, as cybercriminals conduct their attacks covertly to avoid being identified and apprehended (Beebe and Rao, 2010; Seebruck, 2015; Willison and Backhouse, 2006). Of course, security researchers and practitioners can learn from previous security breaches, where forensic investigations detail how cybercriminals performed their attacks, but the skills and techniques of cybercriminals are constantly evolving, thus security researchers and practitioners need to be constantly updating their understanding of how cybercriminals attack organisations (if possible).

Therefore, it is argued in this study that improvements in our understanding of *security testing* (Bertoglio and Zorzo, 2016) may simultaneously improve our understanding of how cybercriminals attack organisations in the real world, which will provide security managers valuable regarding various kinds of attacks against organisations, which will further enable them to develop and implement appropriate security controls to ensure organisations and information are more secure. As such, the remaining section of this chapter introduces the practice of security testing, namely, network-based and physical-based penetration testing.

2.8.1 What is security testing?

There are many kinds of security testing, however in this study the term security testing will specifically refer to *penetration testing*. Penetration testing can involve both network-based and physical-based penetration testing. Further, both types of penetration testing may include aspects of *social engineering* which focuses on the ‘human elements’ rather than ‘technical elements’ of information security, as illustrated in figure 1 below.

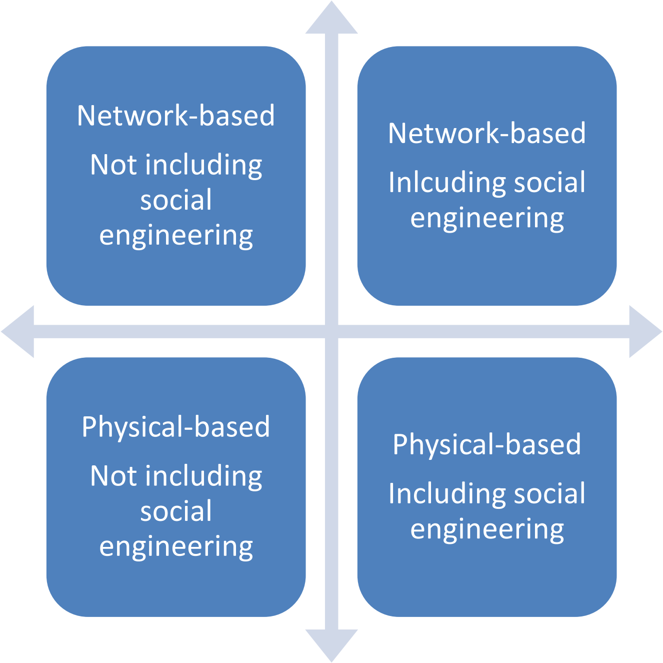
Network-based
Not including social engineering
Network-based
Inlcuding social engineering
Physical-based
Not including social engineering
Physical-based
Including social engineering

Figure 1: The Four Mains Types of Penetration Testing

For example, Dimkov et al (2010) described how a penetration test can assess both the security of an organisation's network and physical security defences. If the security tester wanted to test the security of an organisation's technical infrastructure, then the overall goal is to obtain unauthorised access and control over the organisations network. Whereas, if the security tester wanted to physically test the security of the premises wherein the technical infrastructure is located, then the overall goal is to obtain unauthorised entry into the premises. Dimkov et al (2010, p. 1) further described how both network-based and physical-based penetration testing can be "complemented with social engineering techniques, where the tester is allowed to use knowledge and help from the employees to mount the attack".

Therefore, for the purposes of this study we can understand that the overall goal for security testers is to gain unauthorised access to an organisation's information either remotely, through bypassing the organisation's network defences, or directly, through bypassing the organisation's physical defences (Thornburgh, 2004).

It should be noted that the purpose of including network-based penetration testing alongside that of physical-based penetration testing is to explore the potential socio-organisational factors which shape the overall practice of security testing. For example, although network-based penetration testing may be described as an attack against the technical infrastructure and network defences of an organisation, this will still be influenced by various socio-organisational factors, as security testers will have to determine which attacks are likely to be successful based upon the organisation, its function, and its members (including their levels of security awareness, training etc.). Furthermore, different security testers will play different roles within a network-based penetration test and such aspects of how security testers operate as a team have largely been overlooked in previous research. Therefore, it was decided that the focus should not be exclusively on physical-based penetration testing (i.e. social engineering) in this research. Both network-based and physical-based penetration testing will now be discussed.

2.8.2 Network-based penetration testing

A network-based penetration test is generally described as an authorised and controlled attempt to penetrate an organisation's network defences through the process of identifying and exploiting any vulnerabilities present within that network. Shah and Metre (2015, p. 28) defined a vulnerability as "a software or hardware bug or misconfiguration that a malicious individual can exploit" to gain unauthorised access and control over the network.

Importantly, previous studies have highlighted that security testers deliberately apply the same skills and techniques as those used by cybercriminals. This allows an organisation to develop and implement appropriate security controls to eliminate those vulnerabilities before they are exploited in the real-world (Bertoglio and Zorzo, 2016; Bishop, 2007).

There are two common approaches to classifying network-based penetration testing. The first approach divides testing into external and internal testing. When a test is conducted against 'internet-facing hosts', such as an organisation's webpage, it is considered an external test. When conducted against an organisation's 'internal host network', such as an intranet, it is considered an internal test (Bavisi, 2009).

The second approach classifies testing according to the amount of information that is provided to security testers about the organisation's network that is to be targeted during their attacks. There are three main types: black-box, white-box, and gray-box testing. Black-box testing is when security testers have no prior knowledge about the target. They are required to independently gather all the necessary information to conduct their attacks (Shah and Metre, 2015). White-box testing is when security testers are provided with all the necessary information about a target and are given privileged access to the target's network. The goal is to simulate a real-world internal threat actor like a malicious insider (Bertoglio and Zorzo, 2016). Grey-box testing represents the middle ground between black-box and white-box testing, where security testers are provided partial disclosure of information and partial access, although they can gather additional information during testing should they need to (Bavisi, 2009).

Before providing an example of how a network-based penetration test is conducted, it is important to note that security testing is described as performed in a logical and methodical fashion. For example, previous studies have described how security testing follows "a logical sequence of steps" (Bento and Bento, 2004, p. 681) where security testers recreate an 'attack sequence' where "stepping stones of chained weaknesses are combined to prove the cumulative resultant risk is real" (Yeo, 2013, p. 20). Again, the inherent value of performing security testing is it simulates the actions cybercriminals would likely have to perform in the real-world to successfully attack an organisation and to gain unauthorised access to information. As Chowdappa et al (2014, p. 3391) argued, "irrespective of ethical hacking … or malicious hacking … the hacker has to follow some steps to enter into a computer system". Thus, by improving our understanding of how security testers conduct their attacks against organisations we may simultaneously improve our understanding of how cybercriminals would likely attack them in the real-world. Which may help towards solving the problem described previously about gaining a better understanding of cybercriminal's attack patterns.

There are several models of network-based penetration testing and all describe several attack phases and/or several testing stages. The number of attack phases and testing stages vary between models but usually testing is described as having between 2-3 attack phases and/or 4-5 testing stages (Bavisi, 2009; Bento and Bento, 2004; Bertoglio and Zorzo, 2017; Shah and Metre, 2015; Yeo, 2013). The following are the five most common testing stages described in the literature:

1. *Reconnaissance*: This testing stage involves obtaining detailed information about a target organisation, such as the types of systems an organisation has and the services that are running on those systems (Bertoglio and Zorzo, 2017). This testing stage is sometimes referred to as *passive reconnaissance* because security testers gather information without coming into direct contact with the target organisation’s network. The purpose of performing in such a manner is to remain undetected by the target organisation (Bavisi, 2009; Shah and Metre, 2015)
2. *Vulnerability scanning*: This testing stage involves examining the previously identified systems and services for any security vulnerabilities (Bertoglio and Zorzo, 2017). Unlike the previous testing stage, this is sometimes referred to as *active reconnaissance* because the security tester ‘touches’ the organisation’s network, which increases the chances that they will be detected by certain security controls which will then alert the organisation that someone is ‘rattling the doorknobs’ (Bavisi, 2009).
3. *Gaining access*: This testing stage involves exploiting the identified security vulnerabilities from the previous testing stage to gain unauthorised access to and control over the target organisation’s network (Yeo, 2013). In addition, the security tester will also try to use various tools and techniques to increase the level of access and/or control they have over the organisation’s network (Bento and Bento, 2004; Naik et al, 2009).
4. *Maintaining access*: This testing stage involves making sure that the target organisation’s network remains open for future exploitation or attack (Bertogli and Zorzo, 2017). This is normally achieved by making changes to the configurations of the network and/or implementing ‘backdoors’ to ensure

security testers can regain access (Bento and Bento, 2004; Chowdappa et al, 2014).

5. *Covering tracks*: The last testing stage involves making sure to avoid detection by eliminating all traces of the security tester's presence on the organisation's network (Bavisi, 2009; Chowdappa et al, 2014).

From the above description of network-based penetration testing, it becomes clearer that security testing may present a suitable way to investigate how attacks against organisations would be conducted by cybercriminals. And furthering our understanding of how network-based penetration tests are performed would arguably improve our understanding of how security breaches occur, which will assist organisations and security mangers when developing and implementing various security controls.

In addition to improving our understanding of how organisations may be attacked by cybercriminals, network-based penetration testing has hitherto mainly been researched by computer science-related disciplines – previous studies and/or models developed are therefore very technical – and most models of network-based penetration testing have not been empirically developed. Furthermore, security researchers have argued that there has been limited research done surrounding the experiences of security testers and the challenges they might face during the performance of security testing (Xynos et al, 2010). Thus, this study addresses this issue via an in-depth social study which focuses on the experiences of security testers when conducting network-based penetration testing in organisations.

2.8.3 Physical-based penetration testing

Within the context of security testing, physical-based penetration testing is usually associated with social engineering (although physical-based penetration testing need not involve any social engineering aspects). Social engineering is generally described as using various 'persuasion techniques' to manipulate people into performing some security-related behaviour, such as allowing a person to enter a secure building or area and/or divulging sensitive information which allows a person to gain unauthorised access to an organisation's network (Workman, 2008; Luo, 2011).

Importantly, although social engineering techniques can be used during network-based penetration testing, further discussion of social engineering in this study will mainly refer to the use of social engineering techniques used in physical-based penetration tests. Further, the use of the term social engineering will be treated as interchangeable with physical-based penetration testing.

There are several ways to understand how social engineering attacks are conducted by security testers (Mouton, 2014); however, the most common way to understand them is to break them down into various ‘attack vectors’. For example, Ivaturi and Janczewski (2011) described the following four main attack vectors used during social engineering attacks:

- *Phishing*: This attack vector involves obtaining information by pretending to be a ‘trustworthy entity’ via the use of email. Generally, the security tester creates an email and sends it to the target. The email will contain some form of ‘bait’ which entices the target to visit a website that the social engineer uses to collect the inputted information. This is arguably the most common and well-known form of social engineering attack (Ivaturi and Janczewski, 2011).
- *SMSishing:* This attack vector is almost identical to that of phishing, however instead of the target receiving a fraudulent email they receive a fraudulent text message containing a link to the malicious website (Ivaturi and Janczewski, 2011).
- *Vishing*: This attack vector is like the previous two but takes place over the phone using voice as a medium. However, rather than trying to get the target to visit a malicious website the conversation will focus on getting the target to divulge information that might be of direct use to the security tester. Due to the conversation taking place in real-time this is seen to be a more difficult attack vector (Ivaturi and Janczewski, 2011).
- *Impersonation*: This attack vector is like vishing in that the security tester engages in a direct two-way conversation with the target. However, rather than

being done over the phone it is done in-person and usually on-site (Ivaturi and Janczewski, 2011).

From the above description, we can understand that the first three of the attack vectors listed by Ivaturi and Janczewksi (2011) could be classed as more 'network-based social engineering' and that impersonation attacks could be classed as more 'physical-based social engineering' (Foozy, 2011). Therefore, the first three categories of attack vectors can be understood as remotely gaining access to an organisation's information using social engineering techniques while impersonation attacks can be understood as directly gaining access to an organisation's information using social engineering techniques. Again, because this study mainly focuses on physical-based penetration testing using social engineering, it will largely discuss the process of conducting impersonation attacks against organisations.

The main reason for having this focus on impersonation attacks is that of all the attack vectors listed above, it is generally agreed by security researchers that the most challenging (both in terms of performing the attack and defending against it) is that of impersonation attacks. This is due to the direct and personal nature of impersonation attacks; as Dimkov et al (2010, p. 1) explained: "When the tester enters the facility of the organization and directly interacts with the employees … The absence of any digital medium in the communication with the employees makes the interaction … intense, especially if the employee is asked to break company policies".

When security testers conduct impersonation attacks they almost always rely on *pretexting* (Workman, 2008). Pretexting is defined as "the act of creating and using a contrived scenario to persuade a potential victim to voluntarily reveal information or perform actions" (Luo 2011, p. 4). In other words, it is the backstory which provides the security tester the justification for communicating with their target and is used to help convince the target to perform some security action(s).

When developing a pretext, security testers must consider specific characteristics relating to (1) the security testers, (2) the target (including the organisation, group, or individual person), and (3) the social context within which they will be operating. For example, pretexting can be limited by characteristics relating to the security tester's sex, age, and ethnicity – even the organisational sector can influence the types of pretexts that can be used by security testers (Workman, 2008).

In addition to pretext, social engineering attacks are often described as relying upon the 'peripheral route of persuasion'. For example, Luo (2011) described how the central route to persuasion is when security testers attempt to convince their target via logical thinking and reasoning, whereas the peripheral route to persuasion is when the security tester persuades the target through bypassing such logical thinking and triggers an emotional response instead. There are many ways in which such an emotional response may be triggered by security testers.

For example, Rush (1999) described six factors associated with the peripheral route of persuasion. First is *reciprocation* involving 'normative commitment'; where people perform certain behaviours due to various social obligations tied to those behaviours. For example, when something of value is offered to a person, such as a free sample, they may feel obligated to return the favour by making a purchase. Second is *consistency*, which is when a person becomes 'psychologically invested' in a decision they have made, therefore are more likely to continue to invest in that decision. Third is *social proof* involving 'affective commitment', where people tend to copy the behaviour of their peers, important others, and so on. Fourth is *likeability*, which is when a person complies because they trust the person or find them attractive. Fifth is *authority* involving the use of fear, where people obey commands to avoid negative consequences. And sixth, *scarcity* involving the 'principle of reactance', where people respond to a perceived shortage by placing greater value on the scarce item.

Like network-based penetration testing, social engineering attacks are described as comprising several attack phases and testing stages – although there are far fewer models developed for social engineering attacks within the literature (which highlights the need for more empirical research in this area). Nevertheless, Mouton et al (2016) described a social engineering testing framework which comprised six testing stages:

(1) *attack formulation*, where the security tester identifies both the goal and the target of the attack (2) *information gathering*, where the security tester identifies all sources of information about the target, (3) *preparation*, where the security testers combines the gathered information to develop an attack vector, (4) *develop relationship*, where the security tester establishes communication with the target and attempts to build a relationship, (5) *exploit relationship*, where the security tester exploits the previously established relationship with the target and has them either divulge information or perform the requested action, and (6) *debrief*, where the security tester debriefs the organisation and the success of the social engineering test.

From the above model described by Mouton et al (2016), we can see that social engineering testing may also present opportunities to improve our understanding of how cybercriminals may conduct social engineering attacks against organisations. Which may better enable organisations and security managers to develop and implement security controls to protect information against such attacks.

In addition, research on social engineering is severely lacking. Most research attention in penetration testing tends to be towards network-based penetration testing (although as mentioned above, this still has limitations). This creates a potentially dangerous situation for organisations, as social engineering attacks are becoming more common; as Workman (2007, p. 327) lamented, “Social engineering is a major avenue for information security breaches, yet other than anecdotal materials, there has been little to help managers address the problem”. Moreover, previous research on social engineering has mainly focused on network-based forms of social engineering attacks, such as phishing emails. Very little research has been done on how social engineering attacks, such as impersonation attacks, are conducted (Luo, 2011).

Again, because end users are often the primary targets during social engineering attacks, furthering our understanding of how social engineering tests are performed may help improve the development and implementation of security controls which are purposefully designed to manage their security behaviour, such as security policies and SETA programmes. Therefore, this study significantly contributes towards improving our understanding of how cybercriminals may attack organisations via an in-depth social study of the experiences of security testers of performing social engineering testing.

Before moving on to the next chapter it is perhaps useful to highlight how the six focus areas can be understood as part of an overall process in information security management. As stated above, the five areas of (1) upper management support, (2) information security policies, (3) SETA programmes, (4) monitoring and enforcement practices, and (5) usability of technical controls, should be considered part of a process where each area has equal importance towards determining whether information is properly protected in organisations. Furthermore, the effectiveness of any one area is greatly influenced by that of all other areas – as described by the holistic approach. Now that security testing has been discussed, it may be useful to include security testing as another potential 'critical success factor' alongside the preceding five focus areas of information security management. In other words, security testing may be conceived of as the final stage in the holistic process of managing information security in organisations.

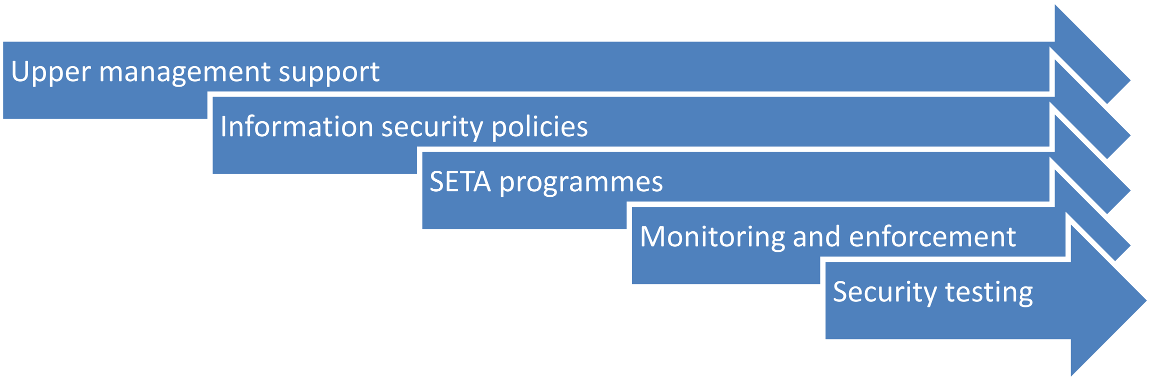

Figure 2: The Six Areas of the Holistic Approach in Information Security Management

For example, keeping in line with the previous top-down approach described by Goo et al (2015), the above figure 2 shows how an organisation may begin the security management process by obtaining upper management support to ensure both enough organisational resources are allocated to security managers and that upper management demonstrate good security behaviour. Following this, the expectations of upper management and the security goals and objectives of the organisation can become enshrined within the information security policies of the organisation. Once this has been accomplished, SETA programmes will be developed and implemented to ensure all employees are willing and capable towards protecting information in organisations. Next, an organisation will monitor and enforce security behaviour to establish high levels of compliance. Finally, an organisation may introduce security testing to determine the actual levels of protection of information and the overall effectiveness of information security efforts, where any weaknesses within the previous five focus areas can be identified and improved upon.

2.9 Summary

This chapter has discussed the nature of information security management and introduced the notion of the insider threat to organisations, namely the insecure behaviour of end users. Following this, there was a critical review of five main areas of the literature relating to end user security behaviour; namely, (1) upper management support, (2) information security policies, (3) security education, training, and awareness (SETA) programmes, (4) monitoring and enforcement practices, and (5) usability of technical security controls. Lastly, the chapter presented a discussion of the practice of security testing and how this may help organisations better understand how to protect information against attacks from cybercriminals.

3 Theoretical Framework

3.1 Introduction

The use of a theoretical or conceptual framework in qualitative social research is common practice. Their use is to provide the researcher with an ‘orienting lens’ which shapes the kinds of research questions being asked and instructs how data are collected, analysed, and presented (Bryman, 2012; Creswell, 2014).

In this chapter the theoretical framework that was used in this study will be presented and discussed, which has been developed in accordance with two widely used theories/approaches in criminology, namely the Routine Activity Approach and the Rational Choice Perspective.

Importantly, the decision to use both the Routine Activity Approach and the Rational Choice Perspective was influenced by two factors. The first being there is currently a lack of criminological theory being used in information security management research; even though cybercriminals attacking organisations, and the resulting security breaches against those organisations, are inherently crime events. Indeed, Willison (2006) argued despite the application of criminological theory potentially providing new perspectives and insights towards improving security behaviour in organisations, such application has been minimal.

Willison and Backhouse (2006) similarly argued, as information security becomes more widely recognised as a sociotechnical problem, the challenge becomes identifying which theories and concepts may prove useful towards improving the protection of information in organisations. Further stating, “If we are attempting to address computer criminals and their criminal behaviour, criminology would appear a suitable body of theory from which to draw on.” (Willison and Backhouse, 2006, p. 412)

The second factor influencing the decision over which theoretical framework to use was both the Routine Activity Approach and the Rational Choice Perspective are widely considered among the most successful theories in criminology (Cornish and Clarke, 2014; Clarke, 2010; 2017; Miro, 2014; Reyns et al, 2016). However, despite this, there has not been much application of either theory in the realm of information security management and/or cybercrime (arguably influenced by the first factor). Hence, the decision was made in this study to use both the Routine Activity Approach and the Rational Choice Perspective when investigating information security management in organisations.

3.2 The Routine Activity Approach

According to criminology scholars, the Routine Activity Approach[1] (hereafter RAA) has become one of the most tested and widely supported theories in criminology (Miro, 2014; Reyns et al, 2016). In their original formulation of RAA, Cohen and Felson (1979; 1980) described *crime events* as the product of the convergence in time and space of three criminal elements: (1) a likely offender, (2) a suitable target, and (3) the absence of capable guardians. Cohen and Felson described a likely offender as anyone with the motivation and capacity to commit a crime. Next, they described a suitable target as any person or object that may be victimised by an offender. The likelihood that a target will be considered 'suitable' by an offender was based upon four attributes: value, inertia, visibility, and accessibility (the so-called VIVA model). Value referred to the real or symbolic value placed upon a target by an offender. Inertia referred to the size, shape, and/or weight of a target which acted as obstacles for an offender. Visibility referred to the level of exposure of targets to an offender. And accessibility referred to how easily targets could be victimised by an offender. Lastly, a capable guardian[2] was described as anyone who can intervene to prevent suitable targets from being victimised (Felson and Cohen, 1980; Miro, 2014).

In the context of information security management, we can understand how the above three criminal elements may correspond with those attacks performed against organisations by cybercriminals. For example, external and internal malicious threat

[1] Often referred to as Routine Activity Theory (Cohen and Felson, 1979)

[2] It is worth noting that guardians are also referred to as 'crime controllers' in later publications due to various advancements in RAA (Vakhitova et al, 2015). However, for the purposes of this study the term guardian will be used.

actors may represent likely offenders, and an organisation's information assets may be considered suitable targets due to the inherent value of information. Lastly, individuals working for organisations may represent capable guardians, as their actions directly or indirectly determine the likelihood that information will be visible and accessible to cybercriminals (Rutger and Yar, 2016; Yar, 2005).

We can also understand from this that while the motivations and capabilities of cybercriminals, as well as the properties of information as a target, may prove useful towards understanding how security breaches may occur, the concept of guardianship deserves particular attention. Indeed, Felson (1995, p. 53) argued "A case can be made that the offender is not the most important actor for explaining crime. From the perspective of the routine activity approach … those who interfere with offenders, however inadvertently, play an even more central role in crime and its prevention". Hence, this study investigates the guardianship of information in organisations to help improve our understanding of how security breaches may occur and how to better protect information in organisations. This is achieved through an empirical qualitative research, based on semi-structured interviews, of guardianship experience of information security management in organisations.

The term guardian is used in this study to refer to three groups of actors whose security-related behaviour is argued to influence the level of protection of information in organisations. This includes *security managers*, who develop and implement various security controls in organisations to manage the security behaviour of end users; *end users*, who regularly handle organisational information as part of their everyday job role; and *security testers*, who perform network-based and physical-based penetration testing against organisations to test both the behaviour of security managers and end users towards protecting information.

It is worth noting however that while these three groups of guardians are included for investigation, the primary focus of this study is towards understanding the security behaviour of end users (as explained in previous chapters, the insecure behaviour of end users has been highlighted as a major cause of security breaches). Thus, the inclusion of security managers is to investigate how they manage the security behaviour of end users and the ways in which they try to improve their security behaviour. Similarly, inclusion of security testers is to investigate how real-world offenders may attack organisations and the ways in which organisations can prevent such attacks, in terms of improvements in the security behaviour of security managers and end users. Thus, the remainder of this section further explores the concept of guardianship as directly relating to the behaviour of end users and discusses how it will be modified and developed for use in this study.

3.2.1 The concept of guardianship

As already mentioned, guardians play a central role in crime events as RAA states crime events can only take place when likely offenders encounter suitable targets which lack capable guardians. For example, Reynald (2010, p. 359) argued "the capable guardian plays a decisive role in the crime event model … as the actors who take up the responsibility of being the ultimate protectors and defenders of any target of crime – be it people or property". Thus, this study primarily investigates the behaviour of end users in organisations and how their security behaviour influences the levels of protection of information in organisations. However, a major problem towards understanding the concept of guardianship is most previous research has taken the notion of the 'capable' guardian for granted. As such, there has been very little research towards explaining what exactly makes a guardian capable at preventing crime. This is important because the term capable guardian implies some level of motivation and/or ability to intervene to prevent crime. However, such aspects of guardianship have received little empirical investigation.

For example, Reynald (2010) argued that while previous studies have emphasised the importance of improving guardianship to prevent crime, there has been little investigation towards the underlying processes that improve the effectiveness of guardianship in practice. Thus, Reynald (2009, p. 2) stated "This elucidates the core of the issue at hand – that guardianship is a multi-dimensional concept that is affected by contextual factors that have not been appropriately considered by most of the previous studies in this area".

Hollis-Peel et al (2011) argued this lack of attention towards understanding the underlying dimensions of guardianship is because most criminological studies still focus on either the offender or the target of crimes. They argued numerous testing has been carried out utilising a wide range of theories upon the motivations of offenders as well as numerous investigations being conducted on the suitability of various targets. However, there remains "no equivalent of "guardianology" as a thorough examination of capable guardianship" (Hollis-Peel et al, 2011, p. 54). Thus, this study shares the assumption that there is a need to further improve our understanding of guardianship to better understand how to prevent various crimes, including cybercrimes.

Importantly, while there is a lack of studies which have attempted to explore the concept of guardianship, there are a select few studies which should be discussed; notably, those studies of Reynald (2009; 2010). Reynald (2009) described guardianship as a multi-dimensional concept. Reynald further described *availability* as the first dimension of guardianship based upon the original formula proposed by Cohen and Felson (1979), where the lack of presence of a capable guardian leads to crime, while presence of a capable guardian prevents it. This makes logical sense. For example, a guardian can only be considered capable at preventing a crime only if they are in some way available to intervene during the commission of that crime. Thus, Reynald (2009, p. 3) argued availability "is representative of what we conceptualize as the foundation level … of guardianship".

However, importantly, Reynald (2010) argued this is where most previous crime researchers stopped when trying to understand guardianship. Reynald claimed previous studies based upon RAA have assumed that an available guardian is someone who *automatically* performs their role as a guardian and intervenes to prevent crime. However, only when available guardians actively engage in protective actions can they truly be considered capable guardians. Thus, to fully understand guardianship we must also understand what makes a guardian actively engage in intervening to prevent crime; as mere presence alone will not guarantee this.

Consequently, Reynald (2009) argued the next dimension of capable guardianship is having the *capability* to perform the necessary protective actions to prevent the crime in question. This, again, is somewhat logical. A guardian can only be considered a capable guardian when they are able to perform the protective actions needed to prevent crime. Otherwise their intervention during the crime event would not result in the crime being prevented (although their actions may still prove disruptive). It is important to note that some crimes may only require the mere presence of a guardian to prevent them, where the capability of the guardian to perform certain actions does not influence the outcome of the crime event; as has been argued previously (Cohen and Felson, 1979). However, other crimes arguably will not be prevented by simple presence of a guardian, where guardians are required to also perform certain protective actions; as will be argued in this study.

Lastly, Reynald (2009) argued the final dimension of capable guardianship is having a *willingness* to perform protective actions. The argument being, even if a guardian is both available and capable at performing protective actions to prevent crime, this does not guarantee they will be motivated to do so. Hence, Reynald (2010, p. 386) argued "The more action a guardian is willing to take … the higher the intensity of guardianship at a place".

Overall, then, the framework surrounding guardianship as described by Reynald (2009; 2010) comprised three dimensions; availability, capability, and willingness to perform protective actions.

It is important to note that because capability forms one of the main dimensions of guardianship, this study instead refers to 'effective guardianship' or an 'effective guardian' rather than using the normal terms 'capable guardianship' or a 'capable guardian' to avoid any confusion when discussing the dimension of capability. As the term capable guardian arguably implies capability to be the most important dimension of guardianship whereas this may not be the case, given the above discussion.

Furthermore, investigation of the dimension of availability will be excluded in this study given how guardianship of information is only necessary when end users directly interact with information and therefore their availability to intervene is automatically ensured by this fact. Thus, the theoretical framework in this study describes the concept of *effective guardianship* which comprises two main dimensions: the first is having the *willingness* to perform protective actions and the second is having the *capability* to perform protective actions.

Now that the two main dimensions of effective guardianship have been outlined and discussed, it is important to further understand how either dimension may be influenced, and how each connects to the managing of information security in organisations. In other words, we must understand what factors may influence whether end users become willing and capable to protect information, and how security managers can strengthen both end user willingness and capability to intervene to protect information in organisations via security controls.

Importantly, it is assumed in this study that many factors will be important towards influencing either dimension of guardianship, and some of these factors will be more influential than others. Thus, while it is assumed that one or more of the factors discussed in the following sections will influence either dimension of effective guardianship, this study takes a qualitative/induction approach, where no factor will be assumed to be more influential. Further, this approach will allow any additional factors that influence effective guardianship that are not included within the initial framework to emerge during the research process. Thus, the various factors described below are included here as an 'orienting lens' rather than hard and fast predictions towards what will influence the willingness and/or capability of end users towards protecting information in organisations.

3.2.2 Influencing the willingness of guardians

There are numerous factors which have been described in both criminology-based and non-criminology-based studies which have potential towards explaining how end user willingness to protect information may be improved. What follows is an overview of the main factors that will be considered important for influencing the willingness of end users to protect information and how they connect to information security management.

3.2.2.1 The responsibility to perform protective actions

The first potential factor for influencing the level of willingness of end users to protect information is *having a responsibility* to act as a guardian. Felson (1995) argued that the willingness of guardians to perform protective actions is potentially influenced by their sense of responsibility to act as guardians. Further, he described four different levels of responsibility. The first level is *personal responsibility* which is taken by those who own the target or who are closely connected to target owners. The next level is *assigned responsibility* which is taken by employees who are specifically assigned to look after targets. Next is *diffuse responsibility* which is taken by other employed persons who have less precise responsibility towards protection. Felson stated this could be someone who doesn't have protection as part of their main job role but in whose normal daily work might provide some level of protection. Lastly, is *general responsibility* which is taken by bystanders or visitors whose presence may prevent crime. Importantly, Felson (1995) argued that each level of responsibility corresponded to a higher level of willingness to act as a guardian, where personal responsibility had the most influence towards motivating a guardian to intervene, and general responsibility had the least influence towards a guardian's willingness to intervene.

In the context of information security management, we can understand how the organisational responsibility of end users to protect information might then be influential toward their willingness to protect information. Further, end users may be understood to be situated somewhere between having an *assigned* and *diffuse responsibility* to protect information, because while they have an organisational responsibility to protect information, they also have additional responsibilities towards meeting primary work targets. This suggests that organisations (or more specifically security managers) may then be able to influence end user willingness by developing and implementing security policies which make end users aware of their organisational responsibilities towards protecting information. Thus, this study investigates the development and implementation of security policies (both from the perspective of security managers and end users) as potentially influencing end user willingness to protect information through communicating an organisational responsibility to protect information.

3.2.2.2 Social pressures towards performing protective actions

Another major work which provided key insight into the potential factors which influence end user willingness is that of Sampson et al (2010). Sampson et al argued guardians will be influenced to perform protective actions via various environmental factors. Interestingly, their argument is based upon the Rational Choice Perspective in criminology (discussed in more detail below), which was originally developed to explore how environmental factors influenced the decision-making of criminals (Clarke and Cornish, 1985; Cornish and Clarke, 1986; 2008). Those advocating the Rational Choice Perspective argued that offender decision-making is influenced by the efforts, risks, rewards, excuses, and provocations (or pressures) associated with committing crime. Sampson et al (2010, p. 45) have attempted to apply this same logic to that of guardianship, arguing that guardians similarly "make choices about when and how to intervene in potential and actual criminogenic circumstances based on effort, risk, reward, excuses and provocations"; where the same five mechanisms can be manipulated to improve the effectiveness of guardianship. Therefore, the main categories of the Rational Choice Perspective have been incorporated into the theoretical framework of this study as potential factors which influence both the willingness and capability of end users to act as guardians.

Of immediate relevance is the concept of *provocation*; which generally refers to when offenders experience temptation to commit a crime or feel socially pressured towards committing a crime (Clarke, 2017; Wortley, 2001). Applying this to guardianship, Sampson et al (2010) argued by reducing the levels of temptation or possible imitation towards not performing protective actions, guardianship effectiveness may be improved. In other words, guardians may be tempted to not perform protective actions or feel socially pressured towards not acting as a guardian via the expectations and observed behaviour of other guardians.

In the context of information security management, we can see how this might connect to end users being influenced by the behaviour of other organisational members (e.g., upper management) and whether they demonstrate positive or negative security behaviours, and how this might influence their willingness towards protecting information.

Interestingly, Sampson et al (2010) also argued towards the existence of *super guardians*[3] who have an especially powerful influence over normal guardians and their behaviour. Sampson et al (2010) argued super guardians do not have a direct effect on the necessary elements of crime events but can influence them indirectly through the behaviour of guardians. They posited that those who exercise the most control in organisations should be considered super guardians as they influence the everyday behaviour of employees.

Again, in the context of information security management, we can understand how upper management in organisations may represent super guardians for information as they indirectly influence the protection of information via providing security managers resources to develop and implement security controls and by promoting information security to end users (even presenting themselves as role models).

The above argument is also in line with previous research which has highlighted the potential influence of the perceived expectations and observed behaviour of upper management towards end user security behaviour (Bulgurcu et al, 2010; Hu et al, 2012; Pahnila et al, 2007; Siponen et al, 2014). Hence, the perceived expectations and observed behaviour of upper management towards information security are included within the theoretical framework of this study as potentially influencing end user willingness towards protecting information.

[3] Sampson et al (2010) used the terms controller and super controller as opposed to guardian and super guardian. However, again, for the sake of brevity and to avoid confusion the term super guardian will be used in this study to match the use of the term guardian.

3.2.2.3 Risks for failing to perform protective actions

As mentioned above, as well as highlighting that guardians may be influenced by what they see and hear around them, such as the behaviour of other guardians and super guardians, Sampson et al (2010) argued guardians will be influenced by the *risks* to guardians for failing to perform protective actions. Thus, Sampson et al argued organisations can exert influence over guardians by manipulating the perceived risks of punishment for not performing protective actions.

In the context of information security management, we can understand how this may connect to monitoring and enforcement practices in organisations, where the security behaviour of end users is monitored and any non-compliance with security policies results in punishment. Following punishment, end users may then become more willing to perform protective actions.

Again, the above argument is in line with previous literature within information security management which have argued the threat of punishment is an important factor towards influencing security behaviour (Cheng et al, 2013; Darcy et al, 2008; Knapp and Ferante, 2012; Siponen et al, 2007; von Solms and von Solms, 2004b). Thus, the risks to end users in terms of punishment are included in the theoretical framework of this study as a potential factor which influences end user willingness towards protecting information.

In addition to improving end user willingness via the risk of punishment for failing to protect information, previous studies have also highlighted that improved awareness and understanding of the general concepts and issues in information security management (e.g., security risks and security breaches) can also positively influence the security behaviour of end users. Further, such improvements are normally the result of organisations developing and implementing SETA programmes; as the awareness and education levels of SETA programmes generally aim to improve end user knowledge and understanding relating to information security management (Alshaikh et al, 2018; Abawajy, 2014; Alzamil, 2012; Chan and Mubarek, 2012).

Therefore, factors relating to end user knowledge and understanding of the risks to organisations for failing to protect information will also be included in the theoretical framework of this study alongside those risks directly related to end users for failing to protect information.

3.2.2.4 Moral pressures towards performing protective actions

As mentioned above, Sampson et al (2010) argued the same motivational factors which influence criminal behaviour may also apply to the behaviour of guardians, and one of the major factors influencing criminal behaviour (based upon the Rational Choice Perspective) is *excuses*. In general, the excuses for committing crime are closely associated with moral excuses, where criminals are more likely to perform criminal actions if they can morally excuse their behaviour (Clarke, 2010; Siponen and Vance, 2010). Thus, continuing with the idea that the same factors that influence offenders may influence guardians, this suggests that guardians will also consider moral aspects of their behaviour, where if they consider performing protective actions to be morally good then this will influence whether they perform them and vice versa (Sampson et al, 2010).

In the context of information security management, this suggests that monitoring and enforcement practices that incorporate informal sanctions alongside formal sanctions, where the moral implications of failing to protect information are highlighted to end users, may help towards improving their willingness to perform protective actions. Again, this argument is in line with previous studies which have challenged the exclusive usage of punishment-based approaches when managing information security and have argued informal sanctions are perhaps more influential (Darcy and Devaraj, 2012; D’Arcy and Herath, 2011; Son, 2011). Therefore, the moral beliefs of end users are incorporated into the theoretical framework of this study as a potential factor which influences end user willingness to protect information.

3.2.2.5 Rewards for performing protective actions

Lastly, based upon the Rational Choice Perspective which states offenders are motivated to commit certain crimes due to associated *rewards*, Sampson et al (2010) argued organisations can help improve the effectiveness of guardians by providing incentives to guardians such as rewards for performing protective actions.

In the context of information security management, this connects to monitoring and enforcement practices which incorporate the use of rewards and incentives alongside the use of punishments. This too is in line with previous studies in information security management which have highlighted that rewards may also influence security behaviour in organisations (Bulgurcu et al, 2010; Chen et el, 2012). Therefore, factors relating to rewards for good security behaviour are included in the theoretical framework of this study as potentially influencing end user willingness to perform protective actions.

Overall, we can now understand that one of the primary dimensions of effective guardianship, namely the willingness of end users to perform protective actions, may be influenced by numerous factors which are in turn influenced by the security behaviour of upper management and the various security controls developed and implemented by security managers in organisations. Again, it is not assumed that all these factors will be influential or that any one factor will be more influential. Their inclusion in this study is primarily to help guide the research process.

The figure below outlines the above discussed factors which may influence end user willingness to perform protective actions, along with their assumed pathways within information security management. In other words, it displays first the relevant focus area of information security management (e.g., upper management support, security policies etc.) and second, the corresponding willingness factor which is potentially influenced by this (e.g., social pressures, organisational responsibility etc.)

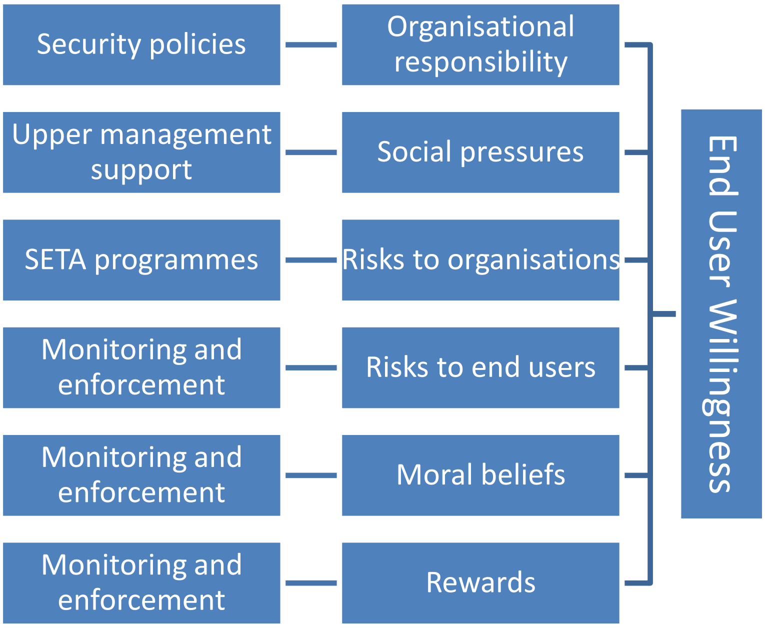

Figure 3: Potential Factors Influencing the Willingness of End Users

3.2.3 Influencing the capability of guardians

As argued above, having a willingness to perform protective actions will not guarantee effective guardianship, as guardians must also have the capability towards performing protective actions. Thus, the various factors which may influence end user capability to act as guardians will now be presented and discussed.

3.2.3.1 Knowledge and experience of performing protective actions

Reynald (2010) argued that having the right levels of knowledge and experience is essential towards having a capability to act as a guardian. For example, Reynald (2010) argued for residential home owners, an essential part of being a capable guardian was having a basic understanding about the types of people and behaviour that should be considered normal or typical in certain local community areas and how to properly intervene when necessary. Thus, Reynald (2010, p. 361) argued that “It seems intuitive to surmise that the more experience and knowledge guardians have … the more confident they will be about their capability”.

In the context of information security management, we can understand how knowledge and experience of guardians may relate to SETA programmes. As explained above, understanding various security risks to organisations may influence end user willingness to intervene (which arguably connects to the awareness and education levels of SETA programmes). However, this does not necessarily mean that end users will be capable at performing the required protective actions, only that they are willing to perform them. Thus, the training level of SETA programmes which instructs end users on how to perform certain protective actions may also be an important part of making sure they are effective guardians. For example, security training programmes can instruct end users how to spot a phishing email; how to encrypt an email; how to create a secure password, which in turn enables them to better protect information (Alshaikh et al, 2018; Chan and Mubarek, 2012; Manke and Winkler, 2012; Peltier, 2005). Thus, the knowledge and experience of end users towards performing security actions are also included in the theoretical framework of this study as potential factors which influences the capability of end users to protect information.

3.2.3.2 The usability of technical security controls

Continuing with the argument made by Sampson et al (2010) that the same motivations that influence offenders will influence guardians, the last remaining category of the Rational Choice Perspective is the associated effort to perform certain actions, where if certain actions require too much effort to perform them, guardians will become less capable at performing them, which in turn may also influence their level of willingness to perform them. Thus, there is an interactive effect between the capability and willingness of guardians via the required effort and time to perform certain actions.

In addition, Felson (1995) argued that design factors can potentially influence the capability of guardians by impacting upon the required effort and time to perform certain protective actions. For example, Felson (1995, p. 62) described various ‘tools of prevention’ and how design factors may influence their effectiveness (i.e., their usability), claiming “a jewelry clerk may benefit by having a mirror to watch the merchandise and a button to summon supervisory help. However, neither are important if these tools of prevention are badly placed and cannot assist those involved in discouragement”.

In the context of information security management, we can understand how this potentially connects to the usability aspects of various technical security controls, where the more usable a technical security control is from the perspective of end users, the less time and effort that is required when performing protective actions (Furnell, 2005; Kainda et al, 2010; Renaud and Flowerday, 2017). Consequently, this may then improve the capability of end users which, in turn, may also result in improved willingness to protect information. Therefore, the usability of technical security controls is also included in the theoretical framework of this study as a potential factor which influences effective guardianship via the capability and willingness of end users.

Overall, we can understand that one of the primary dimensions of effective guardianship, namely the capability of guardians to perform protective actions, may be influenced by several factors, which in turn may be influenced by the SETA programmes developed and implemented by security managers in organisations, as well as design factors relating to technical security controls.

The figure below outlines the above discussed factors which may influence end user capability to perform protective actions, along with their assumed pathways within information security management. In other words, it displays first the relevant focus area of information security management (e.g., SETA programmes and usability of technical controls) and second, the corresponding willingness factor which is potentially influenced by this (knowledge and experience and time and effort).

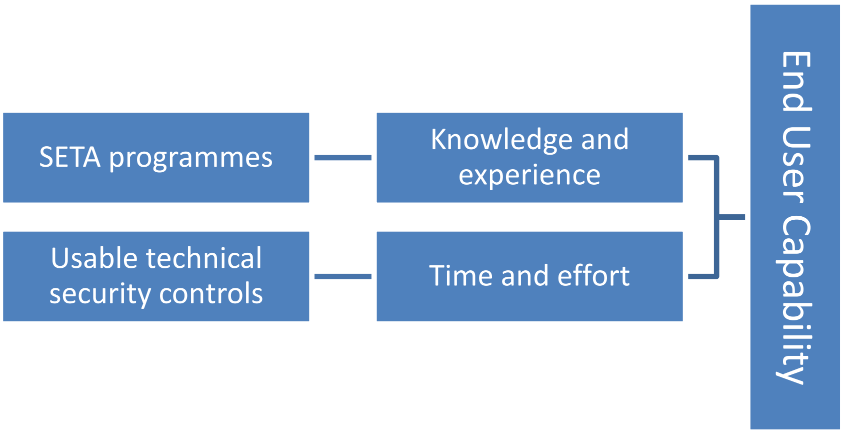

Figure 4: Potential Factors Influencing the Capability of End Users

3.3 The Rational Choice Perspective

As discussed in the previous chapter, this study argues that investigation of security testing may help improve our understanding of how cybercriminals perform their attacks in the real world, as security testing involves simulating real-world attacks against organisations; which may then help organisations improve the protection of information by highlighting areas of improvement in the behaviour of security managers and end users. Therefore, this next section discusses the Rational Choice Perspective and the associated concept of crime scripts and how each will be incorporated into the theoretical framework of this study.

As mentioned above, the Rational Choice Perspective (hereafter RCP) states offenders are influenced by the efforts, risks, rewards, provocations, and excuses for committing crime. The overall goal of RCP is to support that of *situational crime prevention*, which is an approach to crime prevention which utilises tailor-made crime prevention measures (referred to as *opportunity reducing techniques*) that can be put in place to ‘tip the balance’ in favour of criminals refraining from committing crime (Cornish and Clarke, 2014; Clarke, 2010; 2017). Importantly, RCP makes several assumptions about offender decision-making that are important to this study, as it will be argued the same decision-making may occur when security testers perform security testing.

The first assumption is that offenders seek to benefit themselves by committing crime. The benefits of committing crime are numerous and vary between offenders. They can relate to money, sexual gratification, revenge, thrill-seeking, and so on. In addition, offenders are assumed to try and select the best available means to achieve their goal(s). Thus, according to RCP, criminal behaviour is essentially goal-oriented. However, offenders are described as having a 'bounded rationality' where their decision-making is "constrained by limits of time and ability and availability of relevant information" (Cornish and Clarke, 2014, p. 1). Thus, offenders are not considered to possess perfect rationality.

The second assumption is that a crime-specific approach is required to understand crime because different crimes will serve different needs, and different situations will offer different opportunities for offenders to satisfy those needs. Hence the use of tailor-made, opportunity-reducing techniques to try and reduce the opportunities present in any given situation (Cornish and Clarke, 2014; 2017).

Lastly, decision-making is assumed to be of two kinds: *involvement* decisions, which refers to the decisions made by offenders to become involved in crime; and *event* decisions, which refers to the decisions made by offenders prior to, during, and after the commission of a crime (Cornish and Clarke, 2014; 2017).

In the context of information security management, we can understand how RCP may prove useful towards investigating security testing as security testers are described as deliberately applying the same skills and techniques as those used by cybercriminals, so that organisations can then assess their level of risk against such cybercriminals performing various kinds of attacks in the real-world (Bertoglio and Zorzo, 2016; Shah and Metre, 2015). Further, we may understand that security testers, when performing either network-based or physical-based penetration testing, will have certain goals tied to individual tests (e.g., gain unauthorised access to an organisation's information) and will seek to use the best available means at their disposal to achieve their goals.

Importantly, an offshoot of RCP has been the development of *crime scripts* which are designed to help researchers better understand how offenders commit various crimes, which should enable them to better design ways to prevent them from occurring in the real-world. Thus, this next section introduces the concept of crime scripts.

3.3.1 Crime scripts

As mentioned above, the purpose of the Rational Choice Perspective and Situational Crime Prevention is to understand offender decision-making and how various situational factors influence the commission of crime to help develop ways to prevent crime. Further, decision-making is split into two categories, involvement decisions and event decisions. Of relevance here are event decisions; those decisions made by offenders prior to, during, and after the commission of a crime. Again, the purpose of understanding how crimes are committed is to enable practitioners to develop measures that will discourage offenders from committing crime, through manipulating the efforts, risks, rewards, provocations, and excuses for committing a crime. However, a major challenge for practitioners who adopt this approach to crime prevention is understanding exactly how crimes are committed, and where best to implement such opportunity-reducing measures during the crime commission process (Haelterman, 2016). For example, Cornish (1994, p. 160) argued that a major requirement of crime prevention is becoming familiar with the 'procedural aspects of crime', stating that "With the advent of situational crime prevention, the need for detailed crime-commission information has become more widely recognized". To help resolve this problem, Cornish (1994) developed *crime scripts*.

Cornish (1994, p. 175) described crime scripts as a useful way towards understanding the procedural aspects of crime, where "they emphasize the form of crime as a dynamic, sequential, contingent, improvised activity, and the content of specific crimes, considered as activities with particular requirements in terms of actions, casts, props, and spatio-temporal locations". Thus, the overall purpose of using crime scripts to investigate crime is to describe in rich detail every stage of the crime-commission process, the decisions and actions that must be made by offenders for each stage (including the goals and objectives for each) and the required resources, such as criminal cast, tools and equipment for effective action during these stages; which can then be used to help develop more effective ways to prevent crime (Cornish and Clarke, 2017).

In the context of information security management, this highlights the potential for using crime scripts to investigate the security testing activities of network-based and physical-based penetration testing as a means towards improving our understanding of how cybercriminals are likely to perform their attacks, as the attack methods and decision-making involved in real-world attacks against organisations are similarly involved during that of penetration testing (Bertoglio and Zorzo, 2016; Bishop, 2007; Shah and Metre, 2015). Therefore, to better understand how security testers perform security testing we can adopt an approach which focuses attention on those decisions made prior to, during, and after a network-based or physical-based penetration test.

3.3.1.1 The universal crime-script

In addition to developing the concept of crime scripts to help crime researchers investigate how crimes are committed, Cornish (1994) also developed the *universal crime script*, which essentially consists of standardised scenes arranged into a sequential order and offers guidelines for researchers when investigating any type of crime. For example, Cornish (1994) described the following stages that might unfold during the commission of a crime:

> Preparations, often made outside the crime setting, are followed by entry to the setting, and the awaiting, or establishment, of conditions under which the crime in question can be committed. Various instrumental actions then occur, to be followed by the consummately activities which comprise the main action. Actions associated with the aftermath of the main action then follow and, lastly, the players exit from the crime scene. (Cornish, 1994, p. 162*)*

Thus, the main stages outlined as part of the universal crime script presented by Cornish (1994) may prove a useful way of approaching the task of investigating the commission process of both network-based and physical-based penetration testing.

Importantly, in addition to breaking down the crime commission process into various main stages, Cornish (1994) also described how each stage of the universal crime script can be divided up into smaller units of action that are required to achieve various sub-goals. For example, Haelterman (2016, p. 136) argued "in procedural crime scripts, the actions of an offender are considered to be essentially goal oriented … It is important, therefore, to gather as much detail as possible on the offender's … goals and the hierarchy thereof". Therefore, when using the crime script approach in this study there will be a focus towards identifying not only each main stage of performing security testing but also the various goals and sub-goals of each stage.

In addition, Cornish (1994) highlighted when using crime scripts, crime researchers must try to identify the 'procedural requirements' of committing certain crimes. For example, Cornish (1994) argued committing certain types of crime will place various demands upon offenders in terms of *casting*. Casting refers to matching certain types of crime commission to those offenders who possess the appropriate motives and skills required to perform them. Haelterman (2016, p. 135) similarly argued "When listing the various actors involved in the crime-commission process, it is equally important to try and gather insight on their specific roles, skills, and competences". Thus, when using the crime script approach to investigate security testing, this study looks at how certain types of security testing and the different stages therein place procedural requirements on security testers in terms of their skills and abilities.

Lastly, the crime-script approach involves investigating various *props* or tools used during crime commission, as these will also influence whether an offender can successfully complete a stage or perform certain actions during any given stage (Cornish, 1994). For example, Haelterman (2016, p. 135) argued "In coping with or exploiting situational contingencies, offenders may require the possession and use of particular tools. It is important, therefore, to capture detail on the tools that are gathered and used to progress certain actions during crime commission, as this may provide valuable input for the design of future controls". Thus, when using the crime-script approach for investigating security testing there will also be a focus on understanding the various tools and tactics used by security testers during both network-based and physical-based penetration testing and how they influence the successful completion of the penetration test.

3.4 Summary

This chapter has presented the theoretical framework that was used in this study, which was developed in accordance with the Routine Activity Approach and the Rational Choice Perspective. The Routine Activity Approach introduced the concept of guardianship as an essential element of crime events. Further, the concept of guardianship was described above as comprising two main elements, the willingness and capability to intervene to protect information, which were further described as potentially being influenced by numerous socio-organisational factors connected to information security management. In addition, the Rational Choice Perspective introduced the concept of crime-scripts, which were described as a useful framework for breaking down crime events into separate stages in order to explore various goals and sub-goals, as well as accompanying actor roles and actions required for each stage.

4 Research Methodology and Methods

4.1 Introduction

This chapter presents and discusses the various choices that were made regarding both the research methodology and research methods used in this study. The chapter is therefore split into two main parts. The first part presents and discusses the research methodology; namely, the research paradigm, research strategy, and research design. The second part presents and discusses the research methods; namely, participant selection, data collection, data analysis and quality criterion of qualitative research.

4.2 Research Paradigm

Any approach for conducting social research should discuss not only of the procedures of sampling, data collection, and data analysis, but also the various research paradigms that exist within social science (Bryman, 2012; Holloway and Wheeler, 2002; Saunders et al, 2007). This is because each research paradigm has different assumptions about the way researchers should study the social world and these assumptions will underpin the research strategy, research design, and the research methods chosen for conducting social research (Fossy et al, 2002; Ponterotto, 2005). For example, Ponterotto (2005, p. 128) stated "The paradigm selected guides the researcher in philosophical assumptions about the research and in the selection of tools, instruments, participants, and methods used in the study".

Two dominant research paradigms in social science are *positivism* and *interpretivism (*Bryman, 2012; Holloway and Wheeler, 2002). Both have major epistemological assumptions relating to the development of knowledge about the social world which are important to social research. According to Saunders et al (2007), in the context of social research the key epistemological question is whether an approach to the study of the social world can be the same as an approach to the study of the natural world. Those who advocate positivism agree that the methods of the natural sciences can be applied in the social sciences, while those who advocate interpretivism reject this. They generally argue the subject matter of the social sciences is fundamentally different from that of the natural sciences. Therefore, the study of the social world requires a different approach (Bryman, 2012; Fossey et al, 2002; Sale et al, 2002).

For example, Antwi and Hamza (2015) argued, at the epistemological level, positivism views social science as a highly organised method combining deductive logic with empirical observation to discover and confirm probabilistic causal laws that can then be used to predict general patterns of human behaviour. In contrast, interpretivism views the world as socially constructed, interpreted, and experienced by individuals during their interactions with each other and within wider social systems. Thus, according to interpretivists, the nature of social inquiry is fundamentally interpretive, and the goal is to understand certain phenomena rather than to generalise to a specific population. Hence, researchers within the interpretivist paradigm are considered naturalistic, since they investigate real-world situations as they naturally unfold.

The interpretivist research paradigm is often associated with Weber's *Verstehen* approach to social research, which focuses upon the ways in which human beings come to understand and make sense of their social world and attach meaning to it (Holloway and Wheeler, 2002; Ormston et al, 2013; Thanh and Thanh, 2015). Thus, the researcher attempts to "gain access to people's 'common-sense thinking' and hence to interpret their actions and their social world from *their point of view*" (Bryman 2012, p. 30).

As explained in previous chapters, the purpose of this study is to describe information security management within organisations from the point-of-view of three groups of guardians. Therefore, adopting an interpretive research paradigm was deemed most suited to this type of investigation.

4.3 Research Strategy

Following the decision to use an interpretive research paradigm, the decision of what research strategy to use was made. Bryman (2012, p. 35) defined a research strategy as “a general orientation to the conduct of social research”. There are two major research strategies in social science: *quantitative* and *qualitative*.

Quantitative research is a research strategy that focuses on quantification in the collection and analysis of data. It necessitates a deductive approach to the relationship between theory and research and advocates the methods of the natural sciences (i.e., positivism) (Bryman, 2012; Ponterotto, 2005; Sale et al, 2002). For example, Ponterotto (2005, p. 128) stated the “quantitative methods focus on the strict quantification of observations (data) and on careful control of empirical variables. Quantitative research often incorporates largescale sampling and the use of statistical procedures to examine group means and variances”.

In contrast, qualitative research is a research strategy that focuses on ‘words instead of numbers’ in the collection and analysis of data. It necessitates an inductive approach to the relationship between theory and research and rejects the methods of the natural sciences, favouring interpretivism instead (Bryman, 2012; Fossy et al, 2002; Vaismoradi et al, 2013). For example, Vaismoradi et al (2013, p. 398) claimed the main characteristics of qualitative methodologies are “An approach to in-depth understanding of the phenomena, a commitment to participants’ viewpoints, conducting inquiries with the minimum disruption to the natural context of the phenomenon, and reporting findings in a literary style rich in participant commentaries”. Thus, we can understand that qualitative research is a broad umbrella term for research methodologies that describe and explain individual experiences, behaviours, interactions, and social contexts without resorting to the use of statistical procedures or quantification (Fossy et al, 2002).

As mentioned above, this study was situated within an interpretivist research paradigm to enable in-depth understanding of the experiences of guardians towards information security management in organisations. Because of this, a qualitative research strategy was also deemed most suited for this study. This decision was supported by recommendations from social research scholars. For example, Thanh and

Thanh (2015, p. 26) argued if a researcher seeks “understandings and experiences of a group … qualitative methods are likely to be the best-suited methods”.

4.4 Research Design

Following the decision to use a qualitative research strategy, the decision toward what research design should be used was made. Bryman (2012, p. 45) described research design as “a structure that guides the execution of a research method and the analysis of the subsequent data”. In other words, the research design influences where data should be collected, how it should be collected, and how the data should be analysed.

Within both interpretivist and qualitative social research, a major influence has been that of phenomenology. Langdridge (2007, p. 4) defined phenomenology as a research approach that focuses on “people's perceptions of the world in which they live in and what it means to them; a focus on people's lived experience”. Importantly, scholars have highlighted that phenomenology is an umbrella term which encompasses both a philosophical movement as well as a range of research approaches. Thus, scholars have argued that phenomenologists are often extremely diverse in their interpretations of the core issues of phenomenology and what they consider to be the phenomenological approach to social research (Creswell, 2007; Finlay, 2009; Kafle, 2011). For example, Finlay (2009, p. 10) stated that “While all phenomenology is descriptive in the sense of aiming to describe rather than explain, a number of scholars and researchers distinguish between descriptive phenomenology versus interpretive, or hermeneutic, phenomenology”. Although Finlay argued that many scholars, herself included, considered the notions of description and interpretation as a continuum, where specific investigations may be more interpretive than others.

Notwithstanding existing disagreements over what should be considered truly ‘phenomenological’, Finlay (2009, p. 6) claimed that “Phenomenological researchers generally agree that our central concern is to return to embodied, experiential meanings. We aim for fresh, complex, rich descriptions of a phenomenon as it is concretely lived”.

It should be highlighted, that the use of a theoretical framework is somewhat uncommon in phenomenology-based studies due to the influence that a theoretical framework may have upon data analysis. For example, there is a danger that the use of a theoretical framework may draw the attention of the researcher away from how participants themselves describe their experiences (which would constitute a more bottom-up approach) to concentrate more on how such experiences correspond with the associated concepts that make up the theoretical framework (a more top-down approach). However, as already discussed in the previous chapter, the use of a theoretical framework in this study was only to provide the researcher direction towards the different focus areas of information security management that should be explored with participants. For example, the theoretical framework helped the researcher identify potentially important areas within information security management (e.g., upper management support, security policies) which may influence the willingness and/or capability of end users to protect information, which would then prove important towards answering the research question. Thus, when investigating these specific areas, efforts were made to 'stay with the experiences' of those participants to better understand how various socio-organisational factors shaped their experiences of these different areas, rather than having a focus towards connecting these experiences back to those factors outlined in theoretical framework.

Therefore, the research design used in this study is referred to as a phenomenology-inspired investigation of guardianship experiences rather than a thoroughbred phenomenological investigation, where the research design can be suitably located within any one camp. Nevertheless, extreme consideration was made towards developing the research design based upon the recommendations of social research experts of how phenomenology-based studies should be conducted. As a result, the following major steps described by scholars in relation to phenomenology-based investigations were adhered to in this study.

The first major step in a phenomenology-based investigation is to identify a phenomenon to study (Creswell, 2007; Moustakas, 1994; Todres and Holloway, 2004). For example, Todres and Holloway (2004) argued the first step in a phenomenological study involves the researcher deciding upon an experiential phenomenon of interest, which necessitates the researcher making it explicit the interest and agenda of the study. Therefore, as explained in the introduction chapter, the chosen phenomenon for investigation in this study is the experiences of three groups of guardians towards the managing of information security in organisations. Further, the primary focus is towards how various socio-organisational factors shape their experiences. The reason for this investigation is to help address the issue of security breaches in organisations. Further, various socio-organisational factors have often been overlooked in previous studies.

The second major step in a phenomenology-based investigation is for the researcher to 'bracket out' their own experiences of the chosen phenomenon (Creswell, 2007; Moustakas, 1994; Finlay, 2009). For example, Finlay (2009, p. 12) described the 'phenomenological attitude', where the researcher "strives to be open to the "other" and to attempt to see the world freshly, in a different way". Therefore, for this study, efforts were made to limit the influence of any preconceived notions of how various socio-organisational factors may shape the experiences of guardians of information security management in organisations. As explained previously, while there are numerous factors outlined in the theoretical framework developed for this study, there were no assumptions made toward whether such factors would be influential towards influencing the willingness and/or capability of end users towards protecting information, nor were there any assumptions made about which factors would be more influential. Their inclusion is primarily to help guide the research process rather than dictate it.

The third major step in a phenomenology-based investigation is to collect data from those who have experienced the phenomenon under investigation (Creswell, 2007; Moustakas, 1994; Todres and Holloway, 2004). For example, Todres and Holloway (2004, p. 86) argued that the researcher must ensure to collect "descriptions of others' experiences that are concrete occasions of this phenomenon". Further, to achieve this, the researcher "must use open-ended and 'experience-near' questions that invite participants to speak about their lived experiences in relation to the phenomena under study”. More details will be provided below on how the present study used in-depth interviews when collecting data about participants’ experiences.

The fourth major step in a phenomenology-based investigation is the researcher then analyses the data by reducing the information to ‘significant statements’ and combines these statements into themes which capture some important aspects about participants’ experiences (Creswell, 2007; Moustakas, 1994). Again, this will be discussed in more detail below in the section on data analysis and the use of thematic analysis.

The fifth and final major step in a phenomenology-based investigation is the researcher develops a composite description of the experiences of the participants (Creswell, 2007; Moustakas, 1994; Todres and Holloway, 2004). For example, Creswell (2007) described how the developed themes and accompanying significant statements from the previous step are used to write both a description of what the participants experienced (referred to as *textural description*) and the context or setting that influenced how the participants experienced the phenomenon, referred to as *imaginative variation* or *structural description.*

Pietkiewicz and Smith (2014) similarly described how the previous step leads to writing a narrative account of the study. This usually involves taking the themes identified and writing them up one by one. Each theme needs to be described and exemplified with various extracts from interviews, and may be followed by various interpretations and analytic comments from the researcher. The decision to include extracts of participants’ experiences serves two functions. First, it enables the reader to assess the relevance and importance of the interpretations. Second, it allows the voices of the participants to remain the driving force behind the research process. Thus, the final paper should include both the participant’s account of his or her experience in his or her own words, and interpretative commentary from the researcher.

4.5 Research Method

Following the decisions made surrounding research methodology were the various decisions that had to be made regarding research methods. According to Wahyuni (2012, p. 72), a research method “consists of a set of specific procedures, tools and techniques to gather and analyse data … In other words, a method is a practical application of doing research whereas a methodology is the theoretical and ideological foundation of a method". Therefore, the research methods adopted in this study will now be presented and discussed, namely, participant selection, data collection and analysis, and quality criterion in qualitative research.

4.5.1 Participant Selection

Coyne (1997) highlighted the importance of *appropriateness* when sampling participants due the profound impact this has on the quality of social research. Coyne (1997, p. 623) recommended that researchers try to sample participants who are "articulate, reflective, and willing to share" during their participation. Therefore, a sampling design was selected for use in this study to ensure appropriateness of sampling was achieved.

4.5.1.1 Sampling Design

Onwuegbuzie and Leech (2007) described sampling design as the framework within which the sampling occurs, which typically includes *sampling schemes* and *sample size*. Regarding sampling schemes, Onwuegbuzie and Leech (2007) described two major sampling schemes: *random* sampling schemes (i.e., probabilistic sampling) and *non-random* sampling schemes (i.e., non-probabilistic sampling). Onwuegbuzie and Leech further argued that if the goal is not to generalise but to obtain insight into a given phenomenon, then the researcher should *purposefully* select individuals, groups, and settings which increases their understanding of the chosen phenomena. Creswell (2007, p. 125) similarly described how purposive sampling in qualitative research "means that the inquirer selects individuals and sites for study because they can purposefully inform an understanding of the research problem and central phenomenon in the study".

Based upon the previous choices made surrounding research paradigm, research strategy, and research design, a purposive sampling scheme was selected for use in this study, where participants were selected primarily on the basis that they have all experienced the phenomenon under investigation and were considered to meet specific criterion. It is important to note, because organisations differ in terms of their size, operations, resources, and security requirements, where guardianship experiences of information security management will be greatly influenced by this, efforts were made in this study to recruit participants from a wide range of organisations in order to try and capture this diversity surrounding guardianship experience. As mentioned previously, there were three groups of participants included in this study; security managers, end users, and security testers, where each group of participants represented a different vantage point towards information security management in organisations.

In addition, while participants were recruited from a diverse range of backgrounds and had differing levels of experience drawn from a wide range of organisations, it was not possible to provide more details regarding participants due to general concerns participants had regarding privacy and security. Indeed, many participants agreed only to take part in this research project on the basis that no specific details be taken regarding their current job role and/or their employer. It was decided that while such details are normally included, the benefits of having a larger pool of participants outweighed that of having a shorter participant pool with more specific details being provided.

The first group of participants were security managers, who experienced guardianship by managing an organisation's information security. To ensure appropriate sampling of security managers, the following inclusion criterion were used: (1) the participants must have experienced the managing of information security in organisations, and (2) assisted organisations in developing and implementing security controls to manage the security behaviour of end users. There was no exclusion criterion based upon age, sex, nationality, ethnicity, etc.

The second group of participants were end users who experienced guardianship primarily by using an organisation's security controls. To ensure appropriate sampling of end users, the following inclusion criterion were used: (1) the participants must have experienced information security management in organisations, (2) the participants must have had access to and regularly used information and information systems as part of their everyday job role, (3) the participants must be required to protect said information and information systems, and (4) the participants must have experienced using various security controls. There was no exclusion criterion based upon age, sex, nationality, ethnicity, etc.

The third group of participants were security testers, who experienced guardianship by testing the level of protection of information in organisations via the practice of security testing. To ensure appropriate sampling of security testers, the following inclusion criterion were used: (1) the participants must have experienced security testing in organisations, either through network-based or physical-based penetration testing. There was no exclusion criterion based on age, sex, nationality, ethnicity, etc.

Following the decision to use a purposive sampling scheme, the decision toward what sample size should be used was made. Sample size simply refers to the number of participants that will take part in a study. Although qualitative social research typically involves smaller sample sizes compared to quantitative social research, the choice of sample size is still an important consideration. For example, Onwuegbuzie and Leech (2007) described how sample size in qualitative research should not be too large that it becomes difficult to collect 'thick, rich data', but not too small that it becomes difficult to achieve 'data saturation'. Cleary et al (2014, p. 473) similarly described how "too few may risk adequate depth and breadth, but too many may produce superficial or unwieldy volumes of data".

Given the importance of sample size, the recommendations of Marshall et al (2013) were followed in this study. The following three methods were described by Marshal et al (2013) that can be used to justify sample size in qualitative research:

1. To cite recommendations by qualitative methodologists.
2. To adopt the sample sizes used in similar studies.
3. To use 'internal justification', which involves saturation within the dataset.

Therefore, to assist the decision of sample size in this study, the first move was to consult previous studies. However, because there were few studies which have investigated the experiences of guardians in information security management, there were few studies with which to consult. Although, one study was deemed suitable due to the inclusion of one of the three groups of participants connected with this study and is frequently referenced in information security management literature. Albrechtsen (2007) conducted 18 interviews when investigating end user experiences of information security management. Thus, an original target was set for recruiting 18 participants for each group of participants (i.e., 18 security managers, 18 end users, and 18 security testers).

In addition, the principle of 'data saturation' was used to help the researcher determine whether further participants should be recruited during this study. Marshall et al (2013, p. 11) described data saturation as when "the researcher gathers data to the point of diminishing returns, when nothing new is being added". In other words, data saturation typically occurs when all interview questions have been thoroughly explored and no new concepts or themes emerge from the data (Cleary et al, 2014). Therefore, the sample size of the three groups of participants in this study was also determined via the principle of data saturation.

Importantly, because there was an initial problem with gaining in-depth and detailed descriptions from certain participants about their experiences of information security management, the initial target for recruiting 18 participants was extended until data saturation was considered to have been reached. Consequently, there were 86 participants recruited in total for this study. The 86 participants were broken down into: 34 security managers (19 male, 15 female); 28 end users (8 male, 20 female); and, 24 security testers (16 male, 8 female).

Following the decisions of sample scheme and sample size, the next action was to actually source participants. In this study, various sourcing techniques were used as recommended by Robinson (2014). The first sourcing technique was advertisement through social media. Three social media platforms were used, namely, Twitter, LinkedIn, and Facebook. Initially, a Twitter account was created, and followers were gained for the Twitter page. Once large numbers of followers had been achieved, the Twitter page was used to advertise the study to them. Those who had an interest in participating were then able to comment on the advertisement. There was also the possibility that followers would re-post the advertisement on their own Twitter page, thus extending the reach of the advertisement.

Following this, a LinkedIn account was created to advertise the study on the provided ‘news feed’ and to directly communicate with potential participants. For example, having a ‘LinkedIn premium’ membership allows users to send direct messages to other LinkedIn users, regardless of their relationship status. Therefore, this enabled direct communication with potential participants where each participant received a message that described the study along with a request for their participation. After a reply of interest, the participant was provided with additional details about the study.

Lastly, a Facebook profile was created and used to advertise the study. As with previous social media accounts, this involved advertising the study on the provided ‘news feed’ where those interested in participating were able to leave a comment or send a private message expressing their interest.

The second sourcing technique that was used in this study was to recruit a *research champion*. A research champion is someone who will actively help with advertising the study and encourage participation (Robinson, 2014). There were two research champions recruited in this study. The first was a member of the first group of participants, namely security managers. Because of the wide recognition of the research champion within the field of information security, they were able to assist in recruiting participants by posting advertisements on social media with their recommendation towards taking part. This proved to be highly effective at recruiting participants. The second research champion was a member of the second group of participants, namely end users. Following their participation in the study, they were able to successfully recruit an additional 10 participants.

The third sourcing technique that was used in this study was to use *referral chains*. This sourcing technique involves asking participants for recommendations of any person who might qualify for participation in the study (Robinson, 2014). Again, this proved highly effective as participants were often able to provide such recommendations.

Importantly, when sourcing participants, Robinson (2014, p. 35) argued that each must be made aware of "the study's aims, of what participation entails, of its voluntary nature, of how anonymity is protected and any other information that will help them reach an informed, consensual decision to participate". Therefore, each participant that was involved in this study received a *participant information sheet* (see appendix) which included relevant details about the study, what participation involved, the voluntary nature of the study, how to withdraw from the study, the anonymous nature of the study, and how to directly contact the researcher about the study. In addition, participants were required to complete a *participant consent form* (see appendix) which acknowledged they had received enough time to read through and understood the participant information sheet and that they were able to ask any questions they might have had about the study.

4.5.2 Data Collection

This next section outlines the process of data collection via the use of in-depth interviews. The development of interview guides and procedures adopted during data collection will also be presented and discussed.

4.5.2.1 In-depth interviews

Data collection in interpretive/qualitative/phenomenology-based investigations often involves the use of in-depth interviews. For example, Pietkiewicz and Smith (2014) argued because the main concern of qualitative research is to elicit rich, detailed, and first-person accounts of experiences connected to the phenomenon under investigation, then in-depth, one-on-one interviews are considered the most effective method to achieve that. Further, there are generally three types of in-depth interviews described in the literature: unstructured, semi-structured, and structured interviews (Bloom and Crabtree, 2006)

In unstructured interviews, the researcher relies primarily on interactions with the participant to guide the interview process, rather than asking specific questions in a specific order – where all must be asked and answered. Semi-structured interviews are more structured than unstructured interviews (as the name implies), although still have some flexibility in terms of questions asked and question ordering (Turner, 2010). Further, semi-structured interviews are considered the most widely used interviewing format for qualitative social research (Bloom and Crabtree, 2006) and tend to involve the use of an interview guide. The advantages of using interview guides are they "ensure that the same general areas of information are collected from each interviewee … but still allows a degree of freedom and adaptability in getting information from the interviewee" (Turner, 2010, p. 756). Lastly, structured interviews are very structured in terms of the order and wording of questions, which reduces the amount of flexibility the researcher has during interviews.

Due to the present study being qualitative, where an inductive approach was taken towards investigating the experiences of guardians of information security management in organisations, semi-structured interviews were considered the best option for data collection.

4.5.2.2 Interview guides

As mentioned above, semi-structured interviews usually involve the use of an interview guide (Bloom and Crabtree, 2006; Turner, 2010). Turner (2010) described how creating an interview guide with effective interview questions can be one of the most important aspects of using interviews for data collection. Turner (2010, p. 757) recommended researchers who conduct in-depth interviews should make sure that "each of the questions will allow the examiner to dig deep into the experiences and/or knowledge of the participants in order to gain maximum data". Thus, the following list of recommendations, as described by Turner (2010), were followed when developing interview guides:

- Questions should be open-ended (respondents were able to choose their own terms when answering questions);
- Questions should be neutral (efforts were made to avoid any wording that might influence a respondent’s answer, e.g., leading questions);
- Questions should be asked one at a time; and
- Questions should be clearly worded;

In total, three interview guides were developed for use in this study, one for each of the three groups of guardians (see appendix E, F, and G).

When developing interview guides, the author chose to structure the questions being asked in interviews around the six focus areas of information security management that were discussed in the literature review chapter. Of course, depending on which group was being interviewed (i.e., security managers, end users, security testers), this would determine which of the main areas were discussed during the interview.

For example, when interviewing security managers, questions were focused towards eliciting experiences of managing the security behaviour of end users through things like developing and implementing security policies and SETA programmes. Example questions include:

- In your own words, what is information security?
- How supportive/involved are upper management towards information security?
- Can you describe the development and implementation of security policies in organisations?
- Why might end users demonstrate non-compliance with security policies?
- Can you describe the effectiveness of computer-based training and face-to-face training?

When interviewing end users the focus was on how socio-organisational factors influenced their security behaviour and whether they were willing and capable towards protecting information. Example questions include:

- Can you describe your job role?
- What sorts of information do you handle?
- Why do you think information security might be important for organisations/individuals?
- What is your experience of using technical security controls in your everyday work routine?
- How important is information security in your organisation?
- How would you describe your level of awareness regarding information security policies?
- How is information security training delivered within your organisation?
- How regularly do you receive training?

When interviewing security testers (whether for network-based or physical-based penetration testing) the focus was on breaking down testing into different stages, where the goals and objectives for each stage were identified as well as the importance of using various tools and techniques during testing. Examples questions include:

- In your own words, what is penetration testing?
- Why is it important for an organisation to have a penetration test?
- Can you describe the process of doing a penetration test?
- Do you work alone or in a team?
- Can you describe for me the role of technology in carrying out a penetration test?

4.5.2.3 Procedure

Following the development of interview guides, the next step was to select a suitable environment and to conduct interviews. Turner (2010) recommended that interviews be conducted in an environment that is private and quiet. This study used two methods for conducting interviews. The first method was to conduct interviews face-to-face and in-person. The second method was to conduct interviews face-to-face via Skype. Regardless of whether the interview was conducted in-person or via Skype it was conducted in a private and quiet place, such as a meeting room (if conducted in-person) or in the home of the participant/researcher (if conducted via Skype).

When conducting the interview, the following procedures were followed, as described by Turner (2010). First, the purpose of the interview was explained to the interviewee. Second, the interviewee was made aware of the confidential nature of the interview and informed that any answers they provided remained anonymous. Third, the interview format was explained, including how the interview will be recorded and the expected time of completion. Fourth, the interviewee was made aware that they could stop the interview at any time and that their answers would be removed from the study. Fifth, the interviewee was then instructed on how to get in touch with the researcher if they had any questions following the completion of the interview. Following this, they were provided with the participant information sheet and consent form and were provided enough time to read through and sign them.

Each interview was recorded either using an audio recorder application on the researcher’s mobile phone (if conducted in-person) or using a software application on the researcher’s laptop (if conducted via Skype). Because efforts were made to select a suitable environment for conducting interviews there were no problems with capturing clear audio recordings.

Following the completion of interviews the audio recordings were all stored in a single secure location. To gain access to the recordings the researcher was required to log in via a username and password. Further, the folder used to store the recordings was encrypted.

All interviews were transcribed using a professional transcription service. This involved uploading the audio recordings to a secure location (Microsoft OneDrive). A secure link was then provided to the transcription service provider and they were then able to perform transcription from this secure location. Once transcriptions were completed they were similarly stored in a single secure location.

Lastly, data analysis was conducted (more details discussed below) using the qualitative data analysis computer software package *Nvivo*. This specific software package was chosen as previous studies have shown it to be an effective software package (Ibrahim, 2012). Further, Leech and Onwuegbuzie (2011) described how using software packages during data analysis can take qualitative data analysis much further than when performing analysis manually because it will assist the researcher to record, store, index, sort, and code qualitative data.

4.5.3 Data Analysis

This next section discusses the approach of *thematic analysis* and how it was used in this study to analyse interview data. Previous studies have described thematic analysis as primarily focusing on identifying various themes and patterns of human behaviour within data (Aronson, 1994; Braun and Clarke, 2006; 2012; Floersch et al, 2010). For example, Floersch et al (2010, p. 2) argued that thematic analysis "is a commonly used qualitative method to identify, report, and analyze data for the meanings produced in and by people, situations, and events".

When performing thematic analysis, Braun and Clarke (2006; 2012) outlined two common approaches. The first approach is the inductive or 'bottom up' approach, which is primarily driven by the data. In other words, the various codes and themes that emerge during data analysis derive from the content of the data themselves. In contrast, is the deductive or 'top down' approach, where the researcher brings to the data various concepts, ideas, or topics that they use to help code and interpret the data. Thus, the various codes and themes that emerge derive more from the existing concepts and ideas of the researcher and so may not necessarily link closely to the semantic content of the data analysed.

Importantly, Braun and Clarke (2012, p. 58) argued that in reality, when performing thematic analysis, it is “impossible to be purely inductive, as we always bring something to the data when we analyse it, and we rarely completely ignore the data themselves when we code for a particular theoretical construct”. Thus, Braun and Clarke described the possibility of a middle ground between an inductive and deductive approach to thematic analysis, where the researcher mainly codes inductively from the data based upon participants’ experiences (where the theoretical lens does not completely override the experiences of participants), but also deductively draws upon theoretical constructs to render visible important issues that participants may not express explicitly.

Hence, and as mentioned previously, due to the possible tensions surrounding having a theoretical framework, this study adopted a phenomenology-inspired approach, where although the overall goal was to describe the experiences of guardians of protecting information in organisations, this was done via the use of a theoretical framework which guided the research process, such as which areas of information security management may prove important for investigation and the kinds of questions to be asked relating to those areas. Of course, when performing the analysis of data, the researcher proceeded to do so inductively, where important areas that were not originally included within the original theoretical framework were then able to emerge from the data. Indeed, Vaismoradi et al (2013, p. 401) argued that thematic analysis “may begin with a theory about the target phenomenon or a framework for collecting or analysing data, but that does not mean there is a commitment to stay within this theory or framework”.

When performing thematic analysis in this study, the following main stages were completed as per the recommendations of previous studies (Aronson, 1994; Braun and Clarke, 2006; 2012; Floersch et al, 2010; Ibrahim, 2012; Vaismoradi et al, 2013). Importantly, Braun and Clarke (2006) stated that thematic analysis should not be understood as a linear process of simply moving from one stage to the next, as the researcher may often move back and forth between stages if required.

The first stage of performing a thematic analysis largely involves becoming very familiar with the research data. For example, Braun and Clarke (2012, p. 61) argued the aim of stage one “is to become intimately familiar with your dataset’s content, and to begin to notice things that might be relevant to your research question”. Thus, during the first stage, the researcher read through each interview several times carefully before and after identifying themes and codes, which proved beneficial as this allowed the appreciation of the full picture and which helped to establish connections between participant’s experiences, and the overall data collected (Ibrahim, 2012).

The second stage as described by Braun and Clarke (2012) involves the researcher generating an initial list of codes from the data. Braun and Clarke (2012, p. 61) described codes as the building blocks of thematic analysis, where “If your analysis is a brick-built house with a tile roof, your themes are the walls and roof and your codes are the individual bricks and tiles”. Thus, during the second stage the researcher identified any feature(s) within the data that were of significance to the participant, and which may have had some meaning and importance towards understanding the phenomenon under investigation.

At this stage, coding was largely descriptive, where each code was labelled based upon both the activity (e.g., reading a security policy, completing a training programme) and the participants general experience of it (e.g., whether the security policy was easy to read, whether the training programme was unengaging etc.). Codes were then grouped together based upon the main focus areas of information security that were identified in the previous chapters. In other words, listed within Nvivo were the six main areas of information security management that were identified prior to data analysis, which then contained within them all the codes that were identified from interviews which connected to those areas. The end result of this stage was a list of several hundred codes all connecting to different areas of information security management which the researcher deemed to represent some significant feature of participants’ experiences of information security management in organisations.

The third stage of thematic analysis primarily involves searching for themes within the data. Vaismoradi et al (2013, p. 402) defined a theme as “a coherent integration of the disparate pieces of data that constitute the findings ... It captures something important about data in relation to the research question, and represents some level of response pattern or meaning within the data set”. Hence, during the third stage the researcher organised and sorted the different codes into potential themes, along with all the relevant coded data extracts connected to those identified themes. As mentioned already, there were several hundred codes which were grouped together based upon the six focus areas of information security management. However, the goal now was to review the various lists of codes in order to identify any connections between them or areas of similarity, where codes may be clustered together in order to generate potential overarching themes which represented a meaningful pattern within the data. In addition, during this stage the researcher began to explore the relationship between themes, and considered how emerging themes will eventually work together in telling an overall story about the data. Also, Braun and Clarke (2006; 2012) highlighted that some initial codes may form main themes, whereas others may form sub-themes. During the process of identifying themes, there were several main themes that emerged from the data and others which were further broken down into several sub themes.

The fourth stage of thematic analysis involves reviewing themes. Braun and Clarke (2006; 2012) stressed that while data within themes should correspond together in a meaningful way, there should still be clear and identifiable distinctions between them. Thus, during this stage the researcher carefully reviewed each theme in order to ensure that various themes were not in fact better presented as sub-themes of other themes and that each theme was unique and distinguishable from the next.

The fifth stage of performing thematic analysis involves defining themes. Braun and Clarke (2006) explained that defining themes generally corresponds to identifying the ‘essence’ of each theme and determining what aspect of the data each theme captures in relation to the research questions. Thus, during this stage the researcher tried to identify what each theme and sub-theme was about and how it corresponded towards answering the research question and was then defined and named accordingly.

The sixth and final stage of thematic analysis involves producing the findings. For example Braun and Clarke (2006; 2012) argued this stage commences when you have a full set of main themes, and involves the final write-up of the report. Further, they stressed that the purpose is to provide the reader a 'compelling story' about your data, which is based on your analysis. It should be convincing and clear, but also complex and embedded within a specific scholarly field. Thus, during the final stage the researcher presented the findings in such a way that they provided the reader an interesting and insightful account of the guardianship experiences of information security management of three groups of guardians, which may be of significance to the scholarly disciplines of both criminology and information security management (and potentially other related disciplines).

4.5.4 Reliability and validity

This last section discusses the use of quality criterion in qualitative research and how they were used during the present study.

According to Rolfe (2006, p. 304), attempts to establish consensus towards any quality criteria for qualitative research are usually unsuccessful because "there is no unified body of theory, methodology or method that can collectively be described as qualitative research".

Emden and Sandelowski (1998, p. 207) similarly argued that the notion of applying the quality criterion of reliability and validity to qualitative research has undergone various 'transformations', including being championed*,* translated*,* exiled*,* redeemed, and surpassed. The approach taken in this study may be considered that of the translated transformation*.* Emden and Sandelowski (1998, p. 208) described the translated transformation as when "the concepts of reliability and validity are *translated* to fit the canons of qualitative research". Hence, To understand how quality criterion were met in this study, first, an outline of quantitative quality criteria will be provided to compare those used in qualitative social research.

Guba and Lincoln (1994) described reliability and validity in quantitative research as including the following: *Reliability*, whether measurements can be measured repeatedly, and the results repeatedly produced; *Measurement validity* (or construct validity), whether a devised instrument measures the thing it is meant to measure; *Internal validity* (or causality), whether X was in fact caused by Y, and not some other variable, such as Z; and, *External validity* (or generalisability), whether results can be generalised beyond the specific research context.

From the above descriptions, we can now discuss the qualitative equivalents of these as part of the translated transformation (Emden and Sandelowski, 1998). As part of the translated transformation of quality criterion, Lincoln and Guba (1985) introduced the concept of *trustworthiness* for determining whether a qualitative study is good. Trustworthiness involved establishing the following:

- *Credibility*, which parallels internal validity, and referred to how believable were the findings. To ensure good levels of credibility in this study, the researcher performed 'respondent validation' or 'member checking'. This involved the researcher communicating with participants to make sure that the meanings provided by them were properly understood. Further, this was performed both during interviews and following data analysis.
- *Transferability*, which parallels external validity, and refers to whether the findings are applicable to other contexts. While the goal of qualitative research is not to generalise findings, by describing participant's experiences in great detail, it allows the reader to evaluate the extent to which the conclusions drawn are indeed transferable to other people and places. Therefore, transferability was achieved via the use of in-depth interviews which generated 'thick descriptions' of participant's experiences.
- *Dependability*, which parallels reliability, and refers to whether the findings are likely to apply at other times. To achieve dependability, an external audit will

form part of this study. This will involve having an external auditor review the data collection, data analysis, and the results of the research study.

- *Confirmability*, which parallels objectivity, and refers to whether the interviewer has allowed his or her values to intrude into the research process. To ensure good levels of confirmability, the researcher adhered to the concept of ‘bracketing’ (as discussed above in research design), which involved the researcher setting aside their preconceived notions about the phenomenon under study.

4.6 Summary

This chapter has presented both the methodological approach and research methods used in this study. The researcher adopted an interpretivist research paradigm, a qualitative research strategy, and a phenomenology-inspired research design. In addition, the researcher utilised a purposive sampling design in order to recruit participants as well as using various recruitment techniques. Data collection involved the use of in-depth interviews and data analysis was performed using thematic analysis via Nvivo software application.

5 Security Managers Experiences of Information Security Management in Organisations

5.1 Introduction

This chapter presents the findings from interviews with security managers about their experiences of managing information security in organisations. The chapter begins with a brief discussion of security managers experiences towards the nature of information security management. Following this, the chapter is broken down into 4 main sections presenting the findings relating to (1) upper management support, (2) information security policies, (3) security education, training, and awareness programmes, and (4) monitoring and enforcement practices. For each section there will be a description and analysis of how each (according to security managers) influenced the managing of information security in organisations and the willingness and/or capability of end users to protect information.

5.2 The nature of information security management

This section presents the findings relating to the experiences of security managers towards the nature of information security management. During interviews, security managers generally described information security management as primarily developing and implementing security controls to protect the 'critical characteristics' of information; that is, the confidentiality, integrity, and availability of information. For example, one security manager described information security management as,

> Making sure that the information assets of the organisation are kept confidential, are kept with integrity, and are kept accessible. (James, Information Security Education Manager)

Similarly, another security manager commented,

> Information security is essentially putting measures in place to secure your information … to provide confidentiality, integrity, and availability. (Nadine, Information Security Analyst)

Importantly, although security mangers described information security management as developing and implementing security controls to protect the CIA of information, they stressed that this was not achieved solely through developing and implementing technical security controls, but also heavily involved the development and implementation of non-technical security controls, such as security policies and SETA programmes. As one security manager commented,

> Even though it was borne in the technology space, it is not a technology problem … in my view, we cannot solve information or cyber security problems purely with technology. It’s just not possible. (Barry, Principal Security Architect)

Similarly, another security manager commented,

> It's a mix of technology and non-technology. So, obviously you'll have all the technology that actually prevents the bad things coming in … but you also need policies and procedures to help people know what they should and shouldn't be doing in these situations. (Lesley, Information Security Analyst)

Interestingly, when discussing the insecure behaviour of end users, security managers described how the increasing levels of security breaches taking place in organisations were often the result of organisations failing to develop and implement non-technical security controls, rather than it simply being an issue with end users behaving insecurely. In other words, security managers did not describe end users as an inherent vulnerability which often leads to security breaches, rather it was an issue with organisations failing to develop and implement effective non-technical security controls, such as security policies and SETA programmes. As one security manager commented,

> It’s not the end users’ fault … if we are not giving them decent training; if we are just trying to impose what we want them to do without actually … understanding their day job and understanding that often what we ask them to do is really difficult. (Janet, Information Security Consultant)

Thus, security managers described how an important part of information security management is making sure to pay equal attention towards supporting and empowering end users in organisations. As one security manager commented,

> They call people the weakest link, but … If you are giving them the right tools and are training and empowering them, then people can be your strongest link. (Carol, Chief Information Security Officer)

Indeed, one security manager described the overall goal of information security management as,

> To adjust people's behaviour to become more of a *protector* as opposed to someone who introduces exposure of information.
> (Morris, Principal Security Manager)

We can understand from the above comments that the development and implementation of security controls to protect information was described by security managers as the overarching goal of information security management. Furthermore, the selection of security controls was described as performed holistically, where consideration of both technical and non-technical security controls was made to ensure overall effectiveness towards protecting information. Lastly, rather than representing a suitable target for likely offenders, end users were described as potential guardians of information, depending upon the effective development and implementation of non-technical security controls. Of course, there were numerous socio-organisational factors described by security managers which influenced such development and implementation, which forms the basis of the remaining sections of this chapter.

5.3 Upper management support in information security management

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness to perform protective actions forms part basis of effective guardianship – the other being the capability to perform protective actions. Furthermore, the level of willingness of guardians to perform protective actions may be influenced by the behaviour of super guardians.

In the context of information security management, this suggests that the willingness of end users may be influenced by upper management in two main ways: (1) by providing security managers with enough organisational resources to develop and implement security controls to manage the security behaviour of end users, and (2) by promoting information security and demonstrating good security behaviour in front of end users. Therefore, this next section presents the findings relating to security manager's experiences of upper management support in information security management.

5.3.1 The Importance of upper management support

During interviews, security managers described upper management support as an important factor when managing information security in organisations for two main reasons. The first main reason was upper management influenced the amount of organisational resources available for developing and implementing security controls; often referred to as the 'security budget' of the organisation. For example, one security manager commented,

> So, they indirectly influence end users through … how much they empower the security function, which has that knock on effect … it's how much the security team has to hire new people, to bring in new resources, how much they can spend on technology, how much they can spend on training, and that's training both within the end users and training within the security function itself … So, budget is really important. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> To do business securely, what do you need? … If my risk is £100,000 then my security budget has to be somewhere around that … they need to understand … how much needs to be invested to protect that. (Carol, Chief Information Security Officer)

We can understand from the above comments that upper management support was described as an important factor when managing information security because upper management influenced the amount of organisational resources available to security managers to develop and implement security controls.

In the context of guardianship of information, this suggests that as super guardians, upper management may indirectly influence the guardianship of information by influencing the availability of organisational resources for security managers to manage the security behaviour of end users via the development and implementation of security controls.

The second main reason described by security managers for why upper management support was important, was the expectations and observed behaviour of upper management influenced the levels of willingness of end users. In other words, if upper management demonstrated good security behaviour, then end users were described as more likely to have a willingness towards protecting information, which in turn led to improvements in their security behaviour. Therefore, security managers stressed that upper management must regularly demonstrate good security behaviour and actively promote the protecting of information in organisations.

In contrast, should upper management fail to support the efforts of security managers, this was described as demonstrating to end users that protecting information was not important to the organisation, which reduced the overall effectiveness of security managers efforts to properly manage end user security behaviour. For example, one security manager commented,

> I think there is an onus on board members to get to grips with security … because they can give a healthy budget, they can … help set the security goals and objectives, but if their behaviour contradicts what the security team are asking for, then that will be the most powerful message that is received by end users … it sends this message that actually security isn’t important and we don’t need to follow these rules. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> There is a lot of staff training and empowerment that needs to happen and top management have to have that sponsorship … if upper management doesn't give a toss about security and ignores it, then staff are going to be the same. (Carol, Chief Information Security Officer)

Such findings are significant, as they provide empirical support for the argument made by Sampson et al (2010) regarding the influence super guardians may have on the willingness of ordinary guardians. Furthermore, the findings reveal several ways in which upper management can positively support the managing of information security in organisations, where their actions may help to influence the willingness of end users to protect information.

For example, security managers described how during the development and implementation of security policies, upper management could provide an introductory statement which emphasises the organisational need to protect information and the organisational responsibility of end users in relation to this; which would then improve the effectiveness of the security policy. As one security manager commented,

> The policy itself will be written by the security function … but if it's signed off from a senior exec and if there is something that kind of says, this isn't coming from security, this is coming from the business, then certainly in theory it should be more effective. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> If your management will not stand behind that policy, your staff won't stand by it either. They just won't. So, you need the proper sign-off on them when it eventually happens. (Lesley, Information Security Analyst)

In addition to supporting the efforts surrounding security policies, security managers described how upper management 'championed' various SETA programmes to ensure end users took part and were actively engaged. For example, one security manager commented,

> When it came to e-learning time, the first door I knocked on was the chief exec, and I would say it's e-learning time, can you do yours please … And if anybody else in the organisation said I haven't done it, 'Well, the chief exec has done it, are you saying you are busier than they are?' So, it's a really powerful tool to drive behaviours.
> (Stewart, Senior Information Security Consultant)

Similarly, another security manager described how she delivered a security training programme for end users. However, to ensure end users were engaged, upper management also attended, which demonstrated to those end users the organisational importance of the subject matter. As she explained,

> I did a small session to a finance team a while ago and the chief financial officer came along and sat in the training, and … It's really important because I need them to see how important this is, and … it sends that message to them that this is absolutely a top priority'.
> (Janet, Information Security Consultant)

We can understand from the above comments that the support of upper management was described as an important factor towards managing information security in organisations because the expectations and observed behaviour of upper management influenced the willingness of end users' towards protecting information; where if upper management considered it important, then end users were described as more likely to consider it important. Furthermore, upper management were able to demonstrate the importance of protecting information by assisting security managers during the development and implementation of various security controls.

In the context of guardianship of information, this again shows that as super guardians, upper management may also indirectly influence the guardianship of information by influencing the level of willingness of end users to protect information through demonstrating positive security behaviour.

These findings are timely, as previously there has been some debate as to whether the observed behaviour of upper management can positively influence the security behaviour of end users alongside that of peers, immediate supervisors, and security managers (e.g., Herath and Rao, 2009a). Therefore, the above findings suggest that the expectations and observed behaviour of upper management should be considered as an important factor towards influencing end user security behaviour in organisations.

In addition, the above findings show that both security policies and SETA programmes may be an effective way to communicate the expectations of upper management to end users. These findings are likewise significant because previous studies have highlighted a lack of investigation towards how end users develop their understanding of the expectations of upper management and/or how upper management can support the efforts of security managers when managing end user security behaviour (e.g., Hu et al, 2012).

5.3.2 The lack of upper management support

Despite security managers interviewed for this research describing upper management support as an important factor when managing information security, they generally described a lack of support from them. For example, when discussing whether upper management were providing their support toward managing information security, one security manager commented,

> To be brutally honest, in all the organisations I've worked for, it's been a challenge to get information security or ‘cybersecurity’ on the agenda at the top table. (Gordon, Chief Information Security Officer)

Similarly, another security manager commented:

> The organisation that I had been a part of … when I developed the policy and then developed the training to support the policy … there was always some push-back … The challenge I had was, this

> organisation wanted to be secure but didn't want to go through the basic steps to become secure … no matter what I did, they did not want to do the basic things. (Sarah, Senior Security Advisor)

The difficult challenge of securing the support from upper management has been highlighted elsewhere. For example, previous studies have argued that although the allocation of organisational resources to security managers for developing and implementing security controls may be considered one of the most important ways upper management can support information security, in practice, security managers often fail to receive the necessary funds (Kankanhalli et al, 2003; Kajava et al, 2006; Knapp et al, 2006a).

The importance of making sure security managers are provided with enough organisational resources to properly manage information security cannot be overstated, as this will greatly impact their ability to develop and implement effective security controls to manage the level of protection of information in organisations, which includes the managing of end user security behaviour. Thus, the above findings suggest that an initial hurdle that security managers must try to overcome when performing information security work, is gaining the support of upper management.

During discussions with security managers about the lack of support from upper management, they offered numerous explanations as to why they thought upper management failed to get involved. From analysing interview data, several sub-themes emerged towards the lack of support from upper management. Each will now be presented and discussed.

5.3.2.1 The reactive approach of upper management

For many security managers interviewed, they felt that upper management were not providing their support because most upper management were reactive rather than proactive when it comes to protecting information. In other words, upper management in organisations were described as not considering the protection of information as important unless they had experienced some form of security incident, where the negative consequences of the security incident forced them to take information security more seriously. For example, one security manager commented,

> There was a company I worked for a few years ago, and the head of IT said, ‘What we need is a good breach, because if we had a good breach then the board would realise the importance of having good security’ … Until then, it has very little budget to help implement things. (Derek, Information Security Officer)

Similarly, another security manager commented,

> Some companies, until it happens to them then they are not bothered. So, once it’s happened then they will look at it, but by then it’s too late because you’re all over the news. (Carol, Chief Information Security Officer)

We can understand from the above comments made by security managers that a major cause for the reactive approach of upper management was a lack of known security incidents taking place within their respective organisations; where if a security breach had not taken place within an organisation, then security managers described being less likely to be provided with a suitable security budget and/or to have the active support of upper management in promoting information security throughout the organisation.

5.3.2.2 The lack of understanding towards information security risks

Security managers also described how the reactive approach of upper management was often caused by a lack of understanding surrounding various information security risks or because upper management simply believed that security breaches were unlikely to occur within their organisations. For example, one security manager commented,

> I think there is a lack of understanding about how cybercrime is carried out … organisations are going to think, ‘Well we are never going to be targeted. No one is going to come after us’ … without realising that a lot of cybercrime is not targeted in that specific way.

> So, I think it is a combination of optimism, thinking that it’s never going to happen to us … and also a lack of understanding of how ‘cyber’ in security actually operates. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> You’ve also got this continual problem where people always think ‘Oh, it’s not going to happen to us. Why would somebody target us?’, and again, that’s not the way it works. There’s still definitely space for improvement. (Timothy, Cyber Security Analyst)

Interestingly, security managers therefore stressed that alongside end users, upper management must also receive various SETA programmes that are specifically tailored to help improve their understanding in certain areas of information security management (e.g., risk management). For example, one security manager described how when delivering SETA programmes in organisations she would also deliver a separate SETA programme tailored for upper management. She commented,

> We did a session earlier in the week … for general sort of employees and then next week we are doing an executive session; we are going in and doing a kind of session for the ten board members. So, you are giving them awareness-raising training in a lot of the same areas but the angle of it changes. You talk about it in a slightly different way and you talk about different threats, because senior management absolutely need to understand how much of this is targeted at people because they are often a big target. (Janet, Information Security Consultant)

We can understand from the above comments that another important factor towards explaining the reactive approach of upper management, which often led to a lack of support for security managers, was described as partly caused by an overall lack of understanding surrounding information security management, particularly the various information security risks and likelihood of security breaches. Thus, security managers interviewed recommended that SETA programmes be provided to help upper management improve their understanding of information security and ultimately gain their support. Such recommendations from security managers are not without merit, as previous studies have shown that following improvements in the security awareness of upper management, security managers were more likely to receive support, which included increased security budgets (Choi et al, 2008).

5.3.2.3 The perceived costs of developing and implementing security controls.

In addition to a lack of understanding towards security risks, security managers also described how the reactive approach of upper management was due to the perceived high costs of developing and implementing security controls. In other words, if upper management considered developing and implementing security controls as consuming high amounts of organisational resources, then security managers described them as less likely to provide their support. For example, when asked whether enough organisational resources were being provided to properly manage information security, one security manager commented,

> Security budget, it will always be low … it's seen as a cost ... I always try and say it's like insurance, hopefully nothing will ever go wrong, but ... it should be because you've done all the right things to make sure nothing goes wrong, and not just because nobody's attacked you. So, I would say no. (Ronald, Information Systems Security Analyst)

The problem of perceived high costs of security controls was then made worse for security managers by the fact that other areas of organisations were competing for the same scarce organisational resources. As one security manager commented,

> When you look at everything they’ve got planned for the year … and you ask what space is left for security and what sort of priority does security have against everything else. That becomes a real challenge in terms of how you deal with these things … And I think that is a massive problem for most organisations. (Norbert, Head of Information Security)

We can understand from the above comments that the reactive approach of upper management was also described by security managers as the result of the perceived high costs of developing and implementing security controls. This was further exacerbated by the fact that many organisations had limited organisational resources and information security was often viewed in direct competition with other areas of the organisation.

The above findings therefore suggests that however much an organisation understands and accepts the need to protect information, there may always be the problem of competing demands for organisational resources, where information security-related programmes may not be considered as important in relation to other areas of the organisation, which may in turn cause them to be delayed or even abandoned as a result.

5.3.2.4 Information security management is viewed as a technical problem.

Security managers also described how upper management were reactive towards promoting information security because upper management still considered the protecting of information to be a technical problem rather than a business problem. In other words, because upper management considered the protecting of information to be something that primarily required technical security controls, they were described as less likely to want to fund and/or promote the development and implementation of non-technical security controls. Which again made the job of security managers even more difficult, as many of the problems security managers were experiencing required non-technical solutions. For example, one security manager commented,

> Certainly, in terms of C level executives I'd say that typically they're only aware of it when there's a problem … I think up until then, there is still a feeling that it's an IT problem – and it's not; it's a business problem and businesses have to wake up to that. (Timothy, Cyber Security Analyst).

Similarly, another security manager commented:

> There is still a lot of organisations that think this can all be fixed with technology … where people still think it's a very technical thing, you know … they will think, 'Well surely, we can just buy a piece of technology that will sort all of this out? … there is still a long way to go, where senior management understand that this is also an issue with people as well. And we need to focus on people to be more aware and to behave more securely. (Janet, Information Security Consultant)

We can understand from the above comments that a lack of support from upper management was described by security managers as influenced by upper management viewing information security as a technical problem, rather than a business problem. As a result, security managers described being less likely to be provided with organisational resources towards the development and implementation of non-technical security controls as well as receiving the active participation of upper management in promoting information security.

The problem of upper management viewing information security management as a technical problem, which can be fixed solely by purchasing technical controls, has long been a major stumbling block in information security management; where upper management are often described as failing to acknowledge the need for senior level input and support for information security programmes, as well as the need to develop and implement non-technical security controls (von Solms and von Solms, 2004b; Willison and Backhouse, 2006).

5.3.2.5 The poor communications between security managers and upper management.

Security managers described how the reactive approach of upper management was also caused by the poor communications between security managers and upper management. Importantly, the issue of poor communications lay more towards security managers themselves rather than upper management. The problem described by security managers was upper management oftentimes could not understand what security managers where advising them due to some security managers communicating in highly technical terms, and so upper management would simply fail to understand the various security threats and vulnerabilities within their own organisations and the impact that a security breach would have (which connects to the above problems of upper management failing to understand security risks and treating information security as a technical problem). For example, when discussing why upper management do not provide support in information security, one security manager commented,

> The vast majority of people on boards are not techies. I have mentored any number of professionals … I say to them quite regularly, the problem is not with the board, it's with you. You have to speak the same language … you have to help them understand how it's going to help the business. (Veronica, Head of Information Security)

Similarly, another security manager commented,

> They don’t know how to talk business, and so if they go and talk at the board level … they wouldn’t be able to use the right language to communicate it to the board. (Carol, Chief Information Security Officer)

We can understand from the above comments that the reactive approach of upper management was also described by security managers as partly caused by the ineffective communications between security managers and upper management, where the inability of some security managers to explain in simple terms the current organisational needs surrounding information security often led to a lack of support from upper management.

These findings are especially important because, arguably, were the communications between security managers and upper management improved, then upper management may have a better understanding with regards various security risks (which is one of the identified problem areas discussed above), as well as the need for non-technical security controls (another problem area) and how much security controls actually cost to develop and implement, including possible cheaper alternatives (another problem area).

Interestingly, a potential way to assist security managers when communicating to upper management may be to emphasise the negative impacts of security breaches for organisations. For example, one security manager commented

> At the C-level ... implementing security measures in itself can be very expensive and time-consuming … And usually, what we do is … talk in terms of money. So, what is the potential loss caused by a data breach? So, yeah, telling them the potential loss caused by a breach, it will actually get them involved, because then they'll start thinking in those terms. (Nadine, Information Security Analyst)

Again, this suggests that improvements in the communications between security managers and upper management may help improve the levels of upper management support towards information security.

5.4 The influence of security policies on end user willingness

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness to perform protective actions forms part basis of effective guardianship – the other being the capability to perform protective actions. Furthermore, the level of willingness of guardians to perform protective actions may be influenced by the perceived level of responsibility to perform protective actions. In addition, based upon the Rational Choice Perspective, the willingness of guardians may also be influenced by various social norms surrounding performing protective actions as well as the risks to guardians for failing to perform protective actions.

In the context of information security management, this suggests that the willingness of end users to protect information may be improved via the development and implementation of security policies which make end users aware of their organisational responsibilities towards protecting information and the punishments for failing to protect information.

Therefore, this next section presents the findings relating to the experiences of security managers of developing and implementing security policies to influence the willingness of end users to protect information.

5.4.1 The purpose of security policies

During interviews, security managers generally described the purpose of security policies as establishing the following aspects of information security management:

- the organisational need to protect information,
- the roles and responsibilities of employees in relation to this organisational need,
- acceptable and unacceptable behaviours surrounding the use and protection of information within the organisation, and
- the punishments for non-compliance with security policies.

For example, one security manager commented,

> The security policy is one mechanism for establishing direction in an organisation on information security … It’s one of the few ways in which you can communicate to a large group of people, typically employees or external parties, your expectations as an organisation on how information should be protected. (Morris, Principal Security Manager)

Similarly, another security manager commented,

> It provides a statement of intent, where people can understand these are the norms, these are the behaviours that I should be following in this organisation – this is what is expected of me. So, it’s a way for the organisation to communicate that to all the end users. (Janet, Information Security Consultant)

In addition, security managers described numerous types of security policies which can be developed and implemented within organisations depending upon the types of information the organisation stored, processed, and transmitted, as well as the different job roles performed by end users (as this generally determined their need of access to information). For example, when discussing the different security policies organisations are likely to develop and implement, one security manager commented,

> You would have a password policy; you would have an acceptable use policy, what you can and cannot do in terms of internet use for example. A social media policy, which is something that has become increasingly important. You might have a physical security policy, what to do with shredding paper and things like that; work from home policy; bring-your-own-device policy; basically, every area of how people are engaging with technology or information … having a policy that outlines this is the way to do it. (Janet, Information Security Consultant)

We can understand from the above comments that the purpose of security policies was described as making sure end users were aware of their exact organisational responsibilities towards protection information based upon the types of sensitive information they regularly handled as part of their job role. Furthermore, that certain behaviours surrounding the use of organisational information were prohibited by their organisation and that failure to comply with this would lead to punishment. Lastly, because end users might access various types of information and perform various work tasks connected to different job roles, there were numerous security policies which organisations needed to develop and implement to support this.

In the context of guardianship of information, this demonstrates the importance of security policies as a possible mechanism to ensure the willingness of end users by highlighting an organisational responsibility to act as guardians for information, including the specific protective actions they must perform, and which state the punishments should they fail to act as expected.

These findings not only endorse the argument originally made by Felson (1995), that the willingness of guardians may be influenced by their sense of responsibility to act as guardians, but also extends our understanding of how the factor of responsibility can apply in an organisational setting; in particular, the context of information security management, where security policies may be used to improve the level of willingness of end users towards protecting information.

Importantly, while security managers described security policies as an important security control for managing security behaviour, they made it very clear that the existence of security policies in and of themselves does not guarantee that end users will have an awareness and understanding of security policies; and subsequently any awareness and understanding towards their organisational responsibilities in terms of the protection of information. Indeed, there were many aspects relating to the development and implementation of security policies that security managers described as important, and which could potentially reduce the effectiveness of security policies. As one security manager commented,

> The fact that you've got a policy means nothing other than you've got a policy. It doesn't mean to say that you've got secure behaviours … the most fundamental part of a policy is, if people *can't* read it or *don't* read it, then it isn't effective because you're not communicating what you expect from people. (Stewart, Senior Information Security Consultant)

During the process of data analysis, the following four themes emerged in relation to the development and implementation of effective security policies: (1) policy digestibility, (2) policy feasibility, (3) policy inclusion, and (4) policy awareness and communication. Each theme will now be presented and discussed.

5.4.2 Policy Digestibility

During interviews, security managers described how an effective security policy is one that is *digestible* to end users. The digestibility of a security policy generally referred to how easily it could be read and understood by end users. For example, one security manager commented,

> A policy is not effective if … it’s not written in a style which makes them want to read it, or they don’t know what it means for them; they’re all things which will undermine the effectiveness of the policy. (Stewart, Senior Information Security Consultant)

Security managers felt that developing security policies that were easily digestible to end users was a major challenge for many organisations. As one security manager commented,

> The organisation does need to communicate its expectations but it’s actually very difficult in practice to do that … I know from working very closely with organisations in many different sectors, including banking, there are those who really struggle with this … I’ve been doing that kind of work for over twenty years; the largest and most capable … have still not solved that problem. (Morris, Principal Security Manager)

In response to the comments from security managers that many organisations were struggling to develop digestible security policies, interview discussion then moved towards recommendations from security managers on how to improve the levels of digestibility of security policies. What follows are the various sub themes connected to security managers’ experiences of developing digestible security policies.

5.4.2.1 Tailoring security policies to end user job roles

According to security managers, the first common mistake that organisations make when developing security policies is not tailoring them to include only information that is relevant to end user job roles. For example, one security manager commented,

> Some organisations will develop an IT security policy … there’s probably a page worth spread through the different sections of the whole document that are actually relevant to your normal user. For me, that’s always the biggest problem from looking through policies. (Norbert, Head of Information Security)

Similarly, another security manager commented,

> There will be loads of stuff there that's really for IT … finding what they [end users] have to comply with is really tricky … the bits that are relevant to everybody are scattered throughout it. (Ronald, Information Systems Security Analyst)

We can understand from the above comments that according to security managers, the described challenge for end users was trying to locate the information that was relevant to their job roles. The more information that was not relevant to their job roles the less likely they were to read and understand the security policy. Thus, security managers highly recommended that organisations ensure to include only information that was relevant to end user job roles.

5.4.2.2 Avoid using technical language

The next common mistake described by security managers when developing security policies was writing them in an overly technical language or using too much jargon, even though many end users may not have a technical background or aren't performing in a technical job role. For example, one security manager commented,

> Too often … if it's been written by the IT department it will be written in technical language, and people just ignore it. (Janet, Information Security Consultant).

Similarly, another security manager commented,

> A lot of people are not going to have a technical background, so you need to avoid all the jargon. (Lesley, Information Security Analyst).

We can understand from the above comments that the described challenge for end users was trying to make sense of the content of security policies, which was made difficult by the overuse of technical language or jargon. Thus, security managers recommended that organisations use more neutral language when writing security policies to make sure they are digestible to end users.

5.4.2.3 Keep security policies short

The next common mistake described by security managers when developing security policies was making them too long. For example, one security manager commented,

> I’ve seen so many policies in my career that are fifty pages long … Someone isn’t going to read a 50-page document to find the bit that’s relevant to them on page 43 – they’re just not going to do that. (Stewart, Senior Information Security Consultant)

Similarly, another security manager commented,

> Keep your policies as short as you possibly can. The longer they are, the less likely anybody's ever going to read them. (Lesley, Information Security Analyst)

We can understand from the above comments the described challenge for end users was either having the time to sit down and read through security policies or having the patience and determination to read through long security policies. Thus, security managers recommended that organisations ensure security policies were kept short.

5.4.2.4 Do not be copy and paste security policies

The last common mistake described by security managers when developing security policies was organisations copying and pasting the security policies of other organisations. For example, one security manager commented,

> I’ve seen policies go bad in a number of different ways … point number one of failure is copying someone else’s policy … and you see that quite a lot. (Bruce, Senior Information Security Consultant)

The problem described by security managers surrounding the copying and pasting of security policies was they will not have been developed for the end users of the organisation in question. Furthermore, there was no guarantee that the development process of the copied security policy had any consideration towards the above aspects of security policy development.

Importantly, the main explanation described by security managers for the copying and pasting of security policies was a lack of organisational resources available to security managers to develop them (thus, we see here connections to the earlier discussion about the importance of funding from upper management). For example, one security manager commented,

> If a team is under resourced and someone has to quickly pull together policies … then absolutely they are going to go online and look for some policies, and copy and paste … If you are a smaller organisation as well, you might not even have a security function. And so, for them, it might seem like a great option to copy and paste without thinking it through, and what the implications of that could be. (Janet, Information Security Consultant)

We can understand from the above comments, a challenge for security managers was developing security policies that were digestible, which may have been caused by low levels of resources and/or expertise at writing security policies. Because of this, some would copy and paste the security policies of other organisations. However, due to them not accurately reflecting both the organisation and the end users in question, these were described as less effective at managing security behaviour.

Thus, overall, while security policies were described as very important for managing security behaviour in organisations, the development of security policies was not a straightforward task for many organisations and there were many aspects of developing security policies that organisations were described as struggling with. Hence, to ensure digestibility of security policies, security managers recommended that organisations (1) tailor security policies to end user job roles, (2) write security policies in a simple language that end users can understand, (3) keep security polices short, and (4) do not copy and paste the security policies of other organisations.

In the context of guardianship of information, this suggests that end users' understanding of their organisational responsibility towards protecting information, the expectations towards performing specific actions, and associated punishments for failing to act, while potentially important factors towards influencing their willingness, may be greatly influenced by the digestibility of security policies. In other words, if security policies have low levels of digestibility then end users may struggle to understand the content of security policies, which means their levels of willingness towards protecting information may be diminished, which in turn may lead to a reduction in the overall levels of guardianship of information in organisations. Thus, the digestibility of security policies may be considered an important factor when determining the effectiveness of security policies as mechanism towards improving the willingness of guardians to protect information in organisations.

5.4.3 Policy Feasibility

Even though a security policy might be digestible and therefore properly understood by end users, security managers stressed that it must also be feasible for end users, otherwise it will be less effective in terms of managing their security behaviour.

The feasibility of a security policy generally referred to whether end users were able to incorporate the required security actions into their everyday work routines without jeopardising their effectiveness at performing their primary job role. Thus, security policies which were considered feasible were those that properly aligned with the everyday work routines of end users. For example, one security manager commented,

> If you write a policy that nobody can follow, because you're asking them to do behaviours they can't do because of the way their job works, then that document has no credibility. (Stewart, Senior Information Security Consultant)

Similarly, another security manager commented,

> If you have a policy for people that … is at odds with how they have to function to get their job done, then people are going to find workarounds, they are just not going to stick to the policy. (Janet, Information Security Consultant)

Unfortunately, developing security policies that were feasible was also described by security managers as a major challenge for many organisations. For example, one security manager commented,

> A very common situation … the policy sounds great in theory, but in practice it doesn't really work. When you look at the reality in a business environment, where it is trying to compete in a market place … to produce the best products and services. And policies are causing disruptions or presenting obstacles … you will very quickly end up in a situation where staff will just bypass them. (Morris, Principal Security Manager)

Similarly, another security manager commented,

> If we have policy, its challenge is to be … workable for those that it applies to. And a great deal of policy is a real challenge for our day-to-day businesses … especially in large business and government, the policies which we've got ... are not flexible enough … And that's why most policy absolutely fails. (Alistair, Senior Cyber Incidence Response Consultant)

We can understand from the above comments that security policies were described by security managers as having to be feasible for end users because protecting information isn't the only organisational responsibility that end users must comply with; they have other responsibilities relating to their primary job role within the organisation which compete with security responsibilities. Therefore, there must be a good balance or alignment between the two sets of responsibilities otherwise this may create conflict for end users.

In the context of guardianship of information, this suggests that while establishing an organisational responsibility towards protecting information may be an important part of improving end user willingness, such a responsibility competes with and sometimes conflicts with additional responsibilities, which may in fact be considered higher in terms of priority. Thus, the protection of information may be considered less important depending upon the situation.

The findings surrounding the problems of digestibility and feasibility of security policies are especially important because they suggest that the issue of end users behaving insecurely and non-complying with security policies may be due to factors of digestibility and feasibility of security policies rather than factors directly relating to end users. Therefore, the presence of additional security controls may not prove to be an effective way to resolve the situation for organisations. For example, monitoring end user security behaviour and punishing end users for non-compliance may not lead to improved compliance as this does little to improve end user’s understanding of poorly written security policies and/or does little to amend problematic situations caused by unfeasible security policies, unless security policies themselves are reworked and improved.

Interestingly, the findings showed that security managers described how organisations can ensure that any potential conflict between different sets of responsibilities is kept to a minimum by making sure security policies are digestible and feasible from the perspective of end users, as will now be presented and discussed.

5.4.4 Policy Inclusion

Following on from discussions about the above problems of developing security policies that are digestible and feasible to end users, security managers described how organisations should make efforts to include end users during the development process, whether through focus groups or individual interviews. The reason being this would then enable those organisations to review both the digestibility and feasibility of security policies before they were implemented within the organisation. In addition, security managers described how including end users during the development process can also create a sense of ownership over the security policy, which in turn may increase their levels of willingness towards adhering to the security policy. For example, one security manager commented,

> Invite feedback because there may be someone in the organisation who reads it and thinks, ‘Hang on a minute, we can’t do that’ … If you make people feel like you are working together to achieve the right result rather than having it done to them, it’s much more effective. (Stewart, Senior Information Security Consultant)

Similarly, another security manager commented,

> The best policy in my opinion, is the policy that has been developed through conversation with people in the organisation … Policy being developed in such a way that it actually consults the end users, because if the security function just develops the policies in a vacuum, they may not understand how everybody needs to work … if you go and speak to people in the business and say, we need to put this in as a policy, how does that impact your work? Would it work for you, is it feasible? … having that conversation where people actually have an input in the policy and also feel a sense of ownership over it. (Janet, Information Security Consultant)

We can understand from the above comments that while some organisations were described by security managers as struggling to develop digestible and feasible security policies, a useful way of overcoming such difficult challenges was to have good levels of inclusion of end users during the development process of security policies.

In the context of guardianship of information, this suggests that inclusion of end users may help to ensure that security policies are fully understood and fully aligned with the different sets of responsibilities they may have in relation to their job roles. As a result, this may reduce the likelihood of end users failing to understand security policies and/or for potential conflict between different sets of responsibilities, which in turn may ensure higher levels of willingness towards protecting information in organisations are maintained.

5.4.5 Policy awareness and communication

Even though an organisation might have developed a security policy with good levels of digestibility and feasibility (whether through inclusion of end users or not), security managers described how it will not serve to influence security behaviour if end users were not properly made aware of the existence of the security policy and were encouraged to read through it. Hence, security managers described the importance of effectively communicating security policies throughout an organisation. For example, one security manager commented,

> There's no point in developing a new policy with loads of good stuff in it if people aren't aware of it. (Ronald, Information Systems Security Analyst)

Similarly, another security manager commented,

> You can have the best policy in the world but if people don't know about it, then it does no good … Nobody off their own bat goes and reads policies … you kind of need to take them to people. (Janet, Information Security Consultant)

As part of the communication process of security policies, security managers described how organisations must ensure security policies are easily locatable, are available in both digital and physical format, and that regular communications be sent out to encourage end users to access and read them. Further, security managers described numerous occasions where security policies can be sign-posted, including during an initial induction to an organisation, as part of regular email communications sent to end users (which can be supported by upper management), or during the delivering of various SETA programmes. As one security manager commented,

> Policies should be stored where any user can readily access them … and their existence made clear at key gates in the user's experience with the organisation … employee induction, periodic refresher training, and employee annual reviews. (Ewan, Security and Risk Management Officer)

However, despite the above declaration, security managers described how many organisations were failing to effectively communicate security policies to end users. For example, one security manager commented,

> It's often interesting, when you're doing an assessment to ask, ‘Where are your policies?’ and people will be like, ‘I don't know’ … if an end user doesn't know where the policies are, that's their organisation failing them. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> Part of the assessments that I do … I would say, probably, 80% of all companies have policies that users have never seen … That’s disconcerting. What’s the point then of having a policy. (Eveline, Information Security Consultant)

A related problem with the communication of security policies was many organisations were described as only making efforts to communicate certain legal and/or regulatory documents to end users, such as the Data Protection Act, to make sure they were compliant. Therefore, security managers described how many organisations were overlooking the need to develop and communicate specific organisational security policies. For example, one security manager commented,

> I go in and do focus groups with people like end users from different parts of the business … And it’s always the same; people generally aren’t aware of policy … they have read the Data Protection Act, something about GDPR, but in general there is very low awareness. (Janet, Information Security Consultant)

The problem with this situation as described by security managers was, while it is important for end users to be made aware of and understand the Data Protection Act, this was not sufficient for the purposes of protecting information in organisations, where organisations had to also ensure they were developing specific organisational security policies and effectively communicating these to end users. As one security manager commented,

> The Data Protection Act is all about how organisations are allowed or not allowed to use data, and the policies themselves are actually very different … There will be elements in the policy which are derived from it, but the policy needs to stand on its own. (Bruce, Senior Information Security Consultant)

Security managers described how the overall consequence of failing to effectively communicate security policies was they will not be effective at managing security behaviour in organisations, which may then introduce various security risks for organisations and end users themselves. For example, one security manager commented,

> There is kind of a disconnect, where people won't be aware of the policy and … it minimises expectation around cyber security. It means that individuals often don't know what they are supposed to do … for the organisation this then opens them up to risk, where people are engaging in more risky behaviour than they would have liked. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> You tell your staff … you've got to sign it and send it back … to say that you've read the policy. Most people haven't, and … you've put yourself in a really bad position … if people don't effectively understand their responsibilities they may then fall into that category of negligence because they don't know what's expected of them. (Stewart, Senior Information Security Consultant)

Consequently, those security managers interviewed stressed the importance that organisations properly communicate security policies to ensure end users are fully aware of their organisational responsibilities towards protecting information. The above finding is important because it suggests that insecure behaviours such as non-compliance with security policies may be caused by organisational failings, such as the poor communication of security policies.

In the context of guardianship of information, this also suggests that the levels of guardianship of information may be greatly reduced if security policies are not properly communicated, where end users will potentially have less understanding towards their organisational responsibility towards protecting information. As a result, this may introduce various security risks to organisations and end users themselves (as they are still held accountable for the protection of information).

5.5 The influence of security education, training, and awareness programmes on security behaviour

As discussed in chapter three, the theoretical framework used in this study is primarily based upon the Routine Activity Approach, which states the willingness and capability to perform protective actions forms the basis of effective guardianship. Furthermore, the level of willingness and capability of guardians to perform protective actions may be influenced by their levels of knowledge and experience surrounding various threats and the protective actions they must perform.

In the context of information security management, this suggests that the willingness and capability of end users to protect information may be improved via the development and implementation of SETA programmes which (1) improve the levels of awareness and understanding of end users towards general information security concepts and issues through security awareness and security education, which influences their level of willingness to protect information, and (2) improve the skills and abilities of end users to perform security actions through security training, which influences their level of capability to protect information. Therefore, this next section presents the findings relating to security managers experiences of developing and implementing SETA programmes in organisations and how these influence the security behaviour of end users.

5.5.1 The what, the why, and the how of protecting information

During interviews with security managers, the terms security awareness, security education, and security training were often used interchangeably and/or in some combination by security managers (e.g., ‘security awareness training’ or ‘security education training’ or ‘security awareness education’) which made data analysis extremely difficult. However, data analysis revealed that security managers generally described both the concepts of security awareness and security education as corresponding to closely related aspects of SETA programmes, while security training corresponded to further and different unique aspects. Thus, most cases of using terms interchangeably was between security awareness and security education; although security managers would sometimes describe ‘training on security awareness’ or ‘training on security education’, which was still considered different from general ‘security training’. Hence, a useful way to overcome this confusion and to understand how SETA programmes influence security behaviour of end users, is through understanding the *What*, the *Why*, and the *How* of protecting information in organisations – as will now be presented and discussed.

5.5.1.1 The what and the why of information security: Security awareness and security education

As mentioned, during interviews, the concepts of security awareness and security education were the two terms most used interchangeably by security managers**.** Yet, whether security managers used the term security awareness or security education, it usually corresponded to the *What* and/or the *Why* aspect of protecting information in organisations. For example, the What aspect referred to end users’ understanding of what the different threats and vulnerabilities are in information security, and the impacts of security breaches. Similarly, the Why aspect referred to end users’ understanding of why it is important to protect information in organisations and why end users must behave securely; which typically connected back to the What aspect. For example, when discussing the concept of security awareness, one security manager commented,

> What the threats are to the business and how it will impact them, that’s the awareness piece. (Billy, Senior Information Security Consultant)

Similarly, another security manager described the concept of security education as corresponding to:

> What is ‘personal’ data? … And what are the consequences if you lose this? … end users should also know this because you’re allocating responsibilities and accountability … That doesn’t mean they have to know everything about security. It means they need to know enough within what they do. (Carol, Chief Information Security Officer)

We can understand from the above comments that the concept of security awareness and/or security education corresponded to the What and the Why aspect of protecting information in organisations, which provided end users with the knowledge base to better understand the importance of protecting information and what the various threats, vulnerabilities, and impacts are from security breaches, and therefore why it is important to behave securely.

In terms of the guardianship of information, this suggests that end users’ understanding towards the What and the Why aspects of information security may improve their levels of knowledge and experience towards various cybercriminal activities that are likely to target organisational information, and what the consequences were for organisations should they fail to act as guardians for information. Which may then influence their level of willingness towards protecting information.

5.5.1.2 The how of information security: Security training

Although the What and the Why aspects were described as important towards improving the level of willingness of end users, there was still the need to make sure end users were capable at protecting information. Thus, security managers described the concept of security training as corresponding to end user knowledge and experience towards how to perform certain security actions to mitigate or reduce the various threats, vulnerabilities, and impacts that end users had learnt as part of the security awareness/education aspect of SETA programmes. For example, one security manager commented,

> Whereas security training I see more of … showing you exactly how you would then apply those principles that you have learnt. (Christopher, Head of Security Operations)

Similarly, another security manager commented,

> You're educating people on different concepts … The training stage is where you're getting people to the next stage where they are experiencing something … it can be training on how to use the technology … The training is trying to empower people … So, there is a difference between education and training. (Morris, Principal Security Manager)

We can understand from the above comments, that the concept of security training was described by security managers as corresponding to the How aspect of protecting information, which provided end users with enough knowledge and experience towards how to perform certain security actions to properly mitigate or reduce the various threats and vulnerabilities connected to organisational information.

In terms of guardianship of information, this highlights the importance of instructing end users how certain protective actions should be performed to make sure they become confident in their own abilities and that they are sufficiently capable towards protecting information.

Importantly, although each security concept was described as corresponding to different aspects of SETA programmes, security managers stressed that all three aspects had to be present for SETA programmes to be effective. This was because all three aspects of protecting information had to be present to ensure end users were both willing and capable towards protecting information; as having willingness without capability or capability without willingness was ultimately of little use in practice. For example, one security manager commented,

> You have to tie them together. With the awareness, you sit them down and you tell them this is the attacks that are going on against

> us on a daily basis … you say this happened to this organisation or this person, and then you say to mitigate it or prevent it this is what you do … Awareness is the why, the training is the how … If you don't have the why the how doesn't matter." (Billy

Similarly, another security manager commented,

> You want the Why first, or you weave together the What and the Why … this is the threat and this is why it matters, and going into details about different types of threat, and then showing why that matters to people in the room … and then the follow up of, and this is how you protect yourself … these are the mitigations we are suggesting … for me, when I'm doing what I call awareness-raising training or what my client would call awareness-raising training, I am trying to hit all three of those. (Janet, Information Security Consultant)

Lastly, although security managers treated each of the three security concepts as separate and equally important, they often stated that such differences were often overlooked in practice, where many organisations focused too much on the How (e.g., simply telling end users what security actions they must perform) with very little emphasise on what the various threats are in information security and why certain security behaviours are important to the organisation. As a result, the SETA programmes often developed and implemented in organisation would be overall ineffective at influencing both the willingness and capability of end users. For example, one security manager commented,

> If I'm told I can't do this or I can't do that, I'm just going to see security as a blocker … explain to me what the implications are for me not having this, explain to me what the risk is, you treat me like an adult … then I'm going to take that responsibility onto myself because I don't want that negative impact to happen … And I find in security we don't do that … we don't have a sensible adult conversation about the impacts of not deploying good security

> hygiene. And that's why security is often seen to be this blocker.
> (Stacey, Chief Security Consultant)

Thus, we can understand that overall, security managers described the purpose of SETA programmes as developing and improving end user knowledge and experience towards the What, the Why, and the How of protecting information in organisations. Furthermore, an effective SETA programme was described as beginning with the development of knowledge and understanding of the basic concepts of information security (through security awareness/education) which was then followed by demonstrations and practice (through security training) towards the security actions that protect information in organisations. The former focusing upon improving the level of willingness of end users and the latter focusing upon improving the level of capability of end users.

Such findings are of significance because previous studies have highlighted that in practice, the terms security awareness, security education, and security training are often used interchangeably, which often causes major confusion when developing and implementing SETA programmes (Tsohou et al, 2008; Amankwa, 2014). Thus, the above findings from interviews with security managers suggest that a novel way to overcome such confusion in practice may be to understand SETA programmes instead via the What, the Why, and the How aspects of protecting information in organisations.

5.5.2 Developing and implementing effective SETA programmes

Once security managers had described the purpose of SETA programmes in relation to the What, the Why, and the How aspects of information security, interviews shifted towards describing how to effectively develop and implement SETA programmes in organisations.

It is important to note that while the term 'training programme' or 'training session' will mainly be used when discussing development and implementation of SETA programmes, such terms also imply aspects of security awareness and/or security education being present. Again, this is largely due to the way in which security managers used certain terms interchangeably and because any security programme, as mentioned above, was assumed to have all three aspects of awareness, education, and training contained within it – regardless of the name given to it by security managers.

When discussing the development and implementation of SETA programmes, security managers described two main delivery methods, computer-based training and face-to-face training. Each will now be presented and discussed.

5.5.2.1 Computer-based training

The first main delivery method was *computer-based training* (CBT) which typically involved end users completing an online e-learning module or course, which would be uploaded to an organisation's intranet and which had to be completed by a certain date. Further, end users were normally required to pass a test at the end of the module or course. For example, one security manager commented,

> Bigger organisations, they tend to provide online training on an intranet, and people are expected to do that every year. So, they go through the training on the intranet and then they get asked questions at the end of that. (Kevin, Senior Information Security Risk Manager)

Security managers described computer-based training as the most commonly used delivery method when implementing SETA programmes in organisations for two main reasons. The first reason was it was cheap and easy to implement. This was described as particularly useful for organisations which had a large number of end users that needed to be trained on information security. For example, one security manager commented,

> We all know why people do e-learning, because it's cheap, it's easy … you can buy if off the shelf, push it out to everybody via a link. (Stewart, Senior Information Security Consultant)

Similarly, another security manager commented,

> If you've got over a thousand users, then putting them through that online e-learning makes a lot of commercial sense because it is cheaper. (Bruce, Senior Information Security Consultant)

Such findings reiterate those of previous studies which have shown that because computer-based training provides organisations with the ability to quickly and cheaply train large numbers of end users to an organisation-wide standard, they often become the most popular choice for organisations when delivering SETA programmes (Abawayjy, 2014).

The second reason described by security managers for the popularity of computer-based training was because organisations can demonstrate compliance with various legal and/or regulatory requirements. For example, one security manager commented,

> The CBT is very good for compliance. Very good to say to a regulator … we can demonstrate that 100 percent of our employees have gone through this programme twice a year. And they've got a pass-rate. (Morris, Principal Security Manager)

A previous study by Alkasihk et al (2018) argued there are two main approaches towards the use of SETA programmes to manage security behaviour in organisations. The first is the *formal approach* which uses various delivery methods and teaching techniques, and where programme effectiveness is continually measured and internally and externally audited by the organisation to ensure continual improvement. In contrast, is the *ad-hoc approach*, which relies upon various statistics and completion rates in order to evidence that a given organisation has fulfilled various security requirements (Alkasihk et al, 2018). Thus, the above findings suggest that some organisations are perhaps favouring an ad-hoc approach when it comes to delivering SETA programmes to end users, where computer-based training is primarily used to enable organisations to meet various legal and/or regulatory security requirements.

Importantly, despite computer-based training being the most popular delivery method chosen by organisations when implementing SETA programmes, security managers did not describe it as particularly effective in terms of improving end user security behaviour. For example, one security manager commented,

> I'm not convinced that that is the best way to train everybody at everything … But at the end of the day, the cheapest and the most effective in terms of the figures you can produce is always going to be computer-based training. I just don’t think it necessarily is reflected in behaviour. (Whitney, Information Security and Risk Consultant)

Similarly, another security manager commented,

> One of the difficulties with online learning is it’s quite often relatively simple to pass the test at the end, without actually understanding any of the material, and I do think sometimes people switch off when they’re doing online learning. (Kevin, Senior Information Security Risk manager).

We can understand then from the comments above, that despite many organisations using computer-based training, according to security managers interviewed, it was perhaps not the best option for organisations when attempting to improve the levels of willingness and capability of end users.

It is important to highlight that a potential explanation for the overuse of computer-based training, despite the described lack of effectiveness, may be the insufficient security budgets in organisations, where a lack of organisational resources (which the above findings suggest may be an issue for some organisations) might cause some security managers to resort to using computer-based training rather than face-to-face training.

To further understand why security managers did not consider computer-based training to be an overly effective delivery method for SETA programmes, it is helpful to explore the second main delivery method for SETA programmes; namely, face-to-face training. The reason being, the various features that security managers described as making face-to-face training effective, were often those features which computer-based training lacked; thus, it should help towards understanding why computer-based training is potentially less effective at improving security behaviour.

5.5.2.2 Face-to-face training

Security managers generally described face-to-face training as involving classroom-based teaching involving one or more security managers and a group of end users. However, security managers stressed that while face-to-face training was their preferred delivery method for SETA programmes, to effectively change security behaviour, face-to-face training still had to be properly developed and implemented. Otherwise this would undermine the overall effectiveness of the face-to-face training programme.

Interestingly, security managers described how they would measure the effectiveness of face-to-face training programmes via the concept of *engagement*. The concept of engagement was generally described as referring to the level of impact face-to-face training had upon end users' interest towards learning about information security and their subsequent ability to protect information during their everyday work routines. As illustrated by the following comment:

> Engagement for me is, someone who is sitting up and listening to what it is you are trying to say. It is someone who is actively participating in taking in the information that you are giving them. And, for me, what it really means is they will go away and change their behaviour. So, you can do all the awareness-raising you want, but if it doesn't actually lead to more positive behaviour, then for me it hasn't properly been engaging. So, when you are doing the awareness-raising training in whatever form it is, you want people who are really actively listening, asking questions, relating what you are saying to what they do, and reflecting on how they behave with information. (Janet, Information Security Consultant)

We can understand from the above comment that security managers generally considered the overall effectiveness of face-to-face training to be usefully measured by the levels of engagement of end users. The argument being, the higher the levels of engagement of face-to-face training, the more end users will be influenced by the face-to-face training sessions, which in turn improves their security behaviour.

In terms of the guardianship of information, this suggests that higher levels of engagement of end users towards face-to-face training may help improve the levels of willingness and capability of end users towards protecting information; where low levels of engagement may lead to reduced levels of willingness and capability towards protecting information.

Interestingly, security managers described several techniques which they used during the development and implementation of face-to-face training to help ensure high levels of engagement for end users. Thus, to ensure higher levels of engagement, security managers recommended that organisations adopt the following techniques.

5.5.2.3 Tailor face-to-face training to end user job roles

Security managers described how engagement in face-to-face training sessions can be improved by tailoring the training material to end user job roles. In other words, organisations must take into consideration the types of security behaviours end users are likely to perform in their everyday work routines and focus the training material around this.

For example, the What, the Why, and the How aspects can focus on the specific job roles of those attending and the various threats and vulnerabilities they are likely to face, and the specific security actions they are likely to perform in those job roles to mitigate those threats and vulnerabilities. This way, the face-to-face training will ensure end users are engaged by avoiding any irrelevant information which might reduce their levels of engagement. For example, one security manager commented,

> The main thing is, in my opinion, is to understand exactly what that end user is doing … and it's not giving them more than they need to

> know … So, an IT department, or a team of administrators, is going to need a far more extensive, far more technical set of training than a call-centre agent, and a call-centre agent is going to need a different focus of training to a salesperson on a shop-floor, for example. (Amanda, Information Security Manager)

Similarly, another security manager commented,

> I did one in-house and … that one was quite precise because we knew exactly what their jobs were, and we could tailor that to exactly what they were trying to do … Generally, you have to align or pitch the training at that level. (Billy, Senior Information Security Consultant)

We can understand how this may relate back to why security managers described computer-based training as a less effective delivery method. For instance, with face-to-face training it is possible to tailor training materials to end user job roles, which meant security managers could ensure higher levels of engagement. Whereas because computer-based training had to be more standardised, due to it being delivered to a larger group of end users, who will vary in their job roles, it will ultimately be less tailored and potentially less engaging; which again may reduce its overall effectiveness at improving the willingness and capability of end users. Indeed, when discussing why computer-based training is less effective, one security manager commented,

> You're not understanding anything about them [end users] before you deliver it to them … most people won't understand why they're having to do it. (Billy, Senior Information Security Consultant)

Similarly, another security manager described most computer-based training as ineffective because the training material was often not relevant to end user job roles, further commenting,

> People sit down in front of their workstation and think, 'How does that apply to me? Does it apply here? Does it apply here? … if they

> can't see how it's relevant to their role, you're always going to struggle. (Ronald, Information Systems Security Analyst)

Importantly, while security managers described face-to-face training programmes as potentially more effective because training materials can be tailored to end user job roles, they described how many organisations in practice were not taking advantage of this. The main explanation for this was most organisations were trying to demonstrate compliance with various legal and/or regulatory requirements for security training, such as those relating to the Data Protection Act or GDPR. Thus, even though some organisations had implemented face-to-face training programmes, they were more focused towards ensuring compliance rather than improving the levels of engagement for end users, which meant less emphasis was placed on tailoring those face-to-face training sessions. For example, one security manager commented,

> I think the problem is organisations are trying to tick a box. They are trying to satisfy some compliance … as part of a new arrival brief they have to give a half hour brief on information security or data protection … to satisfy that requirement. So, right from the get-go, no one has really bought into it. (Christopher, Head of Security Operations)

Similarly, another security manager commented,

> The face-to-face training … becomes more of an attendance-based approach … It’s more about whether that particular individual turned up on that day for that particular session. (Norbert, Head of Information Security)

We can understand from the above comments that face-to-face training programmes were described by security managers as more engaging when training materials were tailored to end user job roles. Further, because it is easier to tailor face-to-face training sessions than computer-based training, security managers described this as a more effective delivery method. Lastly, security managers felt that many organisations were failing to tailor training materials when delivering face-to-face training sessions due to having a more compliance-based approach.

The above findings again suggest that some organisations may be adopting an ad-hoc approach towards managing security behaviour in organisations. However, previous studies have shown that focusing too much on being compliant with various legal and/or regulatory requirements tends to have a negative impact upon the level of quality and therefore effectiveness of SETA programmes towards improving security behaviour in organisations (Alkasihk et al, 2018).

In the context of guardianship of information, this suggests that organisations may benefit from tailoring SETA programmes to include only information that is relevant to the job roles of end users as this may help to improve the overall levels of engagement, which may then positively influence the level of willingness and capability of end users to perform protective actions.

5.5.2.4 Personalise face-to-face training material

The next technique described by security managers to improve the levels of engagement for end users, which was somewhat an extension of the previous technique, was to tailor training materials in relation to the personal lives of end users rather than their job roles, or to have group discussions where the topics of conversation were the problems end users were having outside of work (in terms of keeping information safe). Thus, security managers described how using the theme of improving security behaviour in 'home life' as opposed to 'work life' helped to improve the levels of engagement of face-to-face training. As one security manager commented,

> All my user-awareness training is about *you*: your personal data; your friend's data; your family's data … What I find is, when I deliver in personal terms to individuals, I change their behaviour in their personal life, and they bring those good behaviours into work. So, I very rarely speak to anybody about 'security at work' … Change their behaviour outside so that they're getting benefit as an individual …

> and they bring that in the workforce. (Gordon, Chief Information Security Officer)

An illustrative example was provided by one security manager towards the possible benefits of this technique. He described how another security manager had previously struggled with delivering a face-to-face training session where despite the training session being mandatory for end users, there was very poor attendance. However, when the training material was changed to 'protect yourself at home', he experienced a significant difference in attendence. Thus, he commented,

> It wasn't mandatory, it was voluntary … and he had a ridiculously high turnout … and he had some personal stories he told … What he was doing was telling people to have secure passwords … make sure you back stuff up, make sure you use malware and all that kind of stuff. But what he was really doing was explaining why it is important at work … and he was very engaging for the audience, and he had a very high success rate. And I don't mean people turning up, I mean being able to see people make a change. (Morris, Principal Security Manager)

Again, we may understand why security managers generally described computer-based training as less effective because its main use (or the main reason it was commonly used in organisations) was to target large numbers of end users, and the training material was often focused on various legislation or regulations due to organisations having a more compliance-based approach. Thus, training material will necessarily focus on that, rather than on the personal lives of end users. Indeed, previous studies have shown that presenting training materials in this way may prove effective towards increasing the levels of interest end users have towards learning about information security (Alaishk et al, 2018; Puhakainen and Siponen, 2010).

Having said that, as mentioned above, security managers described most organisations as failing to tailor the training materials for face-to-face training sessions; thus, extending this problem to the personalisation of face-to-face training sessions, this too was described as often not done in practice. As one security manager lamented,

> I think there is some immaturity surrounding that space … there is a lot of techniques that are being missed. Certainly, from my experience in terms of how that training should be delivered. (Norbert, Senior Information Security Consultant)

We can understand from the above comments that face-to-face training sessions were described as potentially more engaging for end users when the training material was tailored towards making sure end users behave securely both during and outside of work, where improvements in their behaviour outside of work meant they were more likely to behave securely at work.

In the context of guardianship of information, this suggests that improving guardianship of information in general may also prove to be an effective way towards improving the levels of willingness and capability of end users towards protecting information in organisations.

5.5.2.5 Make face-to-face training interactive

The next technique described by security managers to improve the levels of engagement for end users was to make the face-to-face training sessions interactive. The interactivenesss of face-to-face training referred to both the level of interaction between security managers and end users, and the level of interaction amongst end users themselves. Security managers described how interaction during face-to-face training sessions would create improved levels of engagement because it allowed end users to communicate directly with security managers and to ask questions; whether this was because they failed to understand the training material or wished to know more about a particular concept, or because they were unsure as to how a certain concept applied to certain situations in their job role, and so on. Interaction also allowed end users to discuss amongst themselves various aspects of protecting information in their everyday job roles which improved their levels of understanding of the types of knowledge and experience they shared as a group, which would again improve their engagement during the face-to-face training sessions. As one security manager commented,

> If you're doing training, it's not just a case of ... I'm going to throw all this at you ... because that never works well in training... you need to engage them in the training; get them talking, get them asking questions, get them raising points, finding out if they've come across any of these things before. What is their experience? And you'll find, when you do training, people are willing to share that in the room, and that's what creates the engagement. (Lesley, Information Security Analyst)

An illustrative example was provided by one security manager who described the delivering of a ‘cyber work day’ in one organisation, which included several workstations that enabled end users to interact with several security managers and other end users. She commented,

> With one client we had … different workstations set up, and at one of them people were doing lock-picking … they were trying to unlock a box and inside it there was sweets that they could take away. At another one … we put together this fake persona – this online person – and it was having a look at their social media profile and then writing a phishing email, you know … and people then got really into it … so, it’s looking at it from a slightly different way, and thinking what can we do to make it interesting and engaging. (Janet, Information Security Consultant)

Again, we can understand why security managers may have described computer-based training as less effective than face-to-face training because end users arguably have less opportunity to ask questions or to be involved in group discussions with security managers and other end users. For example, one security manager commented,

> I’m dyslexic, perhaps the worst thing in the world you could give me is e-learning … but if you give me somebody who is talking in a room

> and I can ask questions, I can understand the concepts and the Why's, I'm much more engaged with it, and there is lots of people like me. (Stewart, Senior Information Security Consultant)

Similarly, another security manager commented,

> People don't engage if you ask them to just click through some online training where it is just some text on a screen … it doesn't bring it to life for them at all. So, most people are going to click through that as quickly as they can. They are not really going to take that information in, and certainly not retain it. (Janet, Information Security Consultant)

The above comments made by security manager are reminiscent of previous studies which have shown higher levels of interaction between those delivering training sessions and those attending can lead to improved effectiveness of SETA programmes and ultimately better retention of information by end users (e.g., Albrechsten, 2007; Albrechtsen and Hovden, 2010).

Importantly, despite this additional advantage of face-to-face training over computer-based training, security managers again described how many organisations in practice were not delivering face-to-face training that was interactive, where end users instead were simply presented with basic information about what security actions they must perform to be compliant, with little room for group discussion. For example, one security manager commented,

> It's not, go and broadcast some message and then pat yourself on the back … Then forget it for the next 6 months … I think the fact that it needs to be two-way is often overlooked. (Morris, Principal Security Manager)

Similarly, another security manager commented,

> Too often, InfoSec is us telling people what they should do … They are not given the training in a way that is interesting and engaging,

> and interactive, and in a way that it actually lasts with them. (Janet, Information Security Consultant)

Thus, we can understand from the above comments that face-to-face training sessions were described by security managers as more engaging for end users if they were interactive. The main reason for this was it enabled end users to directly communicate with security managers and other end users, which enabled them to ask questions and to share their knowledge and experiences amongst the group.

In terms of the guardianship of information, this suggests that the levels of knowledge and experience of end users can potentially be improved by allowing end users to have in-depth discussions with both security experts and colleagues, which allows them to better understand when and where various protective actions can be applied during their job roles. Further, they can ask for advice, additional information, and it gives security experts the opportunity to measure the levels of knowledge and experience of end users and to assess whether they may need more or different types of training. Which may then help improve the overall levels of willingness and capability of end users to perform protective actions.

5.5.2.6 Make SETA programmes inclusive

The last technique described by security managers to improve the levels of engagement for end users was to include end users in the decision-making processes surrounding SETA programmes (similar to the development processes of security policies). The notion of inclusion was generally described as when organisations attempt to gain feedback or input from end users about the quality of the training they were receiving to help improve the overall effectiveness of SETA programmes. For example, end users can comment on the training material in terms of the relevance of the training material to their job role or the level of difficulty towards understanding the training material. It will also offer the opportunity for end users to request more or less types of security training. As one security manager commented,

> It’s a fantastic opportunity for the trainer or the trainers to extract information back … what’s working and what isn’t and why. How can

> it be improved? … did that work for you? Was it enough or was it too much? Was it a bit too complicated? (Morris, Principal Security Manager)

Overall, security managers believed this would ensure SETA programmes were understood by end users to be *their* SETA programmes, rather than the SETA programmes of the organisations they worked for; and so, end users would then be more likely to engage if they had more control in terms of development and implementation. Indeed, security managers described how many end users might prefer computer-based training (despite the views of security managers towards its effectiveness). If this were the case, then organisations should try and accommodate this variability by providing a mixed method approach. For example, one security manager commented,

> Some people need to hear it, some people need to see it, some people prefer to read it … whatever method the end users find most effective is how the organisation needs to proceed. (Barry, Principal Security Architect)

But of course, this understanding would only become available to organisations if end users were included in some way. To create inclusion, security managers described either allocating time at the end of training sessions to discuss different aspects of the training material or to implement specific communication channels that end users can use to provide their input.

Interestingly, while face-to-face training was generally described as more effective than computer-based training in relation to the previously discussed techniques, inclusion via computer-based training was not considered to be problematic. In fact, this was one area where computer-based training was perhaps more effective. But again, in practice, organisations weren't necessarily trying to receive feedback from end users (either during face-to-face training or computer-based training). As one security manager commented,

> Organisations should be looking for constant feedback … And that’s something that organisations unfortunately still don’t do to this day … some organisations will say they don’t have the time, or the expertise and capabilities to do that. But I would argue you can always start small and grow. (Morris, Principal Security Manager)

We can understand from the above comments that SETA programmes were described by security managers as more engaging for end users when they were included in certain decision-making processes surrounding the development and implementation of SETA programmes. By enabling end users to have their input regarding both the training material and delivery method of SETA programmes, security managers described this as potentially creating higher levels of engagement.

In the context of guardianship of information, this suggests that by allowing end users to communicate with organisations about the effectiveness of SETA programmes, this may also prove an effective means to improve the levels of willingness and capability to perform protective actions and keep information safe.

Security practitioners have previously argued that evaluation and feedback mechanisms are critical components of SETA programmes. Therefore, the continuous improvement of SETA programmes requires some level of understanding towards existing SETA programme effectiveness. Thus, following the implementation of SETA programmes in organisations, there must be processes put in place to monitor compliance and effectiveness (Wilson and Hash, 2003).

In addition, Peltier (2005) argued by having end users more involved in the decision making processes and accepting end user recommendations whenever possible, SETA programmes will truly become the SETA programmes of end users, where they will be more willing to accept and adhere to security requirements.

5.6 The use of monitoring and enforcement practices

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness to perform protective actions forms part basis of effective guardianship – the other being the capability to perform protective actions.

In addition, the Rational Choice Perspective suggests that the willingness of guardians to perform protective actions may be improved by managing both the risks for failing to perform protective actions and the rewards for successfully performing protective actions.

In the context of information security management, this suggests that the willingness of end users to protect information may be improved via monitoring and enforcement practices which (1) monitor the security behaviours of end users, and (2) punish and/or reward end users for either positive or negative security behaviour. Therefore, this next section presents the findings relating to the experiences of security managers of monitoring and enforcement practices in organisations.

5.6.1 The monitoring and enforcement of security behaviour: Good in theory, bad in practice

During the analysis of interview data, one of the major themes which emerged was the ineffectiveness of monitoring and enforcement practices for managing security behaviour in organisations, which security managers generally described as 'good in theory but bad in practice'. For example, during interviews, many security managers initially described monitoring and enforcement of security behaviour as a potentially effective method towards managing security behaviour.

Security managers generally described how end users were more likely to be willing to protect information if they knew they were being monitored and that failure to perform protective actions would result in punishment. As one security manager commented,

> Making them realise there's consequences of not following these policies … That will motivate them in a lot of instances. (Lesley, Information Security Analyst).

Similarly, another security manager commented,

> One thing that you need to do is punish those who don't follow the rules … if you don't have any punishment for people who don't follow the rules, a lot of them won't. (Nadine, Information Security Analyst)

However, although monitoring and enforcement was described as a potentially effective way to manage security behaviour in organisations, there were often numerous challenges for security managers when trying to implement such practices; which brought into question the suitability of monitoring and enforcement as a means of managing security behaviour.

During interviews, security managers described the following challenges to support their position towards the overall ineffectiveness or unsuitability of using monitoring and enforcement of security behaviour.

5.6.1.1 The costs of monitoring security behaviour

The first challenge described by security managers was the associated costs of monitoring security behaviour. The costs included organisations purchasing and implementing the required security controls and then employing security managers with the right levels of expertise and time to manage them effectively. For example, to monitor security behaviour in organisations, security managers generally described this as performed via the use of advanced technology. However, the costs of purchasing and implementing such advanced technology were described as very prohibitive. As one security manager commented,

> Cost is often a huge inhibitor with these things … even for a thousand user organisation, you might be looking at a six-figure implementation … and their whole budget might even be that six-

> figure sum … And when you have so many hundred devices … that could be someone’s full-time job, just monitoring those logs. (Derek, Information Security Officer)

The above costs of monitoring were made even worse when it came to smaller organisations, who had even less resources. As one security manager commented,

> There’s an issue though … people not being able to sift through … all the data and actually manage what’s happening … For a small business, it can be really challenging to kind of have that monitoring in place. (Janet, Information Security Consultant)

Indeed, the negative influence from the costs of monitoring and enforcement were considered so great that security managers described how many organisations were often not properly performing monitoring (or even failed to start monitoring). For example, one security manager commented,

> There’s lots of ways to monitor compliance with controls but again it can become very costly … to implement them and manage the tools effectively … and most organisations don’t even try really. (Billy, Senior Information Security Consultant)

Similarly, another security manager commented,

> These things are going to get overlooked, and I’ve seen that happen so many times … even though these things are stipulations within all sort of regulations, and also the cornerstone of information security is to have this monitoring … you’ll come across large organisations who are yet to even adopt monitoring controls. (Derek, Information Security Officer)

We can understand from the above comments that although monitoring of security behaviour was described as an important aspect of information security management, many organisations were described as struggling to achieve this in practice due to the associated costs of purchasing and implementing monitoring controls, and the costs of hiring security managers with sufficient levels of expertise to manage those controls effectively.

In terms of the guardianship of information, this suggests that while the risks to end users for failing to protect information may, in theory, help improve their levels of willingness; in practice, many organisations may struggle to provide the perceived sense of severity and certainty of punishment required to influence the associated risks of failing to protect information. As a result, monitoring and enforcement may overall prove to be an ineffective security control towards managing the protection of information in organisations.

5.6.1.2 The effectiveness of supporting security controls.

The next challenge described by security managers was the legitimacy of monitoring and enforcement of security behaviour was dependent upon organisations having already developed and implemented supporting security controls, such as security policies and SETA programmes. Moreover, such supporting security controls had to be of a high standard before an organisation can legitimately monitor and enforce security behaviour.

For example, security managers described how organisations cannot legitimately punish end users for behaving insecurely if they have not been made aware of their organisational responsibilities and properly shown how to perform various security actions. Therefore, if end users have not been made aware of the existence of security policies nor been encouraged to read them, as well as not having received any SETA programmes (which the findings above suggest may often be the case), then end users should not be punished for their failure to adequately protect information. As one security manager commented,

> A lot of organisations when they have a problem will look to apportion blame to an individual. And that to me is fundamentally flawed because most people won’t deliberately do wrong … To me, almost all incidents will link back to an organisational failing rather

> than individual failing. (Stewart, Senior Information Security Consultant)

Because of this, security managers described how monitoring of security behaviour should alternatively be used to help identify problems with security controls rather than problems with end users (although the above problem of high costs would still apply in this situation). For example, one security manager commented,

> I prefer to go and talk to people and try to understand what they were trying to do … understand if the actual reason why they've done that particular thing was down to one of the controls we've put in place. (Norbert, Head of Information Security)

Similarly, another security manager commented,

> Most policy violations are because the policy was stopping them from doing what they needed to do so they violated it in order to do business, or they violated it accidently because they weren't aware of it … the problem is somewhere else not with those individuals. (Bruce, Senior Information Security Consultant)

Importantly, security managers acknowledged that some end users will behave insecurely despite there being effective supporting security controls in place. And in these situations, security managers described how the security behaviour in question should certainly be punished by the organisation. For example, one security manager commented,

> Obviously, if someone is wilfully negligent, if someone is malicious, then of course you have to punish them. But if you are punishing people for making an honest mistake, and if you are punishing people in an attempt to use that as a way of changing people's behaviour, it's likely not going to help. (Janet, Information Security Consultant)

Unfortunately, security managers described how some organisations do not recognise this aspect of monitoring and enforcement, where many end users are being punished despite there being a lack of effective supporting security controls in place. For example, when discussing whether organisations should monitor and enforce security behaviour, one security manager commented,

> As long as you have a strong security policy framework in place … because there is a foundation that needs to be in place before you start going to do that … I have seen disciplining in organisations where the policy hasn't been written. (Morris, Principal Security Manager)

Similarly, another security manager commented,

> Things like e-learning and policies are often used as sticks to beat people with … 'you did your training, you know what the policy is, yet you still did the wrong thing. So, you are incompetent.' Well actually, that may well not be the case. The training wasn't very good … the policy is one big policy, its 150 pages long … have we effectively told that person how to do their job? (Stewart, Senior Information Security Consultant)

We can understand from the above comments that monitoring and enforcement practices, while described as good in theory, were often not suitable in practice due to the requirement of effective supporting security controls, which for many organisations were not in place. As a result, security managers described punishment as an illegitimate and potentially counterproductive security control when managing security behaviour in organisations.

In the context of guardianship of information, this again suggests that monitoring and enforcement practices may not be an effective way to improve the levels of willingness of end users towards protecting information in organisations, unless supporting security controls have been effectively developed and implemented. Similar concerns towards the legitimate use of monitoring and enforcement practices have been raised elsewhere. For example, Lowery (2002) argued monitoring and enforcement of end user security behaviour should not take place until end users have been properly made aware of the existence of security policies with which they must comply and are sufficiently trained/educated on information security. Thus, the findings again highlight the problem of organisations not properly communicating security policies to end users and/or making sure end users are provided with effective SETA programmes prior to conducting any formal monitoring of end user activity.

5.6.1.3 Monitoring and enforcement must be consistent

The next challenge described by security managers was, the effectiveness of monitoring and enforcement practices was also dependent upon whether all members of an organisation were being monitored and enforced, which included the security behaviour of upper management. If monitoring of upper management behaviour did not take place, or enforcement did not follow insecure behaviour, then the effectiveness of monitoring and enforcement practices towards end users was described as drastically reduced; as end users were described as less likely to comply due to feeling discriminated against by their organisation.

Indeed, many security managers believed that upper management behaviour was not being equally monitored and enforced in organisations. As a result, they felt this undermined the effectiveness and legitimacy of monitoring and enforcing of end user security behaviour. For example, one security manager commented

> In my current organisation … there's so many exceptions that the rules are worthless in any case, because ... you can only apply some value to that when everybody is treated equitably. So, if because of who you are, that rule doesn't apply to you, you can't expect it to apply to anybody else. (Gordon, Chief Information Security Officer)

Similarly, another security manager commented,

> If you’re going to start disciplining someone then you need to be disciplining everyone … not just some people and not others … and it is problematic because often working with people and making observations in the organisations I work with … often it’s the business leaders, it’s the executive management, the board of

> directors … people at the very top, who have this view that, ‘Well, that doesn’t apply to us’ … As soon as you have that … then you are not going to be able to implement that. (Morris, Principal Security Manager)

We can understand from the above comments that the effectiveness of monitoring and enforcement was described as dependent upon all organisational members equally being monitored and enforced.

In terms of guardianship of information, this suggests that while end users may understand they have an organisational responsibility towards performing protective actions, they may only take on this responsibility if those around them are likewise honouring such responsibilities and face suitable punishment when they fail to act. Further, such practices can be greatly undermined by the behaviours of super guardians; where if upper management do not likewise perform protective actions and/or are not punished when they fail to act, then end users may perceive this as some form of favouritism, which may then undermine the importance of acting as a guardian for information.

The above findings are especially important because previous studies have argued if an organisation does not consistently enforce security behaviour, then security policies may be considered unimportant by end users, which will reduce their effectiveness in managing information security – which connects back to the above problem of gaining upper management support (David, 2002; von Solms and von Solms, 2004b). Furthermore, previous studies have argued if end users consider themselves unfairly treated by their organisation, they may feel less obligated to follow security policies and may even develop feelings of discontent and decide to punish their organisation (Leach, 2003).

The above findings therefore suggest that monitoring and enforcement practices may prove counterproductive if the necessary supporting security controls are not in place and if certain members of an organisation are perceived to be receiving favourable treatment compared to end users.

5.6.1.4 Lack of reporting security incidents

The last challenge described by security managers surrounding monitoring and enforcement was too much monitoring and enforcement (or too harsh punishments for end users) can often cause a lack of reporting of security incidents, which often then makes the situation worse for security managers as they can only respond and manage security incidents if and when they are reported. As one security manager commented,

> I understand the theory about how we can punish people and then they will behave better in terms of security, but in practice it just isn't an approach that I see working… if someone clicks on a link and they report it, and if they get punished, it won't stop them or anyone else clicking on a link in a phishing email, it will just stop them reporting it. (Janet, Information Security Consultant)

Similarly, another security manager commented,

> If anything constitutes a breach at any point and they think they are going to get disciplined for it then they are more likely to try and contain it themselves … Whereas, if I know I can report that anonymously or report it in a way where I can help the security team deal with it quickly and effectively … then I am more likely to do so. (Stacey, Chief Security Consultant)

We can understand from the above comments that the use of punishments to manage the security behaviour of end users in organisations had numerous limitations in practice according to security managers. While in some situations it may influence the willingness of end users to protect information, in other situations it potentially had a counterproductive influence on their security behaviour, where they would choose not to report security incidents for fear of punishment.

In terms of guardianship of information, this suggests that monitoring and enforcement practices may potentially lead to less guardianship of information in organisations if organisations focus too much on punishing end users for their failure to act.

5.6.2 The monitoring and *re*-enforcement of security behaviour

An additional theme that emerged from the data was the use of rewards in organisations as a possible alternative to punishment-based approaches. Thus, in response to the acknowledgement that many organisations struggled to properly implement monitoring and enforcement practices, for the reasons discussed above, many security managers felt that the use of rewards to encourage and support end users may be a suitable alternative when attempting to improve the security behaviour of end users. For example, one security manager commented,

> When people come to you and say, 'We've discovered X, Y, Z' … That person should be rewarded for highlighting that … We do it for all manner of things anyway … It just changes their mind-set, it refocuses their brain a little bit … There're definitely ways you can incentivise people without having to focus on the negative aspect.
> (Billy, Senior Information Security Consultant)

Interestingly, security managers also described how the use of team-play and reward systems can also be incorporated into the regular monitoring and re-enforcement of security behaviour. This was referred to as *gamification* and typically involved creating teams where various campaigns, such as a phishing email campaign, would be deployed against end users. Security managers then awarded prizes to those teams who managed to successfully identify a phishing email. Thus, rewards were described as becoming a regular feature of SETA programmes which were implemented in organisations; which may also help to improve the levels of engagement (recall earlier discussion about the importance of engagement of SETA programmes). As one security manager commented,

> It's trying to find some way of actually getting users to change their behaviours, and one of the methods I'm hugely fond of … is

> gamification. So, if you think you've got something that might be a phishing email … you flag it and then it gets raised up and you get points for doing that. And you're going to have league tables and awards or prizes … I think there has to be some way of getting end users on our side as opposed to making them feel like it's their fault when something goes wrong. (Timothy, Cyber Security Analyst)

A very illustrative example was provided by one security manager surrounding the potential positive influence of using rewards to improve security user behaviour; she commented,

> For my organisation, phishing is our biggest threat, and so one year … I ran a phishing contest. And I offered everybody who sent my information security team a phishing e-mail that they had received, either on their work account or their personal account, I'm happy with either, they got a raffle ticket … It was an extremely effective piece of awareness, because for five weeks, I had people identifying phishing e-mails, and sending them to the security team. And post-contest, I want every person in the organisation, when they get a phishing e-mail, to go 'That's a phishing e-mail', and to send it to the security team … I still to this day, reap the benefits from that exercise." (Veronica, Head of Information Security)

Lastly, security managers described how because of the powerful influence of upper management, they too should become involved in encouraging and supporting end users for good security behaviour. For example, one security manager described the following experience during a security training session that she was delivering to end users,

> A lady described to me how she was walking in the door and she swiped her card and a guy was tailgating, you know, coming in behind her without swiping his card … and she turned around and said, 'I'm sorry do you have your card?' … and it turned out he was extremely senior in the business. And she was sort of a little

> embarrassed, but his response was, ‘This is brilliant, thank you so much for doing your job’ … And that’s absolutely the response you need. Because that empowers her, and it reinforces the security behaviour. (Janet, Information Security Consultant)

We can understand from the above comments that the use of rewards in managing security behaviour may be an effective way to improve the levels of willingness of end users by encouraging them to behave more securely and to act as guardians for information. However, despite arguing toward the benefits of using rewards to incentivise end users, security managers overall did not consider this a common approach used by organisations, where most organisations continued to rely on a punishment-based approach. For example, one security manager commented,

> I think there is far too much of that … going after people for the bad behaviours rather than rewarding people for the good behaviours. (Norbert, Head of Information Security)

Similarly, another security manager commented,

> Those kinds of things can certainly change people’s attitudes … its far better people are reporting those things and having the mind-set to look out for things … and that is an idea that is not commonly used (Derek, Information Security Officer)

5.7 Summary of chapter findings

Overall, the findings from interviews with security managers showed that upper management support was described as an important factor in managing information security because: (1) upper management influenced the amount of organisational resources available to security managers to develop and implement security controls, and (2) the expectations and observed behaviour of upper management influenced the willingness of end users towards protecting information, where if upper management considered it important, then end users were described as more likely to consider it important. Further, security managers described how upper management can demonstrate the importance of protecting information by assisting security managers during the development and implementation of various security controls.

However, despite the importance of upper management support, security managers overall described a lack of support. The reasons for this lack of support were (1) upper management were reactive rather than proactive towards protecting information, (2) upper management had a lack of understanding surrounding various information security risks, where they considered security breaches unlikely to occur, (3) upper management considered the costs of developing and implementing security controls as too high, (4) upper management still viewed information security as a technical problem, and (5) security managers failed to effectively communicate the security needs of organisations to upper management.

Regarding security policies, the findings showed that the purpose of security policies was to establish the organisational need to protect information and the roles and responsibilities of employees in relation to this organisational need; acceptable and unacceptable behaviours surrounding the use and protection of information within the organisation; and the punishments for non-compliance with security policies. Further, security managers described numerous types of security policies which can be developed and implemented within organisations depending upon the types of information the organisation stored, processed, and transmitted, as well as the different job roles performed by end users.

Additionally, there were many aspects of the development and implementation of security policies that security managers described as important, and which could potentially reduce the effectiveness of security policies towards managing security behaviour. First, security policies had to be digestible to end users to ensure they properly understood them. To ensure digestibility, security managers recommended that organisations (1) tailor security policies to end user job roles, (2) write security policies in a simple language that end users can understand, (3) keep security polices short, and (4) do not copy and paste the security policies of other organisations. Second, security managers stressed that security policies must be feasible for end users, where security policies are properly aligned with the everyday work routines of end users. Third, to ensure security policies are both digestible and feasible to end users, security managers recommended including end users during the development process of security policies, whether through focus groups or interviews. Fourth and last, security managers described how security policies will not effectively influence the security behaviour of end users if they were not properly made aware of the existence of security policies and were encouraged to read through them.

Regarding SETA programmes, the findings showed that the concepts of security education, security training, and security awareness were often used interchangeably by security managers. However, each generally corresponded to the Why, the How, and the What aspects of information security respectively.

In addition, there were two main delivery methods described by security managers. Computer-based training and face-to-face training. Computer-based training was described as the most commonly used delivery method in organisations because it was cheap and easy to implement, and it enabled organisations to demonstrate compliance with various legal and/or regulatory requirements. However, in terms of engagement, computer-based training was not described as equally effective as face-to-face training. Furthermore, security managers described how the levels of engagement in face-to-face training was influenced by (1) the tailoring of training materials to end user job roles, (2) the tailoring of training materials to the personal lives of end users, (3) the levels of interaction between security managers and end users, and (4) the levels of inclusion of end users in the decision-making processes surrounding SETA programmes.

Finally, regarding monitoring and enforcement practices, the findings showed that although monitoring and enforcement was described as a potentially effective way to manage security behaviour in organisations, there were often numerous challenges when trying to implement such practices. First, the associated costs of purchasing and implementing the required monitoring controls and hiring expert security managers to manage them effectively were described as major inhibiting factors. Second, the legitimacy of monitoring and enforcing security behaviour was dependent upon organisations having already developed and implemented supporting security controls, such as security policies and SETA programmes. Third, the effectiveness of monitoring and enforcement practices was dependent upon whether all members of organisations were being monitored and enforced, including upper management. Fourth, too much monitoring and enforcement (or too harsh punishments for end users) was described as often causing a lack of reporting of security incidents.

In addition to the above challenges of monitoring and enforcement, many security managers felt that the use of rewards to encourage and support end users may be a suitable alternative, or should be combined in a mixed method approach when managing security behaviour.

6 End User Experiences of Information Security Management in Organisations

6.1 Introduction

This chapter presents the findings from interviews with end users about their experiences of information security management in organisations. The chapter begins by presenting the findings relating to the willingness of end users to protect information and an analysis of the various factors which influenced this. The remainder of the chapter is broken down into the following sections, presenting the findings relating to: information security policies; security education, training, and awareness programmes; monitoring and enforcement practices; and, usability of technical security controls. For each of these sections there will be a description and analysis of how each (according to end users) influenced their willingness and/or capability to protect information.

6.2 The willingness of end users to protect information

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness to perform protective actions forms part basis of effective guardianship – the other being the capability to perform protective actions. Furthermore, the level of willingness of guardians to perform protective actions may be influenced by numerous factors.

In the context of information security management, this suggests that the willingness of end users towards protecting information may be influenced by different factors. Therefore, this next section presents the findings relating to the experiences of end users of working with sensitive information and discusses the main factors which were described as influencing their willingness to protect it.

During interviews, end users described having high levels of access to various types of information which had security requirements, including a customer’s full name, home address, national insurance number, medical records, banking and financial information, passport number, driving license, and employment history. For example, one end user commented,

> I have to do background checks, so passports, driving licenses, bank details for a credit check, proof of addresses for the last 5 years, utility bills and things like that … phone numbers, email addresses, pretty much everything about the person. (Jessica, Recruitment Consultant)

Similarly, another end user commented,

> I've got access to their health records … their name and address, occasionally their financial details if it's someone that is incapable of dealing with it themselves … all your personal and financial information. (Margret, Caregiver)

Importantly, end users described having a strong willingness towards protecting the information they handled during their everyday work routines. Furthermore, during interviews, end users described numerous factors which influenced their willingness.

During the analysis of interview data, the following three main themes emerged surrounding the willingness of end users to protect information: (1) having a responsibility to protect information, (2) the risks to various parties from failing to protect information, and (3) the perceived importance of protecting information within their organisation. Each theme will now be presented and discussed.

6.2.1 The responsibility to protect information

The first main theme was having a responsibility to protect information. In other words, if an end user felt they had a responsibility to protect information they described being more likely to have a willingness to protect information. End users further described how their sense of responsibility to protect information was influenced by three factors.

The first factor was having an *organisational responsibility* to protect information. This derived from the organisation end users worked for, where an end user's responsibility to protect information was part of their job role. For example, one end user commented,

> You are here to do a job, and … you've got a duty of care to make sure that the organisation's data is accurate, so it can be used by the organisation. (Leanne, Business Analyst)

Similarly, another end user commented,

> Without being all sanctimonious about why or whatever … It's just your responsibility to manage it properly and to make sure that you're using data the way that it's meant to be used. (Alistair, Elected Local Government Councillor)

The second factor was having a *legal responsibility* to protect information. This derived from the laws of society, where an end user's responsibility to protect information was part of obeying the law. For example, one end user commented,

> Because it's breaking the law as well … so it's your legal responsibility to make sure that the data is protected, and not available to the wrong people. (Joanne, Healthcare Professional)

Similarly, another end user commented,

> The legal side of it is very much the part that I would be considering. (Jennifer, Recruitment Consultant)

The third factor was having a *moral responsibility* to protect information. This derived from the personal moral beliefs of end users, where an end user's responsibility to protect information was part of being a good person. For example, one end user commented,

> I have where they were born, their date of birth, everything … I feel that morally, I have an obligation to make sure that that is safe. (Jennifer, Recruitment Consultant)

Similarly, another end user commented,

> I’ve had situations where a colleague will ask for information … I’ve chosen not to. Which can be awkward, but I understand that, ethically, it’s the right thing to do. (Colin, Recruitment Consultant)

We can understand from the above comments that end users described their willingness to protect information as being influenced by having a responsibility to protect information, which was in turn described as influenced by three factors; the organisation end users worked for, the laws of society, and personal moral beliefs.

In the context of guardianship of information, this suggests that the level of willingness of end users towards performing protective actions may be influenced by the perceived level of responsibility towards acting as a guardian. Such findings are in line with Felson (1995), who argued that the willingness of guardians to perform protective actions may be influenced by their sense of organisational responsibility to act as guardians. Importantly, however, the above findings also suggest that a guardian’s responsibility may also be influenced by having a legal and/or moral responsibility to act as a guardian, rather than solely being influenced by an organisational responsibility.

In addition, the above findings provide empirical support for the argument made by Sampson et al (2010) that guardians will consider the moral aspects of their behaviour, whereby if they consider performing protective actions to be morally good (or, vice versa, not performing protective actions is morally bad) then this will influence whether they act as guardians (Sampson et al, 2010).

6.2.2 The risks to various parties from failing to protect information

The second main theme was the risks to various parties from failing to protect information. In other words, if an end user felt that a given party was at risk, they described being more likely to have a willingness to protect information. During interviews, end users described the following three main groups of parties at risk.

The first category of parties at risk were end users. End users described their willingness to protect information as influenced by the risks to themselves from failing to protect information. Risks to end users included termination of employment and criminal prosecution. For example, one end user commented,

> Because I'm aware of the implications, it's made me wary of it. I know that, technically, you could go to jail or get a criminal record for doing certain things. (Colin, Recruitment Consultant)

Similarly, another end user commented,

> I think the overarching motivation is … if I make a mistake with data protection or data governance, it's on my head. And I don't want to get in trouble or be fined. (Alison, Product Owner)

The risks to end users for failing to protect information is perhaps one of the most researched aspects of end user security behaviour. Thus, the above findings strongly correlate with previous literature which have argued the threat of punishment is an important factor towards influencing security behaviour (Cheng et al, 2013; Darcy et al, 2008; Knapp and Ferante, 2012; Siponen et al, 2007; von Solms and von Solms, 2004b).

The second category of parties at risk were customers. End users described their willingness to protect information as influenced by the risks to customers from failing to protect his/her information. Risks to customers included mistreatment and/or embarrassment due to personal and sensitive information being disclosed or stolen, and any criminal activity further acted upon the customer by cybercriminals, such as identity theft or fraud. For example, one end user described how it is important to protect information because,

> People could steal people's identity … and use that for illegal reasons. (Joanne, Healthcare Professional)

Similarly, another end user commented,

> We have a lot of personal data for people that could be used to commit fraud. (Jennifer, Recruitment Consultant)

The third category of parties at risk were organisations. End users described their willingness to protect information as influenced by the risks to organisations from failing to protect information. Risks to organisations included reputational damage and/or financial repercussions. For example, one end user commented,

> Say I lost a whole load of data and it ended up in the public domain, and it shouldn't have done … the impact of that would be reputational. (Alistair, Elected Local Government Councillor)

Similarly, another end user commented,

> I know that if there are data breaches, there are massive fines … I think you can be fined up to £500,000 or something for data breaches. (Kenny, Assistant Director of Student Services)

We can understand from the above comments that end users described their willingness to protect information as being influenced by the risks to various parties from failing to protect information. The various parties at risk were end users, the customers to whom the information corresponded, and the organisations end users worked for.

In the context of guardianship of information, this suggests that the level of willingness of end users towards performing protective actions may be influenced by the perceived level of risk towards various parties from failing to act as a guardian. Again, this suggests that the level of willingness of guardians should not be understood as influenced primarily by any one set of factors.

Such findings are of particular interest as they suggest that too much emphasis on the risks to end users (i.e., punishment for failing to protect information) may overlook potential opportunities to enhance end user willingness by drawing their attention towards the potential negative consequences that will fall upon both organisations and customers should they fail to act as guardians for information. Further, previous studies have shown that the development and implementation of SETA programmes may be a useful way to achieve this increased awareness and understanding surrounding security risks (Alshaikh et al, 2018; Abawajy, 2014; Alzamil, 2012; Chan and Mubarek, 2012).

6.2.3 The perceived organisational importance of protecting information

The third main theme was the perceived importance of protecting information within the organisations that end users worked for. In other words, if protecting information was perceived to be important to an end user's organisation, they described being more willing to protect that information.

Importantly, the perceived organisational importance of protecting information should not be confused with having an organisational responsibility to protect information (as discussed above). For example, an end user may feel they formally have an organisational responsibility to protect information as part of their job role but may also feel that doing so is not considered as important to their organisation as other aspects of their job role. Therefore, these factors are treated separately.

End users described how their understanding towards the organisational importance of protecting information developed via the expectations and observed behaviour of other members of the organisation. Further, while in general the views of all organisational members were described as important, the expectations and behaviour of upper management were often described as the most important. Therefore, this section will exclusively focus on how the behaviour of upper management influenced end user willingness to protect information.

End users described how the expectations and behaviour of upper management had a powerful influence both on their own security behaviour and that of other end users. For example, one end user commented,

> I think there is probably a few key people in leadership roles and because they role-model that being taken seriously, it then kind of leaks down and you sort of think, 'If that's important to them then I

> should be taking that seriously as well' … I think that that has the highest impact. (Jill, Healthcare Professional)

Interestingly, end users described developing their understanding of the expectations of upper management via the different security controls that were implemented within their organisations, such as security policies and SETA programmes. For example, when discussing whether upper management considered protecting information important, one end user commented,

> I think they do … because of them saying it profusely, you know, it's drummed down through the policies and procedures that we have in-place. (Jennifer, Recruitment Consultant).

Alongside developing an understanding towards upper management's expectations was the observed behaviour of upper management in organisations, where upper management were regularly demonstrating good security behaviour in front of end users. As one end user commented,

> You can definitely see, you know, CEOs and directors definitely taking that seriously … they never leave details unattended or devices unlocked … you'll never see documentation like personal details on their desk. They all have privacy screens as well. (Fiona, Recruitment Consultant)

Importantly, while end users described the perceived expectations and observed behaviour of upper management as having a powerful influence upon their level of willingness, they described two caveats.

The first caveat was, the expectations of upper management towards protecting information were often described as reactive rather than proactive. In other words, some end users described the good security behaviour being demonstrated from upper management as resulting from their organisation having experienced a security incident; where prior to this, they described there being less consideration towards protecting information. For example, one end user described how the expectations of upper management towards protecting information was,

> Like any business, it would be brought to the forefront if there was a breach of any kind … for it to be heavily crucial, it would have to be triggered by something. (Kelly, Recruitment Consultant).

Similarly, another end user described how in her organisation upper management had expressed the importance of protecting information, however this would,

> Come on the back of some incident, because ... something happens and they're like, 'Oh gosh, we'd better tighten things up here'. (Samantha, Student Services)

Thus, while the expectations and observed behaviour of upper management may positively influence the level of willingness of end users to protect information, end users felt they weren't necessarily demonstrating this unless their organisation had experienced some form of security incident.

The second caveat was, there were certain situations where end users either felt encouraged to forgo protecting information to ensure they met their primary work targets, or they witnessed upper management themselves behaving insecurely to meet work targets, which then undermined those expectations towards end users behaving securely. For example, one end user commented,

> There were sometimes unacceptably short lead-in times for things to be done and you could adhere to processes and procedures and you would overshoot, or you would find ways of cutting corners to get there … And so long as it all goes okay, no one complained. (Donald, Business Analyst)

Similarly, another end user commented,

> It's not just your wee people doing it, its higher up people as well that's doing it … it just makes it seem to everybody else that it's alright to do it and then you just follow suit … if a manager is doing it then it's alright for us to do it, really. (Sally, Social Worker)

We can understand from the above comments that end users’ level of willingness to protect information was influenced by the perceived organisational importance of protecting information, which was heavily influenced by the expectations and observed behaviour of upper management. Further, some end users described the expectations and behaviour of upper management towards protecting information as reactive, and sometimes upper management demonstrated insecure behaviour, which negatively influenced end users’ willingness towards protecting information.

In the context of guardianship of information, this suggests that end users may be influenced by the expectations and observed behaviour of other guardians. Furthermore, the behaviour of super guardians can have an especially powerful influence upon their level of willingness to act as guardians and to perform protective actions, whether this is in a positive or negative manner.

The above findings empirically support the argument made by Sampson et al (2010), that because certain individuals may or may not perform certain behaviours due to social pressures, any reduction in the levels of temptation towards not performing protection actions may improve guardianship willingness. Further, Sampson et al argued because super guardians exert an especially powerful influence over normal guardians, they are in a unique position when it comes to influencing the willingness of guardians to perform protective actions.

6.3 The influence of information security policies

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness to perform protective actions forms part basis of effective guardianship – the other being the capability to perform protective actions. Furthermore, the level of willingness of guardians to perform protective actions may be influenced by the perceived level of organisational responsibility to perform protective actions.

In addition, based upon the Rational Choice Perspective, the willingness of guardians may also be influenced by various social factors and the risks to guardians for failing to perform protective actions.

In the context of information security management, this suggests that the willingness of end users to protect information may be improved via the development and implementation of security policies which make end users aware of their organisational responsibilities towards protecting information and the punishments for failing to protect information.

Furthermore, as already discussed in the previous section, during interviews end users described having a willingness to protect information which was influenced by numerous factors; notably, an organisational responsibility to protect information, the risks to end users from failing to protect information, and the perceived organisational importance of protecting information.

Therefore, this next section presents the findings relating to the experiences of end users of security policies and their effectiveness at influencing their level of willingness to protect information.

6.3.1 End user awareness of security policies

In terms of the levels of awareness towards the existence of security policies (excluding the levels of understanding of security policies), end users varied quite significantly in their experiences. For instance, there were a few end users who described having good levels of awareness of the security policies of their organisation and were able to describe numerous types of security policies, as the following examples demonstrate:

> We've obviously got the Data Protection Act, but then there are other things relating to your own Trust … how to send an email securely, or how to send a fax securely, if you're having to use the telephone, what sorts of information you are allowed to give … they

> always have one about passwords … some of the trusts I’ve worked in have had one about social media … it all comes under the umbrella of information governance. (Nadine, Doctor)

> We've got quite a few different policies, one is passwords, one's on acceptable use … web-filtering policy, we have the data-storage policy … And that says, look at the sensitivity of your data before you decide where you store it. (Leanne, Business Analyst)

However, for many end users they described their experiences towards security policies as either not knowing of any security policies existing in their organisation or they only knew of the Data Protection Act or GDPR-based documentation. As the following examples demonstrate:

> If someone said what’s the policy on this or that I would say I have no idea ... I think people are aware they’re dealing with semi-sensitive information … but if they said what’s the policy, I don’t know what the policy is. (Alistair, Elected Local Government Councillor)

> I don’t know my current company’s security policies. Apart from Data Protection, GDPR … I’m not aware if my company has any or even a specific company policy. (Fiona, Recruitment Consultant)

Importantly, despite many end users having little awareness towards the existence of security policies, this did not mean end users felt they had no responsibility towards protecting information and that there weren’t consequences for failing to protect information. Rather, end users described their sense of having a responsibility to protect information, and the risks to them from failing to protect information, as mainly deriving from reading the Data Protection Act (recall end users also described having a *legal responsibility* to protect information alongside having an organisational responsibility). For example, one end user commented,

> It hasn’t really come from work specifically, it’s mainly because of my general knowledge of the Data Protection Act and the legal requirements relating to that. (Sally, Social Worker)

Similarly, when asked whether her organisation had developed any security policies, one end user commented,

> I would probably say yes, but I think it would probably be relating to the Data Protection Act rather than a specific policy. But I don't know, I just think I would abide by that. (Kelly, Recruitment Consultant)

We can understand then, that for many end users interviewed for this research, they had little awareness of the existence of security policies in their organisation. Which suggests that many end users were not aware of their exact organisational responsibility towards protecting information. However, many were familiar with the Data Protection Act which appeared to give them some sense of legal responsibility towards protecting information in organisations. Such findings are significant as they again suggest insecure behaviours such as non-compliance with security policies are perhaps due to end users not being aware of their organisational responsibility towards protecting information, which highlights an organisational failing regarding the communication of security policies.

6.3.2 The ineffectiveness of security policies at influencing end user willingness

Because there were few end users amongst those interviewed who were aware of and had read the security policies of their organisation, and there were many end users who were familiar with the Data Protection Act (or documentation that was based upon the Data Protection Act), the remainder of this section will jointly discuss the experiences of end users who had read various security policies along with the experiences of end users who were familiar with the Data Protection Act.

During interviews with end users, there was some indication that security policies (including the Data Protection Act) were influential towards improving the level of willingness of end users to protect information. For example, one end user described reading the security policy surrounding the use of email where,

> In the policy it’s all about the things you are allowed to say in an email and things you are not; what’s appropriate to share and what’s not … It makes you realise how serious it is. (Linda, Paediatric Nurse)

However, for most end users, they did not describe security policies as effectively influencing their level of willingness towards protecting information. Following the analysis of interview data, three sub themes emerged to explain the lack of effectiveness of security policies, including (1) problems relating to the digestibility of security policies, (2) problems relating to the feasibility of security policies, and (3) problems with the communication of security policies. Each sub theme will now be presented and discussed.

6.3.3 Problems with the digestibility of security policies

The first sub theme that emerged when discussing the effectiveness of security policies with end users was the problem of digestibility. For many end users, the security policies they had to read were not easily digestible due to the writing style of security policies, such as the overuse of technical language – which meant they struggled to understand them. For example, one end user commented,

> There was a lot of legal terms and some things you don’t fully understand … you read it and you try and understand it, but it’s not always written down in plain English. (Norma, Council Worker)

Similarly, another end user commented,

> Quite frankly, I don’t understand it. A lot of it is jargon … if I want to understand it then I am going to have to go out of my way to understand it. (Fiona, Recruitment Consultant)

In addition to poor writing style, end users described how many of the security policies they had to read were often too long or there were too many. As a result, they became less likely to read and understand them. For example, one end user commented,

> They basically put like snippets of things like legislation and policies that you have to read through … there definitely was a lot of reading

> to go through … it basically meant that I didn't read them. (Alison, Product Owner)

Similarly, another end user commented,

> I'm not going to read through a 50-page document … because that is time-consuming … I think because the policies are so big … I would do the bare minimum to get me through. (Fiona, Recruitment Consultant)

We can understand from the above comments that for many end users interviewed for this research, the writing style of security policies impacted upon the level of effectiveness of the security policy. This highlights the importance of making sure security policies are written in simple terms without the overuse of technical language.

In addition, organisations should try to make sure security policies are kept short and are few in numbers. Otherwise they may not be as easily digestible to end users which may then reduce their level of effectiveness towards influencing their sense of responsibility to protect information, which in turn may reduce their level of willingness.

For example, security researchers and practitioners have argued because security policies will be directed at different audiences, security policies must be tailored to meet the needs of those different audiences, and the actions they must perform in relation to their job roles (Doherty et al, 2009; Goel et al, 2010). Further, the writing style of security policies should avoid the use of technical terms to make them easier to understand, and the length of security policies should be kept to a minimum (Hone and Eloff, 2002a; Wood, 1997).

Indeed, the dangers from organisations failing to produce digestible security policies was not lost on end users. As one end user commented,

> If they can't understand it … they could end up doing something they shouldn't have done and not realise that that can have a definite impact on the business. (Jessica, Recruitment Consultant)

6.3.4 Problems with the feasibility of security policies

Alongside problems with the digestibility of security policies was the difficulty for end users when trying to put security policies into practice, where some end users described security policies as not always feasible, which then caused problems during their everyday work routines. For example, one end user described how she regularly had to work with third-party organisations, however because her organisation had created a security policy which stated she is not allowed to email anyone out with the organisation, this meant that she could only communicate by telephone. While she acknowledged this rule was designed to keep information safe (and she understood that protecting information was an important part of her job role), she described how following this security policy made her primary job much more difficult. As she explained,

> We are not allowed to email anybody out with the organisation, so you can only really share information through phone calls, and sometimes that can be quite hard. Especially when you think you could just put all this in an email … It definitely makes it more difficult; it makes it more difficult for everyone. (Linda, Paediatric nurse)

There were several other cases described by end users, where following certain security policies meant their primary job role became much more difficult to perform. For instance, another end user had the same problem as above, where they were not allowed to email out with the organisation. However, instead of using the telephone to communicate, she had to use fax machines, which were described as being even more problematic. She commented,

> Now, depending on how particular they are about security they might want you to send them a fax with a request … and then they

> will send you a fax back. So, that is very slow … You have to find a fax, find the fax number, make sure it's working, make sure there's paper in it, fax them, wait for them to have the time to print it off and then to fax it; and it just makes everything prolonged, and it's so frustrating – rather than just email. (Nadine, Doctor)

We can understand from the above comments that for some end users the security policies which they had to follow were often not feasible in practice. Consequently, they described being regularly frustrated, as complying with security policies meant they became less effective at performing their primary job roles. Therefore, while security policies may be useful for making end users understand they have an organisational responsibility to protect information and that certain behaviours are considered unacceptable, in certain situations this may prove very difficult for some end users to adhere to, due to the nature of their job role.

In the context of guardianship of information, this also suggests that because end users have different sets of organisational responsibilities, they might come to find themselves in situations where security responsibilities conflict with other job responsibilities (which may be considered of a higher priority), whereof they may feel pressured towards circumventing unfeasible security policies to make sure they fulfil those other job responsibilities (recall the above discussion surrounding the pressure from upper management).

These findings mirror those of previous studies which have shown a major problem in information security management is when certain security controls, such as security policies, are impractical for end users, which sometimes end users feel they need to circumvent to improve their job performance (Beautement et al, 2008; Kirlappos et al, 2013; Renaud, 2012).

This highlights the importance of organisations understanding the everyday work routines of end users when developing security policies and making sure they are feasible in relation to their primary job roles. Again, this aspect of security policy development was not lost on end users. As one end user commented,

> I think it's the whole idea of policy-makers … understanding what it is that people need to do, and how they need to work. (Leanne, Business Analyst)

6.3.5 Problems surrounding the communication of security policies

When it came to the communication of security policies, most of the interviewed end users described how their organisation would upload various security policies to an intranet and then they were able to access and read them. However, beyond simple notification of the existence of security policies, end users described no real effort from their organisation towards incentivising them to read through security policies. As a result, many end users described the communications approach of organisations to be largely ineffective because it heavily relied upon end users taking the initiative to read security policies rather than having their organisation incentivise them. For example, one end user commented,

> It's almost like a pull thing … It's not pushed out to you. You get the whole, welcome to our organisation … this is all the information you need to know as a new member of staff, for example. And one little snippet will be, 'Oh, by the way, the intranet has all these policies you need to read' … But there's no sort of, here's your induction, and have you read this policy? Have you read that policy? (Leanne, Business Analyst)

Similarly, another end user commented,

> If I went looking for policies on the intranet, for example, I think there will be information there, but there's no push to make me do that. (Joanne, Healthcare Professional).

The problem of not being incentivised to read security policies was further exacerbated by the fact that reading security policies was sometimes not considered part of end users' primary job role, which meant they often didn't consider reading security policies as something they had to regularly do. As one end user commented,

> Everyone is just so busy these days and there’s so much to fit into your day and … If it’s not your main job … then it doesn’t necessarily occur to you to think about it all the time. (Samantha, Student Services)

We can understand from the above comments that despite some end users being aware of the existence of security policies, they didn’t feel that their organisation was properly incentivising them to read them. Further, because reading security policies was not a major part of their job role, they often did not consider reading security policies to be of major importance (especially if organisations were not encouraging them to read security policies).

This highlights the importance of organisations making sure to encourage end users to read security policies, as for many this may not seem part of their main job role and so they might not understand the need to access and read through security policies. Further, organisations must ensure to allocate enough time for end users to familiarise themselves with security policies.

In the context of guardianship of information, this suggests that although the willingness of end users towards performing protective actions may be positively influenced by security policies, this will only occur if organisations make efforts to effectively communicate security policies and encourage end users to read through them. Otherwise, there may be minimal influence upon their level of willingness towards protecting information, which in turn, may reduce the overall level of protection of information in organisations.

6.4 The influence of security education, training, and awareness programmes

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness and capability to perform protective actions forms the basis of effective guardianship. Furthermore, the level of willingness and capability of guardians to perform protective actions may be influenced by the levels of knowledge and experience of guardians surrounding various threats and the protective actions they must perform.

In the context of information security management, this suggests that the willingness and capability of end users to protect information may be improved via the development and implementation of SETA programmes which (1) improve the levels of awareness and understanding of information security concepts and issues through security awareness and security education, which influences their level of willingness to protect information, and (2) improve the levels of skill and ability of end users towards performing security actions through security training, which influences their level of capability to protect information.

In addition, as discussed above, end users described their willingness to protect information as influenced by the various risks to organisations and customers for failing to protect information.

Therefore, this next section presents the findings relating to the experiences of end users of SETA programmes in organisations.

6.4.1 The ineffectiveness of SETA programmes

During interviews with end users, they often described how SETA programmes were an important security control in organisations because they made sure end users were willing and capable towards protecting information. For example, one end user commented,

> If you don’t train people, they’re not going to know, and if they don’t know, they’re going to make mistakes. (Colin, Recruitment Consultant).

Similarly, another end user commented,

> You don’t know how to protect yourself against what you don’t know, and … then you’ve got a major part of your workforce that are

> a security threat to you because they don’t know what to look out for. (Toby, Technical Support Analyst)

However, despite their acknowledgement towards the importance of SETA programmes, most end users described SETA programmes as overall ineffective towards influencing their security behaviour. During data analysis, the following two sub themes emerged surrounding the ineffectiveness of SETA programmes: (1) problems with the quantity of SETA programmes, and (2) problems with the quality of SETA programmes. Both sub themes will now be presented and discussed.

6.4.2 The quantity problem of SETA programmes.

The first major problem end users described towards SETA programmes was the number of SETA programmes provided in organisations. Many end users described having no experience or very little experience of SETA programmes. As the following comments demonstrate:

> I had three weeks IT training in total, covering each of the systems I now use daily … but I wouldn't say I have had any specific information security training. (Carol, Public Office Clerk)

> I've been here for three years and I've never had information security or information governance training at all. (Leanne, Business Analyst)

> Not in this company … I don’t think there is any formalised training … I’ve never been asked to do it. (Jessica, Recruitment Consultant)

These findings are significant because previous studies have deplored the low levels of security awareness of end users and their efforts to protect information (e.g., Albrechtsen, 2007; Chan and Mubarek, 2012). Thus, the above findings suggest that a potential cause of such poor security behaviour may be due to a lack of SETA programmes being delivered to end users.

Interestingly, end users who had little or no experience of SETA programmes described using two coping mechanisms. The first coping mechanism was to rely on the knowledge and experienced gained from previous employment, where a previous employer had provided SETA programmes. For example, one end user commented,

> My previous company did. They did proper training like where they take you through everything and help you spot a potential phishing email and what it would look like. But yeah, not in my current company … If I hadn't had that training, then I would be clueless. (Fiona, Recruitment Consultant)

The second coping mechanism described by end users was simply to rely on the cumulative and practical experience gained from current and previous employment, where although there might not have been SETA programmes provided to end users, they had nevertheless developed knowledge and experience towards protecting information tacitly, through general trial and error and so on. For example, one end user commented,

> Although I've not received much training I've developed a sort of general understanding towards data protection over the years towards things like that which sort of makes up for the lack of training. (Sally, Social Worker)

Similarly, another end user commented,

> A lot of that comes with experience, it comes with things that have gone wrong in the past. (Kenny, Assistant Director of Student Services)

We can understand from the above comments that a major problem described by end users was the quantity of SETA programmes provided in organisations, which meant the security behaviour of many end users was not being positively influenced by SETA programmes.

In the context of guardianship of information, this suggests that a major problem surrounding the protecting of information in organisations may be the levels of SETA programmes being delivered to end users, which may then have a negative impact upon their willingness and capability to act as guardians and keep information safe.

6.4.3 The quality problem of SETA programmes

The second major problem for end users was the quality of SETA programmes in organisations; as although some end users had received SETA programmes, they were not described as particularly effective towards changing their security behaviour. To better understand why some end users described SETA programmes as ineffective it is useful to discuss the two main delivery methods of SETA programmes; computer-based training and face-to-face training.

6.4.3.1 Computer-based training

End users described computer-based training as the most popular delivery method. Computer-based training typically involved end users accessing an online e-learning module or course via their organisation's intranet. They would be presented with various bits of information (sometimes scenario-based) followed by a test. End users would be required to score a certain mark otherwise they would have to repeat the whole process again. For example, one end user commented,

> It's like an online learning thing that you had to do … They gave you tick-box options and that kind of thing. And they assess you at the end to see what information you've retained. (Fiona, Recruitment Consultant)

Similarly, another end user commented,

> It will put scenarios in front of you… And then, you would answer yes or no … if you get the questions wrong, they give you the information that's required in order for you to do it correctly. Then you're re-tested and it's not completed until you get every question right. (Colin, Recruitment Consultant)

According to end users, the training material of computer-based training was primarily focused around the Data Protection Act and the sorts of general behaviours or actions end users must perform to be compliant. For example, one end user commented,

> In terms of Data Protection, it basically says don’t access anything you don’t need to access and don’t share it with anybody. That’s kind of it in a nutshell. And if anybody asks for anything then refer them to the legal department. That’s pretty much it. (Natalie, Doctor)

Overall, end users described computer-based training as ineffective in terms of influencing their willingness towards protecting information and they described several reasons for this.

The first reason described by end users was, many end users felt that computer-based training was simply not engaging. Thus, they had little interest in completing the training modules. For example, one end user commented,

> I wouldn’t say it was particularly interesting … a dry screen of text to read along with the Data Protection Act, and blah, blah, blah, which is often, well, what my experience of previous training has been like – you don’t engage in that. (Joanne, Healthcare Professional)

Indeed, the levels of engagement were so low for some end users that they described skipping ahead to complete computer-based training as quickly as possible. As the following comments demonstrate:

> I don’t find the online modules particularly useful or effective. I don’t think you retain the information … my way of engaging with them, which I think is the same as everybody else, is to just skip ahead and have a go at the questions. I don’t think there is any retention from that kind of learning. (Jill, Healthcare Professional)

> Those modules are boring, as you can imagine … And I must admit, there were a couple of them where I just skipped all the content, went straight into the multiple-choice and ... used my current knowledge and guessed a few, just to get it over and done with, really … because it is so boring. (Scott, Healthcare Professional)

The second reason described by end users was, many end users felt that because most of the training material of computer-based training was solely focused on the Data Protection Act, it was not always relevant to their job role. For example, when asked if she felt the computer-based training was useful or effective towards improving her security behaviour, one end user responded,

> No because it wasn't specific to my job role. It was just a general overview of the Data Protection Act … because it doesn't reflect your job role you can't link it to your job role, to be quite honest … there might be some things on it that it says you shouldn't do but actually we do them in our job role because we have to. (Sally, Social Worker)

The lack of tailoring of training material became even more problematic for end users when they had to repeat the same computer-based training every year. As a result, they felt like they were wasting their time and were not learning anything new. As one end user commented,

> I was with that organisation for 4 years and every year it was the exact same training. We weren't learning anything new at all … when it comes to your third year doing it, it's like just click through it because I know all the answers because you've done the exact same training before. (Fiona, Recruitment Consultant)

Lastly, the above factors were exacerbated by the fact that end users were provided very little time to complete computer-based training, which again meant many would skip ahead to complete it quickly. Which end users described as being potentially dangerous for organisations given the importance of SETA programmes towards making sure end users are willing and capable towards protecting information. For example, one end user commented,

> One of the issues I've always had in my organisation is you're always expected to do it in your own time … so, your obviously just scrolling through trying to do it as quickly as possible, and you're not really engaging with it … you can imagine in lots of areas that training is required; so, it's a huge problem. (Natalie, Doctor)

We can understand from the above comments that many end users described computer-based training to be overall ineffective towards influencing their security behaviour. The major concerns were the training material was based upon the Data Protection Act, which meant some end users found it less interesting and engaging, while others felt it was not relevant to their job roles. Further, end users described having to repeat the same computer-based training every year and were not provided sufficient time to complete computer-based training. All in all, this meant most end users would rush through or skip entire segments of computer-based training. Consequently, computer-based training was described as having very little influence upon their willingness and/or capability towards protecting information.

In terms of the guardianship of information, this suggests that computer-based training may have numerous limitations as a means to improve the levels of willingness and capability of end users towards protecting information in organisations.

Such findings are again consistent with previous studies which argue organisations favour computer-based training in order to demonstrate they have fulfilled various compliance requirements (Alkasihk et al, 2018). However, the downside of such an approach is computer-based training may prove ineffectiveness towards improving security behaviour as it is often considered monotonous by end users, which may then lead to end users attempting to complete computer-based training sessions with minimal time and effort (Abawayjy, 2014).

6.4.3.2 Face-to-face training programmes

Although end users generally described computer-based training as a worse delivery method, this didn’t mean that face-to-face training programmes were described any better. Indeed, for the few end users who had received face-to-face training, this was also described very negatively.

Firstly, the training material for face-to-face training was described as the same training material used in computer-based training, where the training material mainly comprised lists of responsibilities or basic actions that end users must perform to be compliant with the Data Protection Act. For example, one end user commented,

> We went through things like, when you have information in hard copy, you shouldn't leave it out on your desk, and to lock things like your cabinets when you leave the office … also, sharing information with your colleagues, making sure that you only share information that is relevant. (Laura, Recruitment Consultant)

Again, because the content was largely focused on being compliant with the Data Protection Act, most end users described face-to-face training as an ineffective way to learn about information security, as the focus of attention was more towards being compliant with the Data Protection Act rather than developing knowledge and experience towards general concepts and issues relating to information security.

Importantly, the major complaints towards face-to-face training were not solely focused upon the training material, as many complaints from end users centred around the actual delivering of face-to-face training sessions.

For instance, the face-to-face training sessions were generally described as lacking interaction, where end users described simply being told what they 'must and mustn't do' rather than having an engaging discussion about what the various threats are in information security and why protecting information is important for organisations. For example, one end user described face-to-face training sessions as ineffective because,

> You're just in the lecture theatre with someone talking at you for twenty minutes about information governance … there not discussion-based sessions; it's just making sure that you know what information governance is and just ticking the box. It's like having a lecture for twenty minutes about information governance. (Nadine, Doctor)

Similarly, another end user commented,

> It was like a lecture where someone would have a PowerPoint presentation and talk to you about it. I would say that's less effective … I think you were less engaged in it; people were either just sitting there daydreaming or looking at their phone. And there wasn't a test at the end of it … probably because they knew everyone would have failed. (Natalie, Doctor)

In addition, the face-to-face training sessions were described by some end users as lacking any tailoring to the different job roles and learning levels of end users, which meant for some it was either irrelevant or it was too basic. Thus, they would not properly engage with the face-to-face training session. As one end user commented,

> Because people have so many different levels of competency or knowledge or experience, whatever, the one-stop-shop doesn't work … And, that's not managed well enough, I don't think. (Toby, Technical Support Analyst)

Previous studies have similarly criticised the approaches taken by many organisations when developing and implementing SETA programmes. For example, Valentine (2006) argued end users in most organisations experience highly generic training sessions regardless of the differences in job role or knowledge and experience. Stewart and Lacey (2012) similarly characterised most organisations as having a 'technocratic approach' when delivering SETA programmes to end users, claiming organisations have shown little sign of innovation in the last few decades.

Interestingly, there was one end user who described her experiences of face-to-face training very positively. However, the reasons she gave for her positive experiences provided further insight into why other end users were perhaps having worse experiences. For example, she described the face-to-face training sessions of her organisation as very effective because,

> It gives you the understanding towards why you need to take it seriously … and it was focused a little bit more on your job because you had it in groups with the people that you worked with … Because

> it was face-to-face you were able to ask questions and even just listening to the questions other people were asking was useful … I feel that now I have enough knowledge to make an informed decision … because I understand why it needs to be taken seriously. I'm more likely to ask the IT or security people to help me … because I don't want those bad things to happen." (Alison, Product Owner)

The comment above exemplifies the importance and potential influence that face-to-face training sessions can have for end users when tailored to end user job roles, where end users are provided the What and the Why as well as the How aspect of protecting information, and the importance of having a two-way conversation with end users to enable them to ask questions and to engage with other end users in group discussion; as this may help to improve their levels of engagement, which in turn may improve the overall effectiveness of face-to-face training sessions.

6.4.4 End user recommendations to improve SETA programmes

Following discussions about the problems of quantity and quality of SETA programmes, end users were asked to give their recommendations to organisations for improving the effectiveness of SETA programmes. End users provided the following main recommendations.

First, end users felt that organisations must provide face-to-face training sessions if they weren't already being provided or to provide more face-to-face training sessions if the numbers were low. As one end user commented,

> I would never recommend that someone purely learn something by doing an online module and answering some questions; that's not how we learn, that's not how we change behaviour … if organisations value this and are seriously wanting to invest in this then it should be face-to-face training. (Jill, Healthcare Professional)

Second, end users recommended that organisations ensure face-to-face training sessions are tailored to better suit the job roles of end users. As one end user commented,

> Using case-studies which are specific to those groups of individuals … so you can understand what the impact is more, what the threat might be … and then you think, ‘Oh actually I do have the control to protect my organisation from these external threats’ … but if I’m just sitting in front of a computer and clicking things, I don’t engage with that really. (Jill, Healthcare Professional)

Lastly, end users felt there needs to be much more emphasis on what the threats and vulnerabilities are and what the impacts are to organisations and why they need to behave securely, rather than simply being told that they must perform certain security behaviours. As one end user commented,

> I always think with these things that you can give all the training that you want, but if your employees are not invested in what they’re actually saying and the reasons behind it, they’re never going to achieve anything. So, I think if there was more emphasis on the reasons why it was important to protect data. (Leanne, Business Analyst)

Similarly, another end user commented,

> They need to know why we do it this way… It’s not the “do it or else”, it’s the “do it because if you don’t, this happens, or this could happen”. The employees need to know what the impact would be on, not just their job, but the whole firm. (Alistair, Elected Local Government Councillor)

6.5 The influence of monitoring and enforcement on end user willingness

As discussed in chapter three, the theoretical framework developed in this study is based upon the Routine Activity Approach, which states the willingness to perform protective actions forms part basis of effective guardianship – the other being the capability to perform protective actions.

In addition, the Rational Choice Perspective suggests that the willingness of guardians to perform protective actions can be improved by managing both the risks for failing to perform protective actions and the rewards for successfully performing protective actions. The Rational Choice Perspective also states that decisions to act may be influenced by moral factors.

In the context of information security management, this suggests that the willingness of end users to protect information may be improved via monitoring and enforcement practices which (1) monitor the security behaviour of end users, and (2) punishes (including formal and informal sanctions) and/or rewards end users for either positive or negative security behaviour.

Therefore, this next section presents the findings relating to the experiences of end users of monitoring and enforcement practices in organisations.

6.5.1 The lack of monitoring and enforcement (both punishment-based and reward-based)

As mentioned in the beginning of this chapter, end users described how their willingness towards protecting information was influenced by the risks to end users for failing to protect information (alongside the risks to customers and organisations). Thus, during interviews, some end users described how monitoring and enforcement of security behaviour can be a useful way of making sure information is protected in organisations. For example, one end user commented,

> We are monitored in terms of what we do on our login … so, I know they will see what I'm accessing and what I'm doing … I do think it influences you. (Nadine, Doctor)

Similarly, another end user commented,

> I think it makes you more aware … you need to watch and evidence why you are looking at certain things. Because anybody at any time can ask why you are looking at that data. (Norma, Council Worker)

However, for most end users, they described having very little awareness towards the monitoring and enforcement practices of their organisations. For example, when discussing whether monitoring and enforcement of security behaviour has an influence on end user willingness, one end user commented,

> I think the punishment one is an interesting one because whilst it's one of the motivations, there has not been any threats made or even any discussion around it. (Alison, Product Owner)

Similarly, another end user commented,

> I have no idea. I've not had any experience of it being enforced. (Alistair, Elected Local Government Councillor).

Further, some end users simply assumed there would be some form of monitoring and enforcement taking place due to their having read the Data Protection Act, where they assumed there would be monitoring in relation to this. As one end user commented,

> For me, it's just a general knowledge that there would be disciplinary action for that … and having a general understanding of the Data Protection Act … It's never been explicitly said to us by the company. (Sally, Social Worker)

Importantly, however, even though many end users described there being a lack monitoring and enforcement within their organisations, they were still willing to protect information. For example, when discussing whether a lack of monitoring and enforcement meant end users could potentially do as they pleased, one end user commented,

> It doesn't matter if I'm being monitored or not … If I accidentally exposed someone's details I would feel really guilty when I've done that because it's not my information … these people are trusting me to look after their information. (Jessica, Recruitment Consultant)

Similarly, another end user responded,

> It’s like saying if you could commit a crime and not be caught or punished for it would you be more likely to commit the crime? For some maybe that would be the case but … I have respect for the people that I am working on behalf of. Therefore, I treat their data with respect. (Jill, Healthcare Professional)

We can understand from the above comments that while the monitoring and enforcement of security behaviour in organisations influenced the level of willingness of some end users to protect information, many end users were unaware of such monitoring and enforcement practices taking place within their organisation. Further, a lack of punishment did not necessarily lead to a decrease in the levels of willingness amongst end users towards protecting information because they described still being influenced by having a moral responsibility to protect information.

In the context of guardianship of information, this suggests that monitoring and enforcement practices may be an effective way to improve the levels of willingness towards protecting information by managing the risks to end users for failing to protect information. Furthermore, this suggests that the willingness of end users towards protecting information may be influenced by a wide range of motivational factors including the moral responsibility toward protecting information. Such findings are of significance as they again suggest organisations who focus too much on punishing end users for failing to protect information may be overlooking potential opportunities to enhance end user willingness by drawing their attention towards the potential negative consequences that will fall upon both organisations and customers should they fail to act as guardians for information, which may be achieved through the development and implementation of SETA programmes.

Lastly, in addition to there being a lack of monitoring and enforcement of security behaviour in organisations, there was also little evidence to suggest that organisations were using any kind of rewards to influence end user willingness. Indeed, the idea of organisations rewarding end users for protecting information was generally met with smiles and laughter from those end users being interviewed. As the following comments demonstrate:

> That doesn't exist in our company … We get rewarded by getting to keep our jobs [laughs]. (Fiona, Recruitment Consultant)

> Absolutely not. That doesn't even come into it. It's just assumed that you will follow the rules and if not, you will be punished for not doing so. (Sally, Social Worker)

> There are none [laughs] there is no incentives I would say … there doesn't need to be some big reward, just something a bit friendlier or more motivating than losing your job. (Nadine, Doctor)

We can understand from the above comments that the organisations end users worked for were described as favouring a punishment-based approach towards managing the levels of willingness of end users (albeit not all were even taking this approach). Consequently, end users did not describe rewards for protecting information as part of the reasons why they were willing to protect information. Again, these findings suggest that various opportunities to positively influence the security behaviour of end users are being missed by many organisations.

6.6 The influence of usable technical security controls on end user capability

As discussed in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states the willingness and capability to perform protective actions forms the basis of effective guardianship.

In addition, based upon the Rational Choice Perspective, the level of capability and willingness of guardians to perform protective actions may be influenced by the effort and time required to perform protective actions.

In the context of information security management, this suggests that the capability and willingness of end users to protect information may be influenced by the usability of technical security controls.

Therefore, this next section presents the findings relating to the experiences of end users of using technical security controls to protect information as part of their everyday work routine.

During interviews with end users, only one technical security control was described as causing them significant problems; user logins and passwords. Therefore, this section largely focuses on those findings relating to end users' experiences of creating and managing secure passwords.

6.6.1 The password problem

End users described having access via username and passwords to various information systems containing the information they used as part of their everyday work routine. They also described having restrictions on the types and amount of information they had access to as part of making sure information was properly protected. As illustrated by the following comment:

> We would use all sorts of different systems to get information about our patients, or to input information about them … We've all got our own logins for the computers, so that if you log into a computer you're only accessing the things that you've got clearance to access. (Joanne, Healthcare Professional)

As part of having access to sensitive information, end users described having to adhere to various password-related rules, including:

- to create 'strong' passwords, which meant they had to have a minimum of six to eight characters, including a number, upper and lower-case letters, and a special character;
- to regularly change their passwords;
- to not write their passwords down, and

- to not share their passwords

This was illustrated by the following comments:

> They have to conform to capital letters, numbers, and special characters; we are not allowed to share them with anyone … we are not allowed to write them down, like have them on sticky notes or anything like that. (Jessica, Recruitment Consultant)

> They have mandatory standards that we need to reach. They need to have a capital letter, a special character, a number … And it has to be changed every 32 days … there is a minimum, I think it's 6. (Norma, Council Worker)

Although end users described understanding that the above password rules were designed to protect information, they described adhering to them as very difficult, where they often performed insecure behaviours such as creating weak passwords, reusing weak passwords on multiple systems, writing passwords down, and sharing passwords.

The main reasons described by end users for behaving insecurely in relation to passwords, were end users had to use various information systems and applications as part of their everyday work routines. Thus, if end users were to follow the above stated password rules, this would mean they would have to remember numerous strong passwords – which they described as very difficult to do – as well as remembering which passwords matched which systems. As a result, many end users described having to create weak passwords and/or reuse weak passwords on multiple systems to help them manage this. For example, one end user commented,

> There are multiple systems, websites, and things that I logon for work and if I didn't have a similar password for them all, I would forget … because there's a lot to remember. (Jill, Healthcare Professional)

Similarly, another end user commented,

> I always try and jumble them up as much as I can … but at the same time I need it to be a word that I'm going to remember … Because I'm trying to remember so many different passwords for different things. (Jessica, Recruitment Consultant)

The above problem was further exacerbated by the fact that end users also had non-work-related passwords, which added to the total number of passwords they had to remember, and they described this as sometimes interfering with their ability to remember work-related passwords. For example, one end user described remembering passwords at work as difficult,

> Because you've got so many, because you've got a plethora and that's just on your work-side; wait until you add in all the other ones. (Alistair, Elected Local Government Councillor)

Similarly, another end user commented,

> There's too many to remember sometimes, and you do forget, and you mix up your work ones with your ones from outside your work … definitely too many passwords. (Norma, Council Worker)

In addition to struggling with remembering numerous passwords, end users described having to regularly change their passwords which made it even more difficult to remember them, which again influenced whether they would create weak passwords and/or reuse them. For instance, if end users had to frequently change their passwords they described this as causing them to forget which password they were currently using (i.e., whether a specific password was an older or newer version). As one end user commented,

> I have to change my password every 4 weeks and I'm always forgetting it … the fact that I have to change it all the time makes it hard to remember. (Alison, Product Owner)

Furthermore, if the time between password changes was considerably short, then end users described being less likely to create strong passwords because it would soon need to be changed again. For example, one end user commented,

> Because you are having to change those passwords constantly … I will just change one of the numbers … all I would have to remember then is what number I am on, rather than what the password is … I know that quite a lot of people do that as well. (Jill, Healthcare Professional)

Interestingly, a difficult situation that some end users found themselves in was when they would reuse a password on multiple systems. However, because those systems would require password changes at different times, this would somewhat negate the benefit of reusing passwords. Indeed, this potentially caused more problems as end users would end up with numerous passwords which were very similar in content, which then made it even harder to remember which password corresponded to which system. For example, one end user commented,

> I find … you end up with different passwords for different systems, and then they need to change at different points. (Joanne, Healthcare Professional).

Similarly, another end user commented,

> There is quite a few, and they do all change out of sync, which is not ideal. (Jill, Healthcare Professional).

Ultimately, end users described how the required level of effort to create and remember strong passwords ironically made the effectiveness of technical security controls such as access control, to be greatly diminished. As one end user commented,

> The password stuff's gone too far, and it's become so strict that it's probably not secure anymore … the more things you're meant to memorise, the less secure it is. (Jill, Healthcare Professional)

We can understand from the above comments that for many end users, creating and remembering secure passwords was very difficult because they had to remember numerous passwords, had multiple systems and applications requiring passwords, and were required to regularly change their passwords, which ultimately lead many end users to create weak passwords and/or to reuse weak passwords on multiple systems.

In the context of guardianship of information, this suggests that if certain technical security controls require too much effort to use, this may reduce the level of capability of end users towards using them, which may then influence their level of willingness towards protecting information, where end users may try to compensate by behaving insecurely. Such findings are important because while passwords have been a major focus in usability research for some time (Adams and Sasse, 1999; Payne and Edwards, 2008), the above findings suggest that the so-called 'password problem' may continue to be a major issue for many end users in organisations.

6.6.1.1 Problems relating to processes and procedures surrounding passwords

In addition to the problems relating to the effort required to remember secure passwords, were problems relating to the slow processes and procedures surrounding access control, such as making requests for user logins or to change passwords. A major problem for some end users was when making requests for initial and/or additional levels of access to certain databases. As already discussed, end users are only allowed to access information that was relevant to their job role. While this was not described as an inherent problem for end users and they understood that access to certain types of information must be restricted, they described situations where certain processes were too slow, which created a situation where they had to decide between complying with password rules (e.g., not sharing their passwords) and potentially failing to complete a primary work task, or not complying with password rules (e.g., share their username and passwords) and completing a primary work task. And in most cases, they would opt for the latter.

For example, one end user described giving her username and password to her students to enable them access to certain systems which were necessary for their training. However, because she had higher levels of access, this meant that students could now use her user login and password to access various databases. She described her doing this as caused by the extended time length to have students provided with access to the systems, which meant they would have spent less time completing their training. Thus, she felt that providing them her user login and password to complete their training was more of a priority than adhering to password rules. Thus, she commented,

> One thing that I do that I know I shouldn't do is … I will sometimes just write my computer login and password down on a bit of paper, and give that to them … obviously, if they didn't have the best intentions, there is a risk they could open up a whole range of databases and access a lot of personal information about people … I know I shouldn't do that, and the reason I'd do that is probably for time saving ... By the time that paperwork was filled out and that was processed, they'd probably be ready to go. (Joanne, Healthcare Professional)

Another end user described a similar situation with gaining access to certain systems, where certain end users had begun working for their organisation but were not provided with access to various systems which were required for their job role. As a result, end users would share their passwords to enable them to perform their job roles. She commented,

> I see an issue quite a lot with people requiring access to things, and because of the security that's around it, the access can take a lot longer to grant, which … means the doctor's been in a job for three days without being able to do any clinical work … and I've no doubt that our junior doctors … are logging in using their consultant's or their supervisor's information … because they just want to get their job done, and that seems the best way to do it. (Jill, Healthcare Professional)

Again, we see here the main concern for the above end user was with completing primary work tasks, where the time surrounding various security processes and procedures were described as too slow, which meant some end users would share their usernames and passwords.

Another example described by end users was when they were resetting passwords and how this required too much time and effort. Therefore, they described being more likely to create a weak password to ensure they wouldn't forget it and to avoid going through the long process of resetting it. For example, when discussing resetting passwords, one end user commented,

> The reason it's a problem is because you then have to phone IT and it can take ages to get through to them, and so you are losing whole chunks of your day spent on the phone just trying to get your password back … and I can't do a lot of work without access to the system. So, yeah, I don't want to forget my password because I don't want to spend hours on hold to IT trying to get my password sorted out. (Jill, Healthcare Professional)

We can understand then from the above comments that overall, despite end users being willing to protect information, if they find themselves in a situation whereby they are not capable of performing certain protective actions because of the required levels of effort and time, then they become less willing to protect information, where they choose instead to behave insecurely to enable them to complete their primary work tasks.

In the context of guardianship of information, this suggest that if certain technical security controls and/or process and procedures surrounding their use take too long in relation to end users primary job roles, this may then influence their level of willingness towards performing protective actions, where they try to compensate by behaving insecurely.

6.7 Summary of chapter findings

This chapter has presented the findings relating to interviews with end users about their experiences of information security management in organisations. Overall, the findings from interviews with end users showed that end users described having a strong willingness to protect information. Further, their willingness to protect information was influenced by three main factors. The first was having a responsibility to protect information, which was in turn influenced by the organisations end users worked for, the laws of society, and end users' personal moral beliefs. The second was the risks to various parties from failing to protect information, which included end users, customers, and organisations. The third was the perceived organisational importance of protecting information, which was heavily influenced by the expressed views and observed behaviour of upper management. However, the views and observed behaviour of upper management were often described as reactive rather than proactive, and sometimes were counter to the protection of information depending on performance levels of organisations and end users.

Regarding security policies, the findings showed that many end users were unaware of the existence of the security policies of organisations. In addition, there were numerous problems relating to development and implementation of security policies. First, the digestibility of security policies was described as poor, mainly due to the overuse of technical language and the length and number of security policies. Second, some end users described problems with the feasibility of security policies, where they felt adhering to security policies caused them to be less effective at performing their primary job roles. And third, end users described the communications approach of organisations as ineffective, where organisations had failed to properly make end users aware of the existence of security policies as well as incentivising them to read security policies.

Regarding SETA programmes, the findings showed that many end users described SETA programmes as overall ineffective towards influencing their security behaviour. There were two main problems connected to SETA programmes. The first major problem was many end users described having no experience or very little experience of SETA programmes. As a result, end users described relying on two coping mechanisms. The first coping mechanism was to rely on the knowledge and experienced gained from SETA programmes provided from previous employment, and the second coping mechanism was to rely on the cumulative and practical experience gained from current and previous employment.

The second major problem was, SETA programmes were described as poorly developed and implemented. End users described the training material of both computer-based training and face-to-face training as primarily focused on the Data Protection Act and the sorts of general behaviours or actions end users must perform to be compliant. As a result, the training material was not always relevant to job roles and training sessions often contained the same training material. In addition, face-to-face training sessions were described as poorly delivered where there was little interaction and group discussion. Overall, SETA programmes were described as lacking engagement which reduced the overall effectiveness of SETA programmes towards influencing the level of willingness and/or capability of end users towards protecting information.

Regarding monitoring and enforcement practices, the findings showed that end users generally described monitoring and enforcement of security behaviour as a useful way of making sure information is protected in organisations. However, most end users described having very little awareness towards the actual monitoring and enforcement practices of their organisations. In addition, even though many end users described there being a lack monitoring and enforcement within their organisations, they were still willing to protect information due to factors relating to their legal and moral responsibility to protect information. Lastly, end users did not describe their organisations as using any kind of rewards systems to influence their willingness to protect information.

Finally, regarding usability of technical security controls, the findings showed that although end users described being familiar with and understanding various rules surrounding the use of passwords, they described adhering to those rules as very difficult, where they often performed insecure behaviours such as creating weak passwords, reusing weak passwords on multiple systems, writing passwords down, and sharing passwords. The main reasons given for this were (1) end users had to use various systems and applications as part of their everyday work routine, which meant they have numerous passwords to remember, and to remember which password matched which system, (2) end users also had non-work-related passwords, which added to the total number of passwords they had to remember, which sometimes interfered with their ability to remember work-related passwords, and (3) end users had to regularly change their passwords which made it more difficult to remember them.

In addition, end users described experiencing problems relating to the processes and procedures surrounding access control, where if they found themselves in a situation whereby they were not capable of performing certain protective actions because of the required levels of effort and time, then they became less willing to protect information, where they would choose instead to behave insecurely to enable them to complete their primary work tasks.

7 Security Testers Experiences of Information Security Management in Organisations

7.1 Introduction

As explained in chapter three, the theoretical framework developed in this study is primarily based upon the Routine Activity Approach, which states that crime events comprise three minimal elements: a likely offender, a suitable target, and the absence of capable guardians. Further, while a major focus of this study is toward understanding how to improve the guardianship of information in relation to end users, it is also argued that security testing may present opportunities to investigate the ways in which likely offenders operate when attacking organisations in the real-world, as the overall goal of security testing is to simulate those attacks that take place in the real-world. This may then help to improve the levels of protection of information in organisations by identifying various security weaknesses and/or possible improvements in the behaviour of guardians, such as security managers and end users.

In addition, it is argued in this study that the crime script approach (developed in accordance with the Rational Choice Perspective) may prove useful when investigating security testing as the crime script approach involves breaking down crime events into different stages with an in-depth focus on what each stage involves, the goals and objectives for each stage, and the different roles and required actions or use of specific tools during the commission of each stage.

Therefore, this chapter presents the findings from interviews with security testers about their experiences of performing security testing in organisations via the use of the crime-script approach.

Lastly, as discussed in literature review chapter, there are two main types of security testing: network-based penetration testing and physical-based penetration testing. The former involves remotely trying to gain unauthorised access to an organisation's network while the latter involves directly trying to gain unauthorised access to an organisation’s network. Further, in real-world settings, both types may incorporate social engineering aspects.

However, during interviews security testers often referred to network-based penetration testing simply as penetration testing, and to physical-based penetration testing simply as social engineering. Therefore, to make things easier in this chapter, when using the term penetration testing, this will refer to network-based penetration testing, and when using the term social engineering, this will refer to physical-based penetration testing.

The chapter is therefore split into two main parts. The first main part presents the findings relating to security testers experiences of penetration testing and the second main part presents the findings relating security testers experiences of social engineering testing.

7.2 The nature of penetration testing

Interviews with security testers began with a general discussion toward the nature of penetration testing. The purpose was to understand first, what is penetration testing, and second, how penetration testing connects to information security management and the role it played in improving the levels of protection of information in organisations.

During interviews, security testers described penetration testing as the simulation of real-world attacks against an organisation’s network. For example, one security tester described penetration testing as,

> Simulating the malicious intent of cybercriminals … trying to take over your system. (Gary, Senior Penetration Tester)

Similarly, another security tester commented,

> We act, when we perform testing, as those people that are out there and they just want to harm you. (Sarah, Senior Penetration Tester)

In addition to the above comments, security testers described how simulating real-world attacks could be broken down into three key elements.

The first key element described by security testers was *identifying vulnerabilities.* Security testers described this as identifying vulnerabilities that existed within an organisation’s network. Vulnerabilities were described as weaknesses in the design, configuration, and/or managing of an organisation’s network which would facilitate real-world threat actors gaining unauthorised access. As one security tester commented,

> Penetration testing looks for vulnerabilities, and vulnerabilities, if you like, are the keys to the door. (Graham, Ethical Hacker)

The second key element described by security testers was *exploiting vulnerabilities.* Security testers described this as exploiting vulnerabilities to provide validation that certain vulnerabilities can in fact be exploited in the real-world. As one security tester commented,

> Identify if there are any obvious vulnerabilities … and then trying to combine issues which I’ve discovered … to see if I can exploit them. (Gary, Senior Penetration Tester)

Importantly, security testers described how exploitation of vulnerabilities provided the validation or ‘proof of concept’ to an organisation that the identified vulnerabilities were in fact exploitable. For example, one security tester commented,

> You pick up on some vulnerabilities that are there … follow that up to extract data, to back up your case. (Graham. Ethical Hacker)

The third key element described by security testers was *fixing vulnerabilities.* Security testers described this as providing recommendations to organisations on how to fix vulnerabilities. As one security tester commented,

> Taking a company’s system and trying to analyse what security defects are in it … and where possible, giving suggestions for how to fix it. (Mary, Director of Penetration Testing Company)

We can already begin to understand from the above comments the important contributions that security testing may have in terms of improving the levels of protection of information in organisations. Not only was penetration testing described as helping organisations identify where they were most vulnerable to attacks from real-world threat actors, but security testers were also able to provide recommendations to organisations on how to prevent such attacks taking place.

In terms of guardianship of information, this demonstrates how security testing may enable organisations to reduce the likelihood that the necessary conditions of crime events converge in time and space. In other words, penetration testing may help reduce the opportunities for likely offenders to converge in time and space with suitable targets lacking capable guardianship.

Indeed, security testers described how successfully performing all three of the above elements would then help to improve information security management in organisations because it enabled organisations to assess the level of protection of information against threat actors in the real-world. For example, one security tester described how organisations,

> Need to find some way to demonstrate … that they, as an organisation, are as secure as they should be … So, having security testing baked into an organisation's security process … makes them less likely to have that kind of issue. (Mark, Accounts Manager at Penetration Testing Company)

Importantly, security testers stressed that although penetration testing is an important part of information security management, organisations must also properly manage other areas of information security, such as the development and implementation of security controls (including technical and non-technical security controls), before introducing penetration testing activities. For example, one security tester described how information security also includes,

> All the other things that are associated with it … things like your firewalls … it also includes things like your information security

> policies … and what training you provide your users. (Mary, Director of penetration testing company)

Lastly, although penetration testing played an important role towards protecting information, security testers described two major limitations. First, penetration testing did not guarantee that an organisation was secure in the real-world. Security testers made it very clear that a penetration test provides a static image of the levels of protection of information within organisations. As an organisation evolves, this may introduce new vulnerabilities or change the level of protection surrounding information. In addition, technology is constantly changing and new ways to protect and attack organisations subsequently emerge. Thus, having a penetration testing performed did not mean that organisations were necessarily secure from current or future threats. As one security tester commented,

> What you’re doing is taking a snapshot of the security of a system, and systems are always evolving, you know. Today it’s in one state and tomorrow it may be in another. (Larry, Senior Penetration Tester)

Similarly, another security tester commented,

> Technology is advancing really fast, and also hacking techniques and things like that are advancing just as fast – they’re keeping up with technology. So, it’s just a moving target all the time. (Juliette, Director of Penetration Testing Company)

Consequently, it was highly recommended by security testers that organisations regularly perform penetration testing as a normal part of managing information security in organisations. As one security tester commented,

> There are vulnerabilities that come out every day … security is a continuous process and they [organisations] need to do it, well, as often as they can. (Gary, Senior Penetration Tester)

The second limitation described by security testers was, penetration testing only assesses an organisation's level of protection against the skillset of the security tester(s) involved, which does not guarantee that all other security testers (and more importantly threat actors in the real-world) would have performed to the same standard. For example, one security tester commented,

> Sometimes these people could be tired. Sometimes they can miss things. Sometimes they could be inexperienced. And so, at the end of the day … it's only as good as the people who are performing it. (Juliette, Director of penetration testing company)

Overall, we can understand from the above comments that security testers described the purpose of penetration testing as simulating real-world attacks against organisations, which were broken down into three key elements: (1) the identification of vulnerabilities, (2) the exploitation of vulnerabilities, and (3) the fixing of vulnerabilities. The value this had for organisations was it enabled them to assess the overall level of protection of information provided by security controls against real-world malicious threat actors.

However, security testers stressed that penetration testing did not provide those organisations concrete assurance that they were secure against all types of attacks due to certain limitations within penetration testing and security testers.

In the context of guardianship of information, this demonstrates the important contributions that security testing and security testers may provide to organisations. By simulating real-world attacks this may help organisations to better understand how offenders are likely to attack them, and to better understand the organisational settings of their attacks, such as which vulnerabilities were exploited and how organisations can fix those vulnerabilities before they are exploited in the real-world. As a result, this may improve the likelihood that information is in the presence of capable guardianship.

7.3 The different types of penetration testing

Following discussions about the nature of penetration testing, were discussions about the various types of penetration tests that security testers performed. The purpose was to try and identify the different types of penetration tests available to organisations; what each involved, and how each influenced the commission of the penetration test.

Security testers described three main types of penetration tests: black-box, white-box, and gray-box testing. Each penetration test was described as simulating the real-world location of the attacker in relation to the organisation, which then determined the amounts of information security testers were provided about the target. Each of the three types of testing will now be presented and discussed.

The first type of penetration test described by security testers was *black-box testing*. Security testers described black-box testing as simulating real-world external attacks. Therefore, security testers were not provided with any information about a target. All the necessary information was gathered during the actual penetration test. For example, one security tester commented,

> Black-box is where you come across a system where you're not told what's running on it, you don't know the code behind it, you don't know the setup, you have to figure all this out … it's more akin to a real external attacker. (Peter, Penetration Tester)

Consequently, black-box testing was described as the most challenging type of penetration test, as security testers had less information with which to plan their attacks. As one security tester commented,

> Those are the most difficult tests because you go on site and you don't know what you're going to face, what kind of tests you need to prepare for. (Gary, Senior Penetration Tester)

The second type of penetration test described by security testers was *white-box testing.* Security testers described white-box testing as the simulating of real-world internal attacks. Further, the simulated threat actor was someone who had high levels of access and knowledge surrounding an organisation's network. Therefore, during white box tests security testers were provided with very detailed information about a target (including 'source code'[4]) and privileged access to an organisation's network. As one security tester commented,

> The tester has knowledge of infrastructure equal to a system administrator, they also have credentials for all the services, applications, and machines on the network. (Peter, Penetration Tester)

The third type of penetration test described by security testers was *grey-box testing:* Security testers described gray-box testing as similar to white-box testing. However, security testers were only provided with partial information about a target and moderate levels of access to an organisation's network. Thus, they were not provided with any detailed information about the types of systems, services, and devices that make up that network. As one security tester commented,

> Then there's the in-between, which is the grey-box testing, where you also have a login to the application, but you don't have the source code. (Michael, Hacker)

This may then represent either a mid-level internal attacker or an external attacker who might have partial information, whether because they gathered it during their attack or got it from someone internally.

We can understand from the above comments that penetration testing involved three main types of penetration tests which served different purposes. Black-box testing served to simulate an external attacker, such as when a malicious hacker tries to hack into an organisations network. White-box testing served to simulate an internal attacker, such as when a malicious insider tries to hack an organisations network from

[4] Source code was generally described as by security testers as human readable information about a system which would enable to better understand how it functioned and whether any vulnerabilities were present.

within. And grey-box testing served as a lesser version of a white box test. For example, a malicious insider who may wish to hack an organisations network from within but does not know or have as much detailed information about an organisations network due to their position within the organisation.

In the context of guardianship of information, this demonstrates the potential suitability of the crime-script approach when investing both security testing and real-world attacks against organisations. For example, we can understand how the various types of box-testing may provide suitable starting points when investigating penetration testing, which may then facilitate further investigation of the different types of attacks that may exist in the real-world.

7.3.1.1 The emergence of red teaming

Interestingly, when discussing the different types of penetration testing, security testers also described the emerging concept *red teaming*. Red teaming exercises were described by security testers as very different from standard types of penetration tests in three main ways.

First, there were no rules surrounding the types of attacks security testers could perform against an organisation. For example, whether performing a black-box, white-box, or gray-box test, security testers usually described there being a set of rules governing their behaviour during their attacks (see more details below on *establishing scope*). However, during red teaming exercises such rules generally did not exist. Which meant security testers were able to perform almost any kind of attack against any part of an organisation's network. As one security tester commented,

> Red team exercises generally will be a no-holds-barred assault on every facet of your system. (Graham, Ethical Hacker)

Second, in addition to being able to conduct any method of attack, security testers described how 'red team members' were required to conduct their attacks without being detected by the target organisation. Thus, during standard penetration tests security testers described how it was common for the organisation to become aware of the attacks being performed by security testers. Indeed, many organisations were described as informing their members that a penetration test was being performed. However, during a red team exercise no such warning would take place. As one security tester commented,

> Red teaming is a different way of doing penetration testing because a red team member is actually a person who will try to penetrate your website without the knowledge of the security operations team. (Matthew, Red Team Ethical Hacker)

Third, red teaming exercises were described by security testers as a more extensive and more in-depth variation of standard penetration testing because they focused not only on technical security controls that prevent malicious threat actors gaining unauthorised access, but also security controls developed and implemented to respond to (or correct) security incidents. For example, one security tester commented,

> It’s not just a test of the prevention mechanism, it’s also a test of your response mechanism … Being able to detect an attack, being able to handle an attack … it’s really more a test of an entire organisation. (Larry, Senior Penetration Tester)

Importantly, although red teaming exercises were described as an extremely valuable and comprehensive evaluation of an organisation’s security posture, security testers described how organisations should not engage in red teaming exercises unless they had already ensured that information security was at a high standard within the organisation. Further, they recommended that organisations first have standard penetration testing performed before moving toward red teaming exercises. For example, one security tester described red teaming as only suitable for,

> Companies that are at the right maturity level … because there are always the companies following the bandwagon … Red teaming is something you want to do when you think you have done all the best that you can, you know. (Larry, Senior Penetration Tester)

We can understand from the above comments that the value of red teaming exercises for organisations was the performing of attacks which were arguably even closer than standard penetration tests, to those performed by real-world threat actors, which also included the different scenarios relating to how an organisation would have to respond to those attacks. However, because red teaming exercises involved more extensive and aggressive attacks against organisations, it was therefore considered important that an organisation had already reached a high level of protection of information before performing read teaming exercises.

In the context of guardianship of information, this again demonstrates the potential value that security testing can have towards improving the protection of information in organisations. By performing red teaming exercises, organisations can experience an attack which more closely resembles that of real-world attacks and allows them to assess the overall security posture of the organisation, including the organisation's ability to detect and respond to security incidents as opposed to just preventing them.

7.4 The different actors involved in penetration testing

As explained in chapter three, as well as breaking down crime events into different stages, the crime script approach involves investigating the different roles and actions that are performed by different actors during the commission of each stage. Therefore, this next section presents the findings relating to the different actors involved in security testing and how different roles were assigned and how this influenced the penetration test.

During interviews, security testers described how penetration testing would be performed by either an individual security tester or by a team of security testers. Further, this was generally determined by (1) the size of the organisation, (2) the number of targets to be penetration tested, and (3) the time-frame within which the penetration test had to be completed. For example, one security tester commented,

> Essentially, any type of pen-testing activity can be accomplished by an individual or by a group, usually it's just a matter of time and budget. (Peter, Penetration Tester)

Importantly, although penetration testing could be performed individually or by teams of security testers, security testers generally described working in teams because this offered them several advantages.

The first advantage described by security testers was, working in teams enabled security testers to combine the different levels of expertise amongst team members which maximised the number of possible attacks they could perform against an organisation. For example, one security tester commented,

> We work together in our current context purely because we both have our own specialities and the area is so broad … so I think it helps to work as a pair. (Graham, Ethical Hacker)

The second advantage described by security testers was, by working in teams this maximised the pool of attackers that an organisation would assess itself against in the real-world (although recall this did not guarantee toward the organisation being secure). Thus, the major advantage here would be for the organisation rather than the security testers themselves when performing the penetration test. As one security tester commented,

> People who have been in the industry long enough realise … combining people means you get a very powerful team … So, overall, you’re better improving your security. (Larry, Senior Penetration Tester)

The third advantage described by security testers was, working in teams provided security testers the opportunity to learn from other team members about different ways to perform certain attacks, which would then help less experienced security testers develop their skillset. For example, one security tester commented,

> You also have the chance to see other ways of doing the same thing and to learn more tricks. (Peter, Penetration Tester)

We can understand from the above comments that penetration testing can be performed by a single security tester or by a team of security testers. However, there were several advantages described by security testers when performed in teams, both to the organisation being penetration tested and the security testers themselves.

In the context of guardianship of information, this suggests that performing penetration testing in teams can further help organisations improve their security against a larger number of possible attackers who may have varying levels of skills and expertise.

This also suggests that the decision-making processes of likely offenders in the real-world may be influenced by the various 'procedural requirements' of performing certain types of attacks against organisations, where certain actions may require certain offenders who specialise in performing those attacks. Thus, in the real-world organisations may not be as vulnerable to different types of attack, or different attackers may not be able to perform certain types of attack due to the skill requirements of performing them.

7.5 The role of technology during penetration testing

As explained in chapter three, the crime script approach also investigates how various tools or 'crime facilitators' help during the commission of crime. Therefore, this next section presents the findings relating to security tester's experiences of using various tools during penetration tests.

Security testers described how technology (both hardware and software) was an important factor when performing penetration testing because the target of the penetration test was the organisation's technical infrastructure, namely its network and all the systems, services, and devices connected to this. As one security tester commented,

> In a sense it is key for us to do testing because what we're testing is running on technology. (Paul, Ethical Hacker)

Interestingly, security testers described how they would regularly use various types of automated technology which provided them two major advantages when performing penetration tests.

First, security described how it drastically reduced the level of effort of performing certain tasks. Indeed, many tasks were described by security testers as performed solely by technology. For example, one security tester commented,

> To actually find out whether it's got that [vulnerability] manually would be the work of weeks … and this tool more or less automates the whole thing and does it for you in like half an hour. (Mary, Director of Penetration Testing Company)

Second, security testers described how automated technology enabled them to multitask during the penetration test, whether during identification of vulnerabilities or during the actual launching of various attacks. For example, when discussing the process of identifying vulnerabilities in an organisation, one security tester commented,

> In that case … it's easier for me to have some kind of tool … that is engaging on the wireless hacking, while I use my laptop to conduct scans … on the internal network. (Gary, Senior Penetration Tester)

Importantly, while security testers described automated technology as providing them with two major advantages, they stressed that the use of automated technology did not necessarily mean that a security tester fully understood how to use such technology. Nor did it mean that the penetration test will properly identify and exploit vulnerabilities; as such technologies still required the input and experience of the security tester(s) involved. For example, one security tester commented,

> The importance of technology is less important than the person that's driving it … what it's doing and what the output is and how to

> interpret it, and then how to use that information somewhere else … that’s where the experience comes in” (Michael, Hacker).

Similarly, another security tester commented,

> A lot of the tools … are pretty automated now. However, knowing where to leverage them, and knowing how to configure them … that’s what separates good penetration testers from great penetration testers. (Leanne, Ethical Hacker)

We can understand from the above comments that technology played an important role during penetration testing because the target of a penetration test was the technical infrastructure of an organisation. In addition, automated technology allowed security testers to multi-task and/or to perform certain tasks more quickly through the process of automation. However, although technology played an important role, the overall success of a penetration test still heavily relied upon the mindset and skillset of the security tester(s) and their ability to apply both during the penetration test.

In the context of guardianship of information, this suggests that certain technology, while playing an important role in defending organisations against cyberattacks, may also facilitate the actions of likely offenders. Moreover, one of the major tenets of the Rational Choice Perspective, which underpins the crime script approach, is that the effort to perform criminal acts will influence the levels of willingness of offenders to perform them. Thus, as technology reduced the level of effort of security testers, this suggest that technology may also help to reduce the level of effort for many real-world threat actors to perform certain types of attacks against organisations.

7.6 Breaking down the crime event: The different stages of penetration testing

As discussed in chapter three, the main purpose of the crime script approach is to identify the key stages of an attack sequence and the goals and objectives of each stage to better understand how an offender might perform an attack against an organisation in the real-world. Further, the crime script approach advocates the use of the *universal crime script*, which offers a standardised set of stages which can be used to map the commission of any crime. Therefore, this next section presents the findings relating to the experiences of security testers of the different stages of performing a penetration test, which are mapped onto the universal crime script.

7.6.1 Preparation stage: Establishing scope

The first stage in the universal crime script is that of the *preparation stage*, where offenders undertake any preparatory actions prior to engagement in the crime event.

Security testers referred to the first stage of a penetration test as *establishing scope*. The main goal of this stage was to establish the parameters within which the penetration test must take place. In other words, how much of an organisation will be included within the penetration test, how the penetration test will be performed, whether it will involve one or more security testers, and the time-frame within which it must be completed. As one security tester commented,

> What happens is you'll get a scope of work created … it can range from just a single day to a number of weeks depending on the size, number of different systems you're looking at, how many people you're throwing at it. (Michael, Hacker)

In addition, security testers described how establishing the scope of a penetration test should be connected to various information assets and security risks of the organisation, as this would maximise the value of having penetration testing performed, where the outcomes properly connected with the security goals and objectives of the organisation. For example, one security tester described how establishing scope should be based upon

> What are your assets, you know … The scope is then worked around that and it says … to prove that this asset is safe we're going to need to do X, Y, Z on system A, B and C. (Neal, Ethical Hacker)

Lastly, security testers described how establishing scope was important because it helped to protect security testers against any actions taking towards them by an organisation should a security breach occur following a penetration test (recall the earlier comments about the limitations of penetration testing). As one security tester commented,

> We would make it absolutely clear in the proposal … because if the shit does hit the fan and something happens … they don't remember the caveats even if they are documented; they just remember the fact that you tested them, and they got hacked and they're in the press. (Juliette, Director of Penetration Testing Company)

We can understand from the above comments that the first stage of performing a penetration test was described by security testers as establishing scope, where the main goal was to determine the parameters within which the penetration test took place. Further, the scope for testing was connected to the various assets and security risks of the organisation being tested. Lastly, by establishing scope, this ensured security testers were protected against any legal actions taken against them following some security incident to the tested organisation.

7.6.2 Pre-condition stage: Information gathering

The second stage in the universal crime script is the *pre-condition stage*, which involves preliminary investigation towards the conditions which would facilitate the commission of a given crime.

Security tester referred to the second stage of a penetration test as *information gathering*. The main goal of this stage was described by security testers as gathering as much information about a target organisation which would then enable them to produce an entire map of the organisation's network, including the systems, services, and devices running on the network. As one security tester commented,

> It's like a military operation – you're planning out what the enemy landscape looks like on your board – they have X in this position, and then it's connected to this … and we think that they have these protections in place. (Leanne, Ethical Hacker)

Interestingly, security testers described two approaches to gathering information about a target organisation, *active* and *passive* information gathering. For example, one security tester commented,

> Information gathering involves gathering preliminary data and intelligence on your target … to better plan your attack. This can be done actively, meaning that you are directly touching the target, or passively. (Peter, Penetration Tester)

Passive information gathering was described by security testers as gathering information about an organisation without the organisation becoming aware of such activities. Thus, security testers described utilising various non-intrusive gathering techniques such as online search engines. In contrast, active information gathering was described as gathering information using various automated security software. For example, one security tester commented,

> You try to work out the attack surface of the system, and often this is where a lot of automated tools are deployed. (William, Senior Penetration Tester)

We can understand from the above comments that the second stage of performing a penetration test was described by security testers as gathering as much information about an organisation so that security testers were better able to plan out their attacks. However, at this stage the goal was only to gather information, which could be performed either passively or actively.

7.6.3 Instrumental pre-condition stage: Vulnerability scanning

The third stage in the universal crime script is the *instrumental pre-condition stage*, which primarily refers to actions such as target selection and identification of the most effective way to commit an attack.

Security testers referred to the third stage of performing a penetration test as *vulnerability scanning*. Security testers described the main goal of this stage as performing vulnerability scans across all the systems, services, and devices that were identified as running on the organisation’s network (which formed the previously produced map of an organisation’s network) to identify any vulnerabilities which might be present. For example, one security tester commented,

> The vulnerability scanner looks for the footprint of the vulnerability … you can kind of assess what services are running … and if those services need to be running and if those services are vulnerable. (Graham, Ethical Hacker)

Interestingly, security testers described how they would deliberately target specific parts of an organisation’s network for vulnerability scans because they were well-known to have security vulnerabilities. As one security tester commented,

> There’s a couple of different packages and free and closed software suites that allow you to scan for tell-tale signs of known vulnerabilities … what we call ‘low-hanging fruit’. (Graham, Ethical Hacker)

Once security testers had successfully scanned the organisation’s network they described moving on to select the most suitable ‘penetration point’ which was based upon the vulnerabilities found, the skills that the security testers possessed, and the required effort associated with performing the selected attack(s). As one security tester commented,

> You’re going to try to identify which systems are vulnerable, and then you’re going to plan out how you’re going to penetrate into the network. (Leanne, Ethical Hacker)

We can understand from the above comments that the third stage of performing a penetration test was described by security testers as primarily involving the scanning of an organisation’s network to identify as many vulnerabilities as possible. Then, depending upon the types of vulnerabilities found, this helped to determine the most suitable target for an attack, which simultaneously determined which security tester would be better suited to perform the attack, due to differences in the skillsets of security testers.

7.6.4 Instrumental initiation, actualisation, and doing stages: Gaining access and control

The fourth, fifth, and sixth stages of the universal crime script are *instrumental initiation*, *actualisation*, and the *doing* stages, which generally describe the main parts of executing a given crime.

The next three stages of performing a penetration test were collectively referred to by security testers as *gaining access and control*. Security testers described the overall goal of these three stages as gaining unauthorised access and control over an organisation's network to enable them to successfully exfiltrate as much organisational information as possible.

The first stage of gaining access and control (which corresponded to the *instrumental initiation* stage of the universal crime script, and which was referred to by security testers as *exploitation of vulnerabilities*) was described as exploiting one or more of the previously identified vulnerabilities to gain preliminary access to an organisations network. For example, one security tester commented,

> Next is gaining access … so, perform exploitation on the targets to gain control. (Peter, Penetration Tester)

The second stage of gaining access and control (which corresponded to the *instrumental actualisation* stage of the universal crime script, and which was referred to by security testers as *escalation of privileges*) was described as using the exploited vulnerabilities to try and identify additional vulnerabilities within the target network, which potentially enabled further manoeuvring within the organisation's network to gain even higher levels of access and control. As one security tester commented

> You'll exploit a particular issue, leverage that … and it might be what we call horizontal or vertical privilege escalation. If you get in as user A, can you get in as user B … and then what can we do from there. (Michael, Hacker)

The final stage of gaining access and control (which corresponded to the *doing* stage of the universal crime script, and which was referred to by security testers as *exfiltration of data*) was described as using the previously gained levels of access and control to then extract the information from the organisation’s network. For example, one security tester commented,

> Exfiltration, which involves taking data outside the target’s network.
> (Peter, Penetration Tester)

We can understand from the above comments that the three main stages which comprised gaining access and control over an organisation’s network were described by security testers as involving initial exploitation of the identified vulnerabilities that formed the basis of the two previous stages, namely information gathering and vulnerability scanning, which was then followed by attempts to escalate privileges to manoeuvre within the organisation’s network to further increase the levels of access and control, and finally exfiltration of information from the organisation’s network.

7.6.5 Exiting stage: Covering tracks and persistence

The seventh stage in the universal crime script is the *exiting stage*, which refers to actions taken immediately following the execution of a given crime.

Security testers referred to the seventh stage of a penetration as *covering tracks*. Security testers described covering tracks in two ways, where each had a specific goal. If security testers were not performing red teaming exercises, then the main goal of covering tracks was to restore any changes made to the organisation’s network back to its original state, simply to allow the organisation to return to normal functioning. However, if security testers were performing red team exercises, then the main goal of covering tracks was to further make sure that any activity on the network during the attack was not detected by security controls which might alert the organisation about the penetration test. For example, one security tester commented,

> The attacker must then take the necessary steps to remove all resemblance of an attack in case of detection. Any changes that were

> made during the attack … all must return to a state of non-recognition. (Peter, Penetration Tester)

In addition, security testers described how during red teaming exercises they would sometimes implement ‘backdoors’ to prolong having access and control over an organisation’s network, which would then enable them to later gain access, such as to continue exfiltration of organisational information. This was referred to by security testers as having *persistence* on an organisation’s network. As one security tester commented,

> In the case of red teaming, you want persistence within the target environment in order to gather as much data as possible. (Peter, Penetration Tester)

We can understand from the above comments that the seventh stage of performing a penetration test was described by security testers as covering their tracks, which mainly involved either restoring an organisation’s network to its original state or involved covering up the actions performed by security testers to make sure they remained undetected by the organisation, and were still able to gain unauthorised access and control should they require it.

7.6.6 Post condition stage: reporting back

The final stage in the universal crime script is the actions which follow the completion of a given crime.

Following the successful completion of a penetration test, security testers described reporting back to the organisation about the penetration test. The main goal of this stage described by security testers was to produce a report which provided the organisation with as much detailed information as possible about the penetration test, such as the process of gathering information and the vulnerabilities which were discovered within the organisation’s network, and how these enabled security testers to perform their attacks, followed by the recommended actions and measures that an organisation can take to prevent such an attack taking place in the real world. For example, one security tester commented,

> I have a process that's well documented and I follow in order to be able to provide … a report which describes what is it finding [the penetration test], how I came up with it, how did I discover it … and also suggest ways to the company to remedy the issue, based on experience and based on best practices. (Gary, Senior Penetration Tester)

Interestingly, security testers also described how reports would normally be split into two sections for two main audiences, one for upper management and one for security managers. This was because upper management and security managers were described as having very different levels of understanding towards information security management. Therefore, the writing style of each section of a report had to accommodate this. For example, the goal towards upper management was described by security testers as helping them to understand how the organisation was successfully attacked, what the impact would be for the organisation in terms of affecting business, and how the organisation can try to prevent this from occurring in the real world. In contrast, for security managers, the goal described by security testers was to help them understand which vulnerabilities were present within their network and how security testers were able to exploit them and what this enabled them to do, and which specific security controls or improvements to existing security controls would have prevented security testers from gaining unauthorised access and control over their networks. As illustrated by the following comment,

> The first three or four pages anyone could pick up and read and it's not technical. It's board level stuff. So, you could read that, you could get the gist of what's going on … we list business context, so we say why that's a risk to your company … and then we follow that with a breakdown of all the vulnerabilities we found. So, generally we name the vulnerability itself … give numbers and compendium of all the information surrounding that vulnerability … and we usually put kind of an action plan that breaks down the order and the priority that we would personally give if we were to fix this, along with some just general network security hygiene stuff. (Graham, Ethical Hacker)

We can understand from the above comments that the final stage of performing a penetration test was described by security testers as reporting back to the organisation about the penetration test. The goal of this stage was to inform the organisation about how security testers were successfully able to gain unauthorised access and control over the organisation's network, including all actions leading up to that point, and then to inform the organisation on how to prevent such actions taking place in the real-world.

This demonstrates the potential value that penetration testing may have had for those organisations, as not only did the penetration test identify and exploit vulnerabilities within their networks, which showed those organisations the likelihood and impact this would have for them in the real-world, but it also helped those organisations (namely, upper management and security managers) to understand how best to fix those vulnerabilities, which ultimately may have improved the levels of protection of information in those organisations.

7.7 Summary of penetration testing findings

Overall, the findings from interviews with security testers relating to penetration testing showed that penetration testing was described as simulating real-world attacks against organisations, which were broken down into three key elements: (1) the identification of vulnerabilities, (2) the exploitation of vulnerabilities, and (3) the fixing of vulnerabilities. further, while having an important role for improving the protection of information in organisations, penetration testing was not described by security testers as providing concrete assurance that organisations were secure against all types of attacks due to certain limitations within penetration testing and security testers.

There were three main types of penetration testing described by security testers; *black-box testing*, which served to simulate external attacks; *white-box testing*, which served to simulate internal attacks; and *grey-box testing*, which served as a lesser version of white box testing. In addition, security testers described red teaming as a more advanced type of penetration testing which involved security testers using more aggressive and covert methods of attacking organisations.

Regarding the various actors and tools used during penetration testing. Penetration testing was described by security testers as performed both by single security testers and teams of security testers; where there were several advantages when performed in teams, both to the organisation being penetration tested and the security testers themselves. In addition, security testers described technology as playing an important role during penetration testing because the target of a penetration test was the technical infrastructure of an organisation. Further, automated technology allowed security testers to multi-task and/or to perform certain tasks more quickly through the process of automation.

Lastly, penetration testing involved numerous stages which were successfully mapped onto the universal crime script. The main stages described by security testers were: (1) *establishing scope*, which comprised establishing the parameters within which the penetration test must take place; (2) *information gathering*, which comprised gathering as much information about a target organisation and its network to plan possible attacks; (3) *vulnerability scanning*, which comprised scanning an organisation's network to identify any vulnerabilities which might be present; (4-6) *gaining access and control*, which comprised exploitation of identified vulnerabilities, followed by attempts to escalate privileges, and culminating in exfiltrating of organisational information from the organisation's network; (7) *covering tracks*, which comprised either restoring any changes made to the organisation's network back to its original state and/or implementation of backdoors to prolong access and control over the organisation's network; and (8) *reporting back,* which comprised the writing of reports which outlined the processes and actions of each stage followed by recommended actions and measures that an organisation can take to prevent such an attack taking place in the real world.

7.8 The nature of social engineering

This second part of the chapter presents the findings from interviews with security testers about their experiences of performing physical-based penetration tests, which as mentioned above were simply referred to as social engineering tests.

Interviews with security testers about social engineering testing began with a general discussion toward the nature of social engineering. Again, the purpose was to understand first, what is social engineering, and second, how social engineering testing connects to information security management, and the role this played towards improving the protection of information in organisations.

During interviews, security testers described how social engineering testing was primarily the simulation of real-world attacks against organisations. For example, one security tester commented,

> You hire good guys who can do bad things to break into your company to tell you how they did it, so the bad guys can't get in. (Colin, Chief Social Engineer)

Similarly, another security tester commented,

> I'm the guy that thinks like a criminal; I will try and attack your business like a criminal, but at the end of it you'll get a nice, glossy report and I'll discuss it with your board. (Ryan, Chief Social Engineer)

However, unlike penetration testing, social engineering testing was described by security testers as identifying and exploiting *human* vulnerabilities rather than *technical* vulnerabilities when attacking organisations. For example, one security tester commented,

> Hacking is the art of making something, not just a computer, do something it was unintended to do. Social Engineering is the same thing … It is all hacking, it's just the medium that is being hacked is different. (Stanley, Social Engineer)

Similarly, another security tester described social engineering as,

> Testing the ‘human element’ … in terms of attempting to use only people to get into an organisation. (Julie, Social Engineer)

Importantly, although security testers described how end users were often targeted during a social engineering test, they emphasised that the ultimate target was the organisation’s information, which the security user either had direct access to or was protecting access to. Thus, security testers described the overall goal of social engineering tests as trying to get the targeted end user to either divulge information that allowed the security tester to gain unauthorised access to the organisation’s network or to convince them to allow the security tester entry into the premises, wherein they could then gain access the organisation’s network. As one security tester commented,

> We don’t care about the person, it’s what the person controls … whether it’s the server, or whether it’s the office space, that’s what the attacker wants access to. (Colin, Chief Social Engineer)

We can understand from the above comments that the overall goal of social engineering was described by security testers as similar to penetration testing. The main difference being the pathway to which security testers tried to gain unauthorised access to the organisation’s information. In other words, rather than trying to remotely gain access by bypassing technical defences, security testers instead described trying to directly gain access by bypassing human defences. Consequently, security testers recommended that organisations performed both penetration testing and social engineering testing to make sure both technical and human defences were working together in tandem to protect information in organisations. For example, one security tester commented,

> You have to have security in both … if I’m using ancient software, I’ve not updated antivirus, my firewall rules stink, I have vulnerable software on all the computers *and* my human fails, now there’s a big risk for the company. (Colin, Chief Social Engineer)

Although security testers described social engineering as a necessary and important part of information security management, they felt that organisations generally favoured penetration testing over social engineering testing. For example, one security tester commented,

> I would say that the physical is probably the most overlooked area of weakness … a lot of the clients I work with, they don’t tend to put a focus on the physical controls as much as I would like. (Naomi, Chief Social Engineer)

Similarly, another security tester commented,

> We’re seeing an increase in social engineering pen tests but … A lot of companies are sadly not seeing them as co-joined. (Colin, Chief Social Engineer)

Consequently, security testers felt that many organisations and information were at increased risk because social engineering was becoming a more popular method of attack in the real-world, precisely because lower levels of attention were being paid towards making sure end users are capable at defending against social engineering-based attacks. As one security tester commented,

> If a company has heavily invested in technology to defend its assets and the challenge in terms of technology is too high … the attacker falls back on the end user using social engineering. If I can ask for a password instead of having to crack it, it’s much easier. (Peter, Penetration Tester)

Similarly, another security tester commented,

> Would you rather try… to penetrate a network or would you just rather make a phone call and get that information? As a social engineer, I’d rather make the phone call because in my mind that’s easier. Well, if it’s easier for me to think that way, then it’s easier for

> an attacker to think that way and that’s why it’s becoming more of an issue. (Naomi, Chief Social Engineer)

Thus, security testers stressed that social engineering testing must become an important part of information security management in organisations because it assesses the level of protection of information in relation to the non-technical controls developed and implemented by organisations. As one security tester commented,

> You can’t achieve cyber security without including social engineering … it’s necessary to look at humans and … that’s where it really fits in to all the cyber security. (Naomi, Chief Social Engineer)

Lastly, security testers described how social engineering testing had several limitations. The first two limitations were described by security testers as the same two limitations for penetration testing; namely, social engineering tests produced a static image of an organisation’s level of security (which may change over time) and that an organisation is only assessing itself against the security tester(s) performing the social engineering test. As one security tester commented,

> Social engineering tests are a snapshot of time and place; the thing that works today might not work tomorrow. (Stanley, social engineer)

In addition, security testers described a third limitation for social engineering testing, where certain types of attacks may not be allowed due to potential risks to individual targets. As a result, this somewhat reduced the level of realism of social engineering testing, as real-world attackers would not have such limitations. For example, one security tester commented,

> We would look at doing whatever we needed to do … and the problem is, obviously when you’re doing a test, you can only go so far … So, you’re hamstrung by both moral and legislative rules, which mean you can only take it so far. But in the real world, criminals don’t have that constraints. (Julie, Social Engineer)

Similarly, another security tester commented,

> As a social engineer you are going to try and find the path of least resistance … and this is what professional criminals do as well when they employ social engineering … but at the same time you have limitations because you still need to apply ethics while criminals do not … criminal social engineers, they may use blackmail or other methods of recruitment … but this is not possible when it comes to our job, we cannot do that. (Claire, Social Engineer)

We can understand from the above comments that social engineering, like penetration testing, was described by security testers as the simulation of real-world attacks against organisations. However, rather than trying to remotely bypass an organisation's technical defences, security testers would directly try to bypass an organisation's human defences. This helped towards understanding an organisation's level of protection of information and whether it was vulnerable to social engineering-based attacks. However, as with penetration testing, this should not be considered as providing definitive proof that an organisation is secure against social engineering attacks, due to certain limitations inherent within social engineering tests and security testers.

In the context of guardianship of information, this helps demonstrate the potential contributions that security testers and social engineering testing may provide to organisations. By simulating real-world attacks this may help organisations better understand how offenders are likely to attack them and to identify various human vulnerabilities. This also helps demonstrate the important role that both security managers and end users play as guardians of information and the importance of organisations making sure end users are both willing and capable towards protecting information against social engineering attacks in the real-world.

7.9 The different kinds of social engineering tests

Security testers described four types of social engineering tests (generally referred to as attack vectors).

The first type of social engineering test described by security testers was *phishing.* Security testers described phishing as when the security tester tried to bypass human defences through email, and which involved tricking the targeted end user into either opening an attachment which contained malicious software or to visit a fake website which allowed the security tester to harvest their credentials. For example, one security tester described phishing as,

> Send someone an email, get them to double click on an exe … that thing then connects out to a command and control server, and then a hacker can get into your network from that one PC and branch out. (Michael, Hacker)

The second type of social engineering test described by security testers was *smishing.* Security testers described smishing as identical to phishing, although the attack would be performed through text messages sent to the targeted end user. As one security tester commented,

> You can bring your own devices to work. Attackers know that so they're sending SMS messages with links that go to malware … that phone connects to a corporate network and now they can use that to hack the network. (Colin, Chief Social Engineer)

The third type of social engineering test described by security testers was *vishing*. Security testers described vishing as when trying to bypass human defences through voice and involved tricking end users into divulging information about an organisation that might enable them to remotely gain access to the organisation's network, or as a method of gathering information which could be used during an impersonation attack (see below). As one security tester commented,

> The next one, alongside phishing, is vishing, which is talking to someone over the phone. (Wesley, Social Engineer)

The fourth type of social engineering test described by security testers was *impersonation.* Security testers described impersonation as when a security tester tries to directly bypass human defences through pretending to be someone who is either authorised to access an organisation’s network or is someone who is authorised to enter into the premises, wherein the security tester can then gain access to an organisation’s network. As one security tester commented,

> And of course, impersonation … acting like an employee to get onsite. (Colin, Chief Social Engineer)

We can understand from the above comments that social engineering testing was described as comprising four main types of security tests or attack vectors. In the context of guardianship of information, this again demonstrates the potential suitability of the crime script approach when investigating social engineering-based attacks against organisations. For example, we can understand how each of the above attack vectors may present suitable areas for further investigation relating to social-engineering attacks which may help improve our understanding of how real-world attacker may tack organisations.

As explained in previous chapters, the focus in this study is mainly on physical-based or direct forms of social engineering attacks. Therefore, the remaining sections of this chapter will largely focus on those findings relating security testers experiences of performing impersonation attacks against organisations. Again, the reason being the first three types of social engineering tests may be understood as remotely gaining access to an organisations network and may also form part of a penetration test. Whereas impersonation attacks may be considered directly trying to gain unauthorised access, and arguably they heavily rely upon social engineering-based tactics. Therefore, they potentially offer the most insight into the different tactics and tools used by security testers during social engineering testing.

7.10 The tactics and tools used by security testers during social engineering tests

As explained in chapter three, as well as breaking down crime events into different stages, the crime script approach involves investigating the different actors and tools that are used during the commission of each stage of a crime event. To better understand these aspects of performing social engineering testing, it is useful to understand the tactics and tools used by security testers during social engineering tests. Therefore, this next section presents the findings relating to two main persuasions techniques used by security testers to bypass human defences during impersonation attacks, as this will help understand the above related aspects of performing social engineering tests.

As discussed above, the goal of a social engineering test was described by security testers as trying to get end users to either divulge certain information that allowed the security tester to gain unauthorised access to an organisation’s network or to allow the security tester to enter an organisation’s premises wherein they could gain unauthorised access. Whether or not the security tester achieved the former or latter was described by security testers as dependent upon their ability to persuade or convince the targeted end user to perform either action. Thus, when performing an impersonation attack against an organisation, security testers described using two main persuasion techniques. Both will now be presented and discussed.

7.10.1 Pretexting

The first main persuasion technique described by security testers was *pretexting*. Security testers generally described pretexting as establishing the ‘cover story’ of the security tester. For example, one security tester commented,

> A lot of it involves coming up with what’s called a pretext, basically … the reason why you are there. (Wesley, Social Engineer)

Similarly, another security tester commented,

> One way to get to people, is to pretend to be someone … where the goal of that is to get them to respond to that, to give you information. (Julie, Social Engineer)

The importance of pretext was described by security testers as providing them with a reasonable explanation as to why they were directly communicating with the targeted end user, which then assisted security testers when trying to convince them to either divulge information or to allow them to enter the premises. For example, one security tester described how pretext,

> Can make you believe that I'm part of your system, I'm part of your world, and then it seems a little less likely that I'm trying to pull the wool over your eyes. (Naomi, Chief Social Engineer)

Interestingly, security testers described how pretext worked by playing to the various expectations that end users would have towards a chosen pretext, whereby if certain factors of the security testers pretext closely aligned with the pre-existing beliefs that end users had towards it, this then created a sense of familiarity towards the security tester which would then reduce the likelihood that end users would not believe the authenticity of the security testers pretext. As one security tester commented,

> You create a narrative that enables you to hit a person or to get a person to give you access. … you're not giving them enough reason to doubt a pretext … and it's setting off those kind of familiarity biases … What you have to do is get someone over the line of doubt. (Julie, Social Engineer)

Thus, security testers described how the overall effectiveness of using pretexting was influenced by the various factors relating to end user expectations connected to various pretexts; which required security testers to then use various tools or props to make sure the pretext closely aligned with those expectations. For example, one security tester commented,

> If we are going for the service technician, part of your pretext, to make it believable is, you have to have the uniform … You will need a fake ID, you will need to have all this in advance … And then … you will need to know what they say, how they say it, how they walk … And you have to play to that. (Wesley, Social Engineer).

Similarly, another security tester commented,

> You need to anticipate somebody's questions and answer them credibly … So, what is your reason for being there … And how long

> are you going to be there? So, you need to have answers that are very believable … You need to look like that kind of person. I can’t go in with my high heels on and pretend to be a technical repair person … I would be better going in with boots … I would definitely need to have a bag, things like that. The things that the person who did that type of job would wear. (Claire, Social Engineer)

Interestingly, security testers described how the use of team play would enable them to better perform certain pretexts and how having a variety of security testers meant they were better able to align their chosen pretexts with the expectations of those targeted during their attacks. For example, one security tester commented,

> Sometimes you need a team … you sometimes need someone who suits the pretext, rather than trying to tailor the pretext to suit you … we had to get into a PR company in London and everyone in there was under 30 and they all cycled in, they were all into their yoga and veganism and all this. And there was no way that I was fitting that profile … rather than me work something out … we had her [another security tester] as the frontman and to open the door … she is the best person to get in and then I’m the best person once I’m on the ground. (Julie, Social Engineer)

Similarly, another security tester commented,

> For the most part we work as a team, especially because in my company we’re 50% men, 50% women, and we'll utilise different pretext and vectors based on social bias … the right hand in my company is a small tiny little Japanese woman, and when we break into a company, social bias dictates that people will expect me to be the boss. Why? Because I’m a big male and she’s a tiny female, so we'll play on that, we'll utilise that … So, we like team efforts because we tend to be able to use different expectations while doing the attacks based on that. (Colin, Chief Social Engineer)

Lastly, security testers stressed that although pretexts were generally established prior to making contact with a targeted end user, oftentimes pretexts would need to be improvised depending on the situation the security testers found themselves in. For instance, it might transpire that the security testers understanding of the end users' expectations surrounding a chosen pretext might not be as expected, which meant the security tester would then have to try and adjust the pretext accordingly during the actual social engineering test. Thus, security testers described an important skill of security testers was being able to 'think your feet' to avoid end users doubting the authenticity of their pretext. As one security tester commented,

> Your pretext will only take you so far. Sometimes the situation will unravel in ways you don't always expect. And that's where improvisation comes in … so having a story is good but you should not stick entirely to what you are supposed to say at all times, you need to be able to improvise effectively if need be … You are supposing that everything will go wrong and you are always expecting it. (Claire, Social Engineer)

We can understand from the above comments that developing a pretext was described by security testers as an important part of social engineering testing and that the success of a social engineering attack heavily relied upon the ability of the security tester(s) to fully align themselves with the various expectations of their targets towards their chosen pretext. Further, depending on the pretext chosen, certain actors and props may play an important role when performing social engineering tests, which may also require improvisation during their engagement.

In the context of guardianship of information, this again shows the potential and important contributions security testers and security testing may have toward unearthing the many ways in which malicious threat actors may use social engineering tactics to bypass human defences in organisations, which may help organisations improve their defences against such attacks.

7.10.2 Emotional triggers

The second main persuasion technique described by security testers was using *emotional triggers*. The use of emotional triggers to bypass human defences was generally described by security testers as when the targeted end user primarily based their decisions upon emotional responses rather than through the logical and correct alignment between their expectations towards a chosen pretext, and the pretext delivered by security testers. For example, one security tester commented,

> What you're trying to do with emotion is get them into a frame of mind where logic just leaves them … emotion just kicks logic off the cliff … and people will then no longer be rational. (Julie, Social Engineer)

For instance, it might be the case that an end user is not fully convinced towards the authenticity of the security tester's pretext and may decide not to divulge information or to deny them access to a secure building. In such a situation, the security tester can then attempt to utilise one or more emotional triggers to compensate for this.

In general, security testers described two types of emotional triggers regularly used during social engineering tests, the *positive* and the *negative*. For example, one security tester commented,

> You can get someone to do something by threatening them. By pretending to be their superior… the other side is the softer side… that's more my style. (Wesley, Social Engineer)

The *positive* side was described by security testers as using positive emotional triggers to influence the security behaviour of end users. Security testers often described making end users develop a liking towards them through such things as flattery and pretending to have similar interests to end users, which they described as increasing their chances of success when trying to bypass security. For example, one security tester commented,

> We all have egos that liked to be stroked … perhaps somebody is proud of their appearance or has lost a lot of weight and so they will respond to a compliment … particularly to flattery that connects to hard work, you know, that's linked to their achievements; people find it difficult to push back against that … your cognitive defences then go down. (Julie, Social Engineer)

Similarly, another security tester commented,

> Usually those which improve your chances of success are whether you are likable … and if that person believes you belong to their tribe, because you have built rapport and likability it's much easier … for them to do things for you or to chat to you more. (Claire, Social Engineer)

In contrast the positive side, the negative side was described by security testers as using negative emotional triggers such as fear and intimidation to persuade end users. For example, one security tester commented,

> I would say fear ranges from anxiety to terror … it's such a strong physiological trigger, you know, people have a physiological reaction to fear … you will do what I tell you or I will hurt your family is a very effective persuasion technique. You don't need to be a diplomat or a politician to work out that most people will respond to that. (Julie, Social Engineer)

Besides using fear and intimidation, security testers described regularly using empathy to trigger a negative emotional response from end users, which would then cause them to behave in an insecure way. For example, one security tester commented,

> Say that you're the new kid … being the new kid sucks because everyone's asking you to do everything all at once, and you don't know who to talk to … you don't even know where to go. (Naomi, Chief Social Engineer)

Similarly, another security tester commented,

> You go in and say, 'Sorry I am having the worst morning ever; the truth is, I'm running late because my kid spilt all over my papers for my interview, and now I'm left without it and I'm not sure what to do, and how to figure this whole motherhood thing out in combination with a job'. And that way … it creates that emotional pressure because you will feel bad if you cannot help … And it's a situation you will understand if you are a parent. (Claire, Social Engineer)

We can understand from the above comments that the use of various emotional triggers was also described by security testers as a very effective way to increase their chances that end users either divulged certain information or allowed them to enter into an organisation.

In the context of guardianship of information, this again shows the potential and important contributions security testers and security testing may have towards unearthing the many ways in which malicious threat actors may use social engineering tactics to bypass human defences in organisations, which may help organisations improve their defences against such attacks.

7.11 Breaking down the crime event: Performing a social engineering test

As discussed in chapter three, the primary purpose of the crime script approach is to identify the key stages of an attack sequence and the goals and objectives of each stage to better understand how an offender might perform such an attack in the real-world. Further, the crime script approach advocates the use of the universal crime script, which offers a standardised set of stages which can be used to map the commission of any crime. Therefore, this next section presents the experiences of security testers of the different stages of performing a social engineering test, which are mapped onto to the universal crime-script.

7.11.1 Preparation stage: Establishing scope

The first stage in the universal crime-script is that of the *preparation stage*, where offenders undertake any preparatory actions prior to actual engagement in the crime event.

Security testers referred to the first stage of performing a social engineering test as *establishing scope*. The main goal of this stage was to meet with the organisation to determine the ‘ins and outs’ of performing the social engineering test, such as when it will take place, the types of tactics that security testers may use, the potential targets of their attack, and the time-frame within which the testing had to take place. As one security tester commented,

> You need the company to define scope: what is it you’re allowed to do, what you can’t do … those kinds of things. So, scope works towards what the company wants done and how they want it done. (Colin, Chief Social Engineer)

Security testers also stressed that scope must be properly established. For instance, if the scope of the social engineering test was too big there may be too much for security testers to investigate and/or security testers may waste time investigating areas of little significance to the organisation in terms of security. Alternatively, if the scope was too small then certain important areas might not be within range of their attacks, which would leave those areas exposed. As one security tester commented,

> Scope is one of the most important things to get right, too narrow and the test is pointless, too large and the client won't get value for money. (Stanley, Social Engineer)

Further, security testers described how they would try to improve the value of social engineering tests by aligning scope to the specific risks associated with or that had already been identified by the organisation they were testing. For example, one security tester commented,

> When it comes to the scope, you don’t necessarily test everything … some companies might just let you lose to go find some vulnerabilities but for some it might become very targeted, where they want you to test certain things … and it all depends on their risk matrix. So, if they have … a high-risk scenario then we would go for that first. (Claire, Social Engineer)

We can understand from the above comments that the first stage of performing a social engineering test was described by security testers as establishing scope, where the main goal was to determine the boundaries within which the social engineering test took place. Further, striking the right balance for scope was considered very important to ensure an organisation got the most value from the social engineering test.

7.11.2 Pre-condition stage: Reconnaissance

The second stage in the universal crime script is the *pre-condition stage*, which involves preliminary investigation towards the conditions which would facilitate the commission of a given crime.

Security testers generally referred to the second stage of performing a social engineering test as *reconnaissance.* Security testers described reconnaissance as an extensive and preliminary search for information about a target organisation and all the end users who worked for the organisation. For example, one security tester commented,

> What I do, my process, I do a lot of reconnaissance prior to doing anything. I want to know everything about that company that is on the internet, or at least is possible for me to get. (Naomi, Chief Social Engineer)

Similarly, another security tester commented,

> I’d look at the business, the industry – it’s like a funnel – the macro environment, the company within that environment, the actual

> department, the function, the person, and then that whole team. (Julie, social engineer)

We can understand here some key similarities and differences between a penetration test and a social engineering test. Both were described by security testers as trying to map out an organisation's network. However, the former involved mapping an organisation's *technical* network while the latter focused on the *social* or *human* network of an organisation.

Interestingly, when performing reconnaissance, security testers described two main ways to perform this; remotely and directly. To perform remote reconnaissance, security testers described primarily using the internet to gather intelligence about the target organisation and end users, such as the organisation's webpage, personal webpages, social media profiles, and/or blogs to help them better understand the various likes/dislikes and daily work and leisure routines of end users. As one security tester commented,

> A lot of it involves looking at social media … who they are, what their age is, what their background is, their interests, who their friends are … where they prefer to eat lunch, who they eat with, those sorts of things. (Wesley, Social Engineer)

To perform direct reconnaissance, security testers described visiting the organisation in-person to directly gather intelligence, such as the normal working hours of the organisation, the dress-code and any variations this might have during the week (e.g., casual Friday); the security protocols for entering and exiting the building; and whether there were any 'gatekeepers' (e.g., a security guard or receptionist). As one security tester commented,

> You sit for a day or two or even a week, it depends on the size of the office or the work building, to see the workflow of the employees, to see the way they dress, when they have their lunch breaks, when the office is empty, all these sorts of things … where is the best entrance

> to go to, when are the guards the most sleepy or bored, these things matter. (Claire, Social Engineer)

We can understand from the above comments that the second stage of performing a social engineering test was described by security testers as performing reconnaissance, which primarily involved gathering as much intelligence about a target organisation and all the end users that worked for the organisation. Further, this could be achieved either remotely, through using various open source intelligence, or directly, through covertly visiting the physical premises of the target organisation.

7.11.3 Instrumental pre-condition and initiation stage: Target selection and establishing pretext

The third and fourth stages in the universal crime script are the *instrumental pre-condition* and *instrumental initiation stage*, which primarily refers to actions such as target selection and identification of the most effective way to commit a criminal attack.

Once security testers had successfully developed a profile of the target organisation, including detailed information about the end users who worked for the organisation, they then described performing *target selection*. The main goal of target selection was to select a suitable target (e.g., a specific end user) whom security testers considered would be most susceptible to a social engineering attack. For example, one security tester commented,

> I tend to pick the ones that either know very little, or you just kind of think, I could get away with it. So, if you look at someone's personal Facebook … and there's not one mention of anything technical, then you're going to go, 'Right, perfect, I've got someone here'. (Ryan, Chief Social Engineer)

Similarly, another security tester commented,

> You target people … like, I wouldn’t go to an IT buyer, I wouldn’t want somebody with commercial and technical skills. (Julie, Social Engineer)

Once security testers had selected the most suitable target, they described the next stage as deciding upon which pretext would be most effective and to prepare any necessary props and or tools which they may need to use during actual engagement. For example, one security tester commented,

> Then you pull the team together to see what we have … and you put it together, and depending on what the organisation wants tested … you try to figure out how you are going to get in. (Wesley, Social Engineer)

Similarly, another security tester commented,

> Once this is done you then develop your pretext and determine the best way in or to approach … The whole pretext you have created depends on the information you have collected, you cannot just figure out pretext on its own. That’s why the reconnaissance comes first, and then right after, based on that, you figure out the pretext. (Claire, Social Engineer)

We can understand from the above comments that the third and fourth stages of performing a social engineering test were described by security testers as target selection, where security testers would select the most suitable target based upon the information gathered from the previous stage, followed by the development of the pretext and preparation of props and tools to be used during the engagement with the chosen end user.

7.11.4 Instrumental actualisation and doing stages: Establishing relationship and exploiting relationship

The fifth and sixth stages of the universal crime script are *instrumental actualisation* and *doing stages*, which generally describe the main parts of executing a crime.

The next two stages of performing a social engineering test were referred to as *establishing a relationship* with the targeted end user and then *exploiting the relationship* to bypass security. The overall goal of the two stages was to establish a relationship with the targeted end user to enable exploitation, where the security tester would either extract information from the target or convince the target to allow them entry into the organisation. For example, one security tester commented,

> The next stage is to make contact and after we make contact we establish a relationship … and then we would exploit that vulnerability. (Julie, Social Engineer)

Similarly, another security tester commented,

> You go in and you act as natural as one can possibly act … building a rapport is very important especially if you have a positive pretext. And from that point you move on and generally you try to have as little contact with them as possible, just enough to enable you to gain entry to the room or to gain certain information from them. (Claire, Social Engineer)

Interestingly, security testers described the time-frame to develop and then exploit the relationship with an end user as varying from a quick conversation to many weeks or months of building up trust. For example, one security tester described a successful attack involving a quick conversation,

> You start talking to them, you talk about their kids, and of course if it's at night they're bored and lonely … and then next thing you know, 'Hey, I forgot something on my desk and my desk's inside; can I get in really quick and just grab something off my desk?' (Naomi, Chief Social Engineer)

In contrast to this, another security tester described how making contact can possibly take place over several days or even weeks. She commented,

> If you're looking at someone's pattern, if they go to the same coffee shop, I'd be looking to go to that coffee shop once or twice a week …

> and I would literally build it up slowly, until in the end, I might 'bump into them' and … it would be so familiar that their guard's down already. (Julie, Social Engineer)

We can understand from the above comments that the next two stages of performing a social engineering test described by security testers involved making contact with the selected end user, in order to first establish a relationship with them, which was then followed by exploitation of that relationship (which, as discussed previously, may be aided by the use of pretext or emotional triggers) to bypass security.

7.11.5 Exiting scene

The next stage in the universal crime script is the *exiting scene* stage, which refers to actions taken immediately following the execution of the crime.

The sixth stage of performing a social engineering test was generally referred to by security testers as *exiting scene*. The main goal of exiting scene was to leave the location of the attack (i.e., the targeted organisation). Security testers generally described exiting scene as when the security tester(s) had decided that they have achieved their goal and must now exit the vicinity. As one security tester commented,

> Once you have exploited the trust … At that point where the person has done so many things for you or you were able to gather information on different things, then you can leave. And at that point you are confident enough that they will not find you out. (Claire, Social Engineer)

Importantly, security testers described continuing with the chosen pretext to avoid arousing any immediate or later suspicions about their interactions with end users. As one security tester commented,

> It's easy once you've got what you need … to cut your losses and run. But you don't want to do that, you want to stick to the pretext, you want to keep the act going, and see things out, so that they don't realise something is wrong. (Wesley, Social Engineer)

Once security testers had successfully exited the scene, they described this as finishing the actual ‘attack phase’ of the social engineering test, and they moved onto the final stage.

7.11.6 Post-conditions: Reporting back

The final stage in the universal crime script is the actions which follow the completion of a crime.

Following the completion of the social engineering test, security testers described having to produce a detailed report for the client organisation. This was described as having a similar format to penetration testing reports. As one security tester commented,

> I do have a report format that does mirror our penetration testing reporting … so keeping that vocabulary pretty much the same.
> (Naomi, Chief Social Engineer)

Therefore, security testers described the reports for social engineers testing as including a summary of the key points about the attack, along with specific details relating to the type of attacks security testers performed, the targets that were selected and how intelligence was gathered for them, and a detailed description of the communications between end users and security testers, and then any recommendations to help improve the level of security for the organisation. For example, one security tester commented,

> A full write up of all the reconnaissance we gathered, how one thing led to another … what their vulnerabilities are and how we exploited them, but also this is what you can do to fix those. (Wesley, Social Engineer)

Similarly, another security tester commented,

> In this report … you need to describe the steps you took … I did that on that time, on that day, with that person, this was their response, this is what I said, fully describing what went on. You shouldn’t hide

> anything. At then at the end of the report, usually what we do is, we provide recommendations on what could be done better, what could have gone really wrong, and what were their weaknesses and how to move on from that point. (Claire, Social Engineer)

We can understand from the above comments that the final stage of performing a social engineering test was reporting back to the organisation about the test. The goal of this stage was to inform the organisation about how security testers were successfully able to gain unauthorised access to information or to gain entry into an organisation, including all actions leading up to that point, and then to inform the organisation on how to prevent such actions taking place in the real-world.

Again, this shows the potential value that social engineering testing can have for organisations as not only does social engineering testing identify and exploit various human vulnerabilities, which may help to demonstrate to organisations the likelihood and impact this would have for them in the real-world, but it may also help organisations to understand how best to fix human vulnerabilities, which ultimately may have improve the overall levels of protection of information in those organisations.

7.12 Summary of social engineering testing findings

Overall, the findings from interviews with security testers about their experiences of performing social engineering testing showed that social engineering testing was described as the simulating of real-world attacks against organisations, where the purpose of social engineering tests were to help organisations identify various human vulnerabilities in security and to recommend ways to prevent social engineering attacks in the real-world.

While having an important role for improving protection of information in organisations, social engineering testing was not described by security testers as providing concrete assurance that organisations was secure against all types of social engineering attacks due to certain limitations within social engineering testing and security testers. Further, security testers described four main types of social engineering attacks: phishing, smishing, vishing, and impersonation attacks.

Regarding the various actors and tools used during social engineering testing, security testers described using two persuasion techniques. First, security testers utilised various pretexts to make end users believe they were authorised to communicate with them or to allow access to physical premises. Second, security testers described using various emotional triggers to increase their chances of successfully bypassing human defences.

Lastly, social engineering testing involved numerous stages which were suitably mapped onto the universal crime script. The main stages described by security testers were: (1) *establishing scope*, which comprised establishing the parameters within which the social engineering test must take place; (2) *reconnaissance*, which comprised remotely and/or directly gathering intelligence about a target organisation and its end users; (3-4) *target selection* and *establishing pretext*, which comprised selecting a suitable target based upon the intelligence gathered from the previous stage, and then developing a suitable pretext and preparation of props; (5-6) *establishing relationship* and *exploiting relationship*, which comprised the establishing of a relationship with the targeted end user to build a level of trust, followed by the exploitation of that trust to allow security testers to either gain information or to gain access to an organisation; (7) *exiting scene*, which involved leaving the scene of the attack; and (8) *reporting back,* which comprised the writing of reports which outlined the processes and actions of each stage followed by recommended actions and measures that an organisation can take to prevent social engineering attacks in the real world.

8 Discussion

8.1 Introduction

This chapter will provide a comprehensive discussion of the major findings of this study. The contributions of research that this study has made will be presented and discussed in the following sections and sub-sections.

To become more effective and efficient both public and private organisations are increasing their utilisation of information and information systems. However, by doing so, organisations have simultaneously become more vulnerable to various kinds of attacks from cybercriminals; a major consequence of which are security breaches. Further, despite previous studies showing that a major cause for security breaches is the insecure behaviour of end users, information security if often viewed as a technical problem only, where research into how socio-organisational factors influence security behaviour in organisations is currently lacking. Therefore, the present study sought to contribute towards addressing the problem of insecure behaviour of end users by conducting a phenomenology-inspired investigation into the socio-organisational factors that influence both the managing of information security and the security behaviour of end users.

To assist investigation, the present study developed and expanded the concept of guardianship, originally developed as part of the Routine Activity Approach in criminology. Previous studies have generally only considered the dimension of *availability* when exploring the concept of guardianship. However, the concept of effective guardianship was argued in this study to also comprise the *willingness* of guardians to perform protective actions and the *capability* of guardians to perform protective actions. Further, the present study broke new grounds by applying the concept of effective guardianship to information security management in organisations, where dimensions of effective guardianship of information were argued to be potentially influenced by numerous socio-organisational factors, such as organisational responsibility towards protecting information, the social pressures towards performing protective actions, the various risks and rewards connected to performing protective actions, and the moral aspects of protecting information; which were in turn connected to various aspects of information security management.

The findings that emerged showed the willingness of end users towards protecting information in organisations was influenced by: (1) positive and negative demonstrations from upper management towards behaving securely, (2) the effectiveness of security policies to communicate both the expectations of upper management and the organisational responsibilities of end users towards protecting information, (3) the effectiveness of SETA programmes to improve end users' understanding towards the What and the Why aspects of information security, (4) monitoring and enforcement practices which emphasised the risks to end users for failing to protect information, (5) the moral beliefs tied to protecting information, and (6) the rewards given by organisations for performing protective actions.

Emergent findings also showed the capability of end users towards protecting information was influenced by: (1) the effectiveness of SETA programmes to improve the knowledge and experience of end users of performing protective actions, and (2) the usability of technical security controls, which influenced the effort and time required to perform protective actions.

Lastly, the findings showed that the effectiveness of security managers towards managing the security behaviour of end users was also influenced by the level of upper management support for information security, as they determined the amount of organisational resources available for managing information security.

In addition to investigating how socio-organisational factors influenced security behaviour in organisations, this study also sought to investigate how various socio-organisational factors influenced the practice of security testing, namely, network-based and physical-based penetration testing – which simulate real-world attacks against organisations and are performed by security testers. The purpose of investigating security testing was to help improve our understanding of how cybercriminals may attack organisations in real-world settings, which may provide security managers valuable insight towards developing and implementing more effective security controls to manage the security behaviour of end users.

To assist investigation, the present study adopted the crime script approach, developed as part of the Rational Choice Perspective in criminology. It was argued the crime script approach may prove suitable for investigating security testing as the crime script approach aims to describe every stage of the crime-commission process (including the goals and objectives for each stage), and the required actors and tools for effective action during each of these stages; which can then be used to help develop more effective crime prevention measures.

The findings showed that network-based and physical-based penetration testing identified, exploited, and fixed vulnerabilities in organisational information security. Further, the findings showed that both network-based and physical-based penetration testing comprised numerous stages, which could be mapped using the universal crime script; where the goals and objectives for each stage, as well the required use of tools and tactics used by different actors, were successfully identified for each stage.

The remainder of this chapter further discusses the major findings of this study in relation to previous research in information security management to highlight both research contributions and how the present study answered the research question.

8.2 Upper management support in information security management

Findings from interviews with security managers and end users showed that upper management support was described as an important socio-organisational factor in information security management. Upper management support was described as primarily influencing the protection of information in organisations in two ways. Major findings relating to both will now be discussed.

8.2.1 Influencing the security behaviour of end users

Findings from interviews with security managers and end users showed that the perceived expectations and observed behaviour of upper management were described as important factors towards influencing the willingness of end users towards protecting information.

Such findings are significant because they empirically support the argument of Sampson et al (2010) that the willingness of guardians to perform protective actions may be influenced by the behaviour of super guardians; as previously, Sampson et al (2010) only proposed super guardians may influence the behaviour of guardians but offering no empirical evidence to support their argument.

They also support previous studies which have argued the perceived expectations and observed behaviour of upper management can positively influence security behaviour in organisations (Bulgurcu et al, 2010; Hu et al, 2012; Pahnila et al, 2007; Puhakainen and Siponen, 2010; Siponen et al, 2014) and contest those who have argued upper management do not have an influence on security behaviour in organisations (Herath and Rao, 2009a).

Therefore, the present findings support the inclusion of upper management as an important factor towards influencing end user security behaviour in organisations alongside that of peers, immediate supervisors, and security managers.

In addition, the findings from interviews with security managers and end users showed that end users primarily developed their understanding of the expectations of upper management through certain security controls. Both security policies and SETA programmes were described by security managers and end users as an effective way to communicate the expectations of upper management to end users, which empirically substantiate those recommendations of security practitioners that security policies and SETA programmes should be endorsed by upper management to improve their effectiveness (Hone and Eloff, 2002; Kajava et al, 2006). This is an important finding because previously, such recommendations by security practitioners were not supported empirically.

The above findings are also important because previous studies have highlighted a lack of investigation surrounding how end users develop their understanding of the expectations of upper management and/or how upper management can support the efforts of security managers when managing end user security behaviour (Hu et al, 2012). Thus, findings relating to how end users develop their understanding of the expectations of upper management offer new and important insight into how to positively influence end user security behaviour in organisations.

Lastly, findings from interviews with security managers and end users showed that the behaviour of upper management was described as potentially having a negative influence on end user security behaviour. This is a new and significant finding as most previous research into the security behaviour of upper management has focused on the positive influence upper management can have on end user security behaviour rather than the negative impact (Bulgurcu et al, 2010; Hu et al, 2012; Pahnila et al, 2007). Thus, while the present study suggests that the security behaviour of upper management may positively influence the security behaviour of end users, poor security behaviour from upper management may also reduce the level of protection of information by signalling to end users that information security is not important, which then reduces the likelihood that end users will behave securely.

Overall, the findings of this study not only extend our understanding towards upper management support as an important socio-organisational factor in information security management, but also extends our understanding of how upper management can effectively communicate their expectations to end users that protecting information is important, which in turn may lead to improvements of security behaviour in organisations.

In practice, this translates to upper management ensuring they are leading-by-example, and are fully cognisant of how their own security behaviour will shape and determine those security actions performed by other members of the organisation, in particular end users. Further, they must be seen to endorse those recommendations made by security managers, and where possible take part in information security initiatives such as those tied to SETA programmes.

8.2.2 Influencing the security behaviour of security managers

In addition to influencing the security behaviour of end users, the findings from interviews with security managers showed that upper management support was described as an important socio-organisational factor in information security management because they influenced the amount of organisational resources made available to security managers to develop and implement security controls. Moreover, the findings suggested that many security managers may not be receiving adequate security funding, which is in line with previous studies which show security managers often lack the required funding for managing information security (Gaunt, 2000; Johnson and Goetz, 2007; Kankanhalli et al, 2003; Knapp et al, 2006a).

In practice, if security managers are not provided with enough security funding, this may greatly influence their capability towards developing and implementing effective security controls in organisations, which ultimately may influence the level of guardianship of information. Therefore, as a practical consideration, organisations must ensure that upper management are fully supporting the efforts of security managers and ensuring they are properly equipped to deal with the problem of managing end user security behaviour.

Importantly, findings from interviews with security managers and end users showed there were numerous factors potentially influencing whether upper management provided their support, whether this related to providing a security budget to security managers or promoting the protection of information to end users.

The findings showed that upper management were described by security managers and end users as having a reactive rather than proactive approach towards information security. Previous studies have made similar characterisations, where upper management tend to provide support for information security only after some form of security incident, such as a security breach (Johnson and Goetz, 2007; Ashenden, 2008).

However, in addition, a new and significant finding was the reactive approach of upper management was described by security managers as influenced by their lack of understanding surrounding the various security risks to organisations, where upper management believed security breaches to be an unlikely occurrence. Further, security managers tried to improve the lack of understanding of upper management through delivering SETA programmes which were tailored specifically for them. This suggests that in practice, a useful way to counteract upper management's lack of understanding of security risks may be through purposefully developing and implementing SETA programmes for upper management alongside those for end users.

The perceived costs of developing and implementing security controls were also found to be an inhibiting factor surrounding upper management support, where upper management were described by security managers as often considering the costs of developing security controls as too high (whether technical or non-technical). Furthermore, the perceived high costs of developing and implementing security controls were exacerbated by competing needs within organisations, where security managers described security needs as often having to compete with other areas of the organisation. Such findings are generally line with previous studies which show a similar lack of support for information security due to concerns about the expensive nature of developing and implementing security controls (Gaunt, 2000; Kajava et al, 2006; Kankanhalli et al, 2003; Knapp et al, 2006a).

Another significant finding was security managers described upper management as viewing information security as a technical problem rather than a business problem, where upper management were described as less likely to want to invest in non-technical security controls and/or to take part in promoting information security if they felt it primarily involved technical aspects. This has been a major problem in information security management for decades now; where upper management often fail to acknowledge the need for input and support for information security programmes, where they are often ‘delegated or downgraded’ to technical departments and conveniently forgotten about (von Solms and von Solms, 2004b; Willison and Backhouse, 2006). The findings of this study therefore suggest that the problem of viewing information security as a technical problem to be dealt with solely by security managers may continue to be a major hurdle for some organisations.

Lastly, the above problems with upper management support were shown to be influenced by poor communications between security managers and upper management, where the language used by some security managers was described as too technical for upper management to understand. Previous studies have shown how poor communications can often cause a lack of understanding surrounding information security which may then lead to a lack of support from upper management (Ashenden, 2008; Werlinger, 2009). For example, Ashenden (2008) argued there exists a ‘communications gap’ between upper management and security managers because the language used by security managers tends to be highly technical. Consequently, upper management fail to engage.

Importantly, because the present findings showed that upper management were described as responding better to the negative impacts of security breaches, in practice, it may serve well for security managers to focus their communications around the potential negative impacts of security breaches when attempting to persuade upper management of the importance of improving the levels of protection of information.

Indeed, a useful way for security managers to achieve this may be to have security testing performed in organisations. For example, the findings from interviews with security testers showed that the purpose of security testing was to demonstrate the levels of vulnerability of information to cybercriminals and the real-world impacts of security breaches to organisations. This suggests that security testing may be a useful way for security managers to demonstrate to upper management the negative impacts of failing to protect information, which may then help towards improving the levels of support from upper management. Security testing was also described by security testers as providing useful recommendations on how to prevent such attacks taking place in the real-world, which might also help to persuade upper management of the need to develop and implement non-technical security controls.

Overall, the findings of this study relating to upper management support not only extend our understanding towards upper management support as an important socio-organisational factor in information security management, due to their influence upon both the ability of security managers to develop and implement security controls and the willingness of end users towards protecting information, but also extends our understanding of the reasons why upper management might fail to provide their support, and the ways in which security managers can try to rectify this.

8.3 The influence of information security policies on end user willingness

Findings from interviews with security managers and end users showed that security policies were described as an important socio-organisational factor towards managing the security behaviour of end users. These findings are in line with previous studies which have argued security policies are an essential security control for managing security behaviour in organisations (Doherty et al, 2009; Flowerday and Tuyikeze, 2016; Kirlappos et al, 2013; Safa et al, 2015; Soomro et al 2016).

In addition, findings from interviews with security managers and end users suggested that the primary mechanism through which security policies influenced the security behaviour of end users was by communicating an organisational responsibility to protect information, which in turn influenced end user willingness to act as guardians for information. The significance of such findings are twofold. First, these findings provide empirical support for the argument originally made by Felson (1995) – that the willingness of guardians may be influenced by their sense of responsibility – as this argument was not empirically supported by Felson; and second, such findings provide new insight into how the factor of responsibility can apply in the context of information security management, where organisational security policies can be used to improve the level of willingness of end users towards protecting information.

Unfortunately, findings also showed that while security policies were described as an effective security control towards managing end user security behaviour, there were numerous problems described by security managers and end users relating to development and implementation, which reduced the overall effectiveness of security policies in practice.

8.3.1 The problems of development and implementation

Findings from interviews with security managers and end users showed that the digestibility of security policies was described as a major problem in some organisations, which may reduce the level of influence of security policies upon the willingness of end users.

The poor digestibility of security policies was described by security managers and end users as influenced by several factors, including too much irrelevant information, an overuse of technical language, and the long length of security policies, which all made end users less likely to read through and understand them. Such findings again are in line with those recommendations outlined in previous studies (Doherty et al, 2009; Goel et al, 2010). Again, it should be highlighted that while these findings are supportive of recommendations laid out in previous work, many of these were not empirically supported, rather they were the recommendations of security practitioners (Hone and Eloff, 2002a; Wood, 1997).

Another important finding was that security managers described some organisations as copying and pasting the security policies of other organisations, which further influenced the level of digestibility of security policies for end users. Importantly, this was described as sometimes caused by a lack of organisational resources made available to security managers for developing security policies, which connects to the above findings surrounding upper management support and security funding.

Previous studies have highlighted the dangers of copying and pasting security policies, where the resulting security policies will not provide proper direction when managing information security within the contexts of the organisations they are implemented, which may then reduce the level of protection of information, and which ultimately may increase the chances that those organisations experience security breaches (Flowerday and Tuyikeze, 2016).

In addition to poor digestibility, findings from interviews with security managers and end users showed that the feasibility of security policies was also a major problem for some organisations. This suggests that a major challenge for organisations when managing information security may be developing security policies which are feasible for end users, where end users subsequently may decide not to comply with security policies because it is practical to do so, which is line with previous studies which showed similar results (Beautement et al, 2008; Kirlappos et al, 2013; Renaud, 2012).

The findings of the present study are significant because they suggest that the mere existence of security policies will not guarantee that end users will behave securely and that organisations are adequately protecting their information from cybercriminals. Further, the findings surrounding the problems of digestibility and feasibility of security policies suggest that the issue of end users behaving insecurely and non-complying with security policies may be due to factors of digestibility and feasibility of security policies rather than factors directly relating to end users. Therefore, the presence of additional security controls may not be an effective way to resolve the situation for organisations.

For example, monitoring end user security behaviour and punishing end users for non-compliance may not lead to improved compliance as this does little to improve end user understanding of poorly written security policies and/or does little to amend problematic situations caused by unworkable security policies, unless security policies themselves are reworked and improved.

Therefore, in practice, to become more effective at managing security behaviour, organisations and security managers should strive to make security policies as digestible and as feasible for end users as possible. By doing so, security policies may become more influential towards improving their security behaviour. A useful way for organisations to achieve this may be to conduct focus groups and/or interviews with end users to allow them to provide their input. Lastly, all the good work that goes into developing security policies may be undone if organisations do not properly communicate security policies to end users. Therefore, organisations must ensure that all end users who are to comply with security policies are regularly told about the existence of security policies and understand the importance of reading them. Further, such communications can be assisted by upper management to underline their importance.

With regards to improving the digestibility and feasibility of security policies, a significant finding from interviews with security managers was that including end users during policy development processes may help organisations to determine whether a security policy is digestible and/or feasible for end users. Previous studies have also argued such an approach might prove useful when developing security policies (Flowerday and Tuyikeze, 2016; Renaud, 2012). Thus, the present study suggests that end users should be made aware that security policies can be challenged and that end users should have access to policy development teams to make sure both security managers and end users are working together to improve the effectiveness of security policies.

Lastly, findings from interviews with security managers and end users showed that many organisations were described as not effectively communicating security policies. This is crucially important because it again suggests that insecure behaviours such as non-compliance with security policies may be caused by organisational failings, where end users are simply not aware of their need to perform certain security actions and that their behaviours are not in accordance with security policies. This is supported by previous studies that have found many organisations fail to properly communicate security policies to end users, which in turn may cause insecure behaviour (Fulford and Doherty, 2003; Chan and Mubarek, 2012).

Overall, the findings relating to the influence of security policies on end user willingness, and problems relating to the development and implementation of security policies, are significant because previous studies have called into question whether security policies are an effective security control for managing the security behaviour of end users (Doherty and Fulford, 2005). The findings from this study provide numerous important insights towards answering this timely question and suggest that, in practice, the situation is not that security policies are ineffective at managing end user security behaviour, instead problems relating to the development and implementation of security policies may be negatively influencing the overall effectiveness of security policies.

8.4 The influence of security education, training, and awareness programmes on end user willingness and capability

Findings from interviews with security managers and end users showed that the development and implementation of SETA programmes was an important socio-organisational factor when managing information security in organisations. This is in line with previous studies which have argued SETA programmes are an essential security control toward making sure end users are aware of various security threats to organisations and are able to perform their job roles effectively and securely (Alshaikh et al, 2018; Abawajy, 2014; Alzamil, 2012; Chan and Mubarek, 2012; Bada et al, 2015).

Findings from interviews with security managers showed that SETA programmes were generally described as comprising three learning levels of security education, security training, and security awareness; although the learning levels of security awareness and security education were closely related. Further, the terms relating to each learning level were often used interchangeably, however most cases of using terms interchangeably were between security awareness and security education; which may be explained by the fact they both related to similar aspects of SETA programmes.

The problem of using such terms interchangeably has been discussed elsewhere in the literature (Amankwa, 2014; Tsohou et al, 2008). However, a new and significant finding from interviews with security managers was that an effective way to overcome such confusion surrounding each security concept, was to understand information security management via the What, the Why, and the How aspects of protecting information in organisations.

Therefore, in practice, it may prove useful for organisations to develop and implement SETA programmes based upon these different aspects of information security management; where security awareness and education materials focuses on delivering the What and the Why aspects of protecting information, which may help to improve the willingness of end users towards protecting information; while security training materials focuses on delivering the How aspects of protecting information, which may help to improve the capability of end users to perform various security actions which keep information safe.

8.4.1 The problem of quantity of SETA programmes

Although the findings showed that SETA programmes may prove an effective way to improve both the willingness and capability of end users towards protecting information, they also showed that both security managers and end users described major issues with the amount of SETA programmes being delivered in organisations, where many end users may not be receiving SETA programmes, whether computer-based training or face-to-face training.

These findings are important because while previous studies have criticised the levels of security awareness of end users and the amount of security actions they perform (e.g., Albrechtsen, 2007; Chan and Mubarek, 2012), the present findings suggest that a potential cause of this is a lack of SETA programmes being delivered to end users. This is supported by previous studies which show the lack of SETA programmes provided to end users was a major cause of the absence of information security awareness in organisations (Alzamil et al, 2012).

Thus, in practice, the findings of this study highlight the importance of organisations making sure SETA programmes are being provided to end users, otherwise any benefits that may come from SETA programmes towards improving their security behaviour (such as understanding the What, Why, and How aspects of protecting information) will arguably be non-existent, where end users may become less willing and/or capable towards protecting information in organisations. More importantly, this should be understood as an organisational failing rather than the individual failing of end users, as they have little control over this.

Possible explanations for why organisations may not provide SETA programmes comes from a survey by Hagan et al (2008) who found that only half of the surveyed organisations had trained and/or educated end users on information security. Hagen et al argued organisations may not provide SETA programmes due to concerns surrounding the resource intensiveness of SETA programmes; that SETA programmes must be regularly delivered to be effective; and the completion of SETA programmes distracts end users from performing normal work duties. This connects back to the findings discussed earlier about a lack of understanding and support from upper management towards developing and implementing non-technical security controls and problems relating to the perceived high costs of managing information security. Which further suggests that many organisations may view information security as inhibiting rather than enabling organisations, where time spent on security training and security awareness/education would be better spent elsewhere.

In addition to findings which showed an overall lack of SETA programmes being delivered, were findings showing computer-based training was more commonly used than face-to-face training. Interviews with security managers and end users showed that computer-based training was described as a more popular delivery method in organisations. Further, security managers described two reasons for this, the first being computer-based training being cheap and easy to implement in organisations.

Previous studies have shown that computer-based training provides organisations with the ability to train large numbers of end users to an organisation-wide standard (Abawayjy, 2014) and by enabling end users to study independently and remotely, computer-based training can effectively reduce travelling and accommodation costs that may be incurred for attending off-site information security courses. Further, computer-based training is very cost-effective, following initial setup costs there is minimal maintenance required (Furnell et al, 2002; 2003; Wilson and Hash, 2003).

The second reason described by security managers for common usage of computer-based training was because organisations can demonstrate compliance with various legal and/or regulatory requirements. Again, previous studies have argued computer-based training tends to be the favoured option in many organisations because it allows them to effectively demonstrate to various legal and/or regulatory bodies that they as an organisation have fulfilled various compliance requirements (Alkasihk et al, 2018);

Importantly, while in practice there may be certain advantages to using computer-based training (such as reaching large numbers of end users) and certain basic forms of security training and/or education may be better suited to computer-based training, the findings of this study suggest that due to the variations in end user learning preferences and the higher levels of engagement that can be achieved with face-to-face training, organisations may yield improved levels of secure behaviour by adopting a mixed method approach.

8.4.2 The problem of quality of SETA programmes

Findings from interviews with security managers and end users showed that the quality of SETA programmes was described as a major problem in many organisations, both relating to computer-based training and face-to-face training.

A new and significant finding relating to SETA programmes was the concept of engagement of end users, and how this varied depending on both the delivery method chosen and the development and implementation practices adopted by security managers. For example, findings showed that despite computer-based training being the most common delivery method, it was not described as an effective way to train, educate, and/or raise the awareness of end users about information security. The main problem with computer-based training was security managers and end users described it as unengaging. Further, this was described as influenced by several factors, such as the content of computer-based training focused mainly on compliance with the Data

Protection Act, which meant it wasn't always relevant to end user job roles. Also, the content of computer-based training was described as the same every year and end users often had little time to complete computer-based training. Therefore, many end users described skipping ahead to complete computer-based training.

Previous studies have shown that because computer-based training must be targeted to large numbers of end users it must be generalised (Abawayjy, 2014; Furnell et al, 2002; 2003). Importantly, this lack of tailoring may have reduced the overall effectiveness towards improving the security behaviour of end users as they considered it monotonous, which may then have caused end users to complete security training sessions with minimal time and effort (i.e., skipping ahead). This also connects back to the ad-hoc approach described by Alkasihk et al (2018).

Regarding face-to-face training, findings from interviews with security managers and end users showed that although face-to-face training was generally considered a more effective delivery method for SETA programmes – due to potentially higher levels of engagement for end users – the effectiveness of face-to-face training programmes was nevertheless influenced by numerous development and implementation factors.

For instance, findings showed that engagement of face-to-face training was influenced by the level of tailoring of training materials to end user job roles. This provides much needed empirical support for those security practitioners who have argued end users generally pay more attention during face-to-face training sessions if they feel that training materials are developed specifically for them (Desman, 2003; Peltier, 2005; Wilson and Hash, 2003).

In addition, interviews with security managers and end users showed that the levels of engagement of face-to-face training programmes was described as influenced by the levels of interaction between security managers and end users, where interaction enabled end users to ask questions directly and to discuss amongst themselves various aspects of protecting information in relation to their everyday job roles. These findings are in line with previous studies which show improvements toward the effectiveness of SETA programmes can be achieved by increasing the levels of interaction between those delivering training sessions and those attending (Albrechsten, 2007; Albrechtsen and Hovden, 2010).

Findings from interviews with security managers and end users also suggested that engagement can be improved by including end users in the decision-making processes surrounding SETA programmes. The notion of inclusion generally referred to organisations receiving feedback or input from end users about the quantity and quality of SETA programmes. Importantly, while such evaluation and feedback mechanisms have previously been argued to be critical components of SETA programmes, they remained largely without empirical support. Therefore, the present findings again provide much needed empirical support for those recommendations of security practitioners relating to the value of providing feedback channels for end users.

Importantly, despite findings which showed that face-to-face training may be more engaging for end users than computer-based training, findings also showed that in practice face-to-face training programmes were often found to have low levels of engagement, caused again by training materials focusing more on being compliant with the Data Protection Act, rather than developing end user knowledge and understanding towards general information security concepts and issues.

In addition, interviews with security managers and end users showed that face-to-face training sessions were generally described as lacking any tailoring to the different job roles and learning levels of end users, which meant some end users found face-to-face training either irrelevant or too basic. Face-to-face training sessions were also described as lacking interaction. Thus, the overall findings of this study suggest that some organisations are favouring a one-size-fits-all approach when developing and implementing face-to-face training programmes. Such findings are important because many security practitioners have criticised the approaches taken by many organisations when developing and implementing SETA programmes (e.g., Valentine, 2006; Stewart and Lacey, 2012). Therefore, the present findings empirically support such arguments made by security practitioners.

In addition, these findings are significant because previous studies have argued, much like for security policies, that SETA programmes may not be an effective way to improve security behaviour in organisations, due to the continuing low levels of end user security awareness and the lack of secure behaviour of end users in organisations. However, the findings of this study suggest that the effectiveness of SETA programmes to improve security behaviour may be influenced by numerous factors relating to development and implementation. Which corroborates the argument made by Manke and Winkler (2012) that SETA programmes are not an inherently flawed security control, rather the development and implementation of SETA programmes in organisations vary greatly in both quantity and quality. Hence, the lack of improvements in end user security awareness or the continuation of a lack of security actions being performed by end users following SETA programmes may not be due SETA programmes being inherently ineffective, but may be due to the poor development and implementation of SETA programmes in organisations.

Therefore, in practice, organisations may benefit from trying to improve the overall levels of engagement of end users, which in turn may be achieved by, first, incorporating the What, the Why, and the How aspects of protecting information into the training materials. Second, training materials should be as tailored as possible to the job roles of end users and the actions they must perform. Third, if possible, training materials should incorporate aspects of improving security behaviour outside of work, so that end users receive additional benefits from attending and completing SETA programmes**.** Fourth, organisations and security managers should try to make SETA programmes as interactive as possible, involving both group discussions with end users themselves and direct communication with security managers. Fifth and last, organisations should strive to receive regular feedback from end users about SETA programmes, as this will help organisations stay on top of and address any issues end users have with SETA programmes.

8.5 The influence of monitoring and enforcement practices on end user willingness

There were numerous new and important findings relating to the monitoring and enforcement practices of organisations and their influence on end user willingness. Thus, the major findings are split into two sections discussing first, the use of punishment-based approaches, and second, possible alternatives to using punishments to improve security behaviour.

8.5.1 The punishment-based approach

Findings from interviews with security managers and end users showed that monitoring and enforcement practices were described as an important socio-organisational factor in information security management, where security managers and end users both described possible improvements in security behaviour of end users due to a fear of being monitored and subsequently punished for non-compliance. However, in practice there were numerous challenges described by security managers which influenced the overall effectiveness of monitoring and enforcement practices.

First, findings showed that security managers described the costs of monitoring practices as very high and many organisations were described as not monitoring security behaviour as a result, which would then reduce the effectiveness of monitoring and enforcement practices at improving end user compliance. This is a new and significant finding as a previous study by Vroom and von Solms (2004) argued there may be numerous practical obstacles which come into play when attempting to monitor and enforce security behaviour, such as the large amounts of organisational resources and manpower required for this to be effective. However, due to their being no studies which have empirically investigated monitoring and enforcement practices, this remained largely speculative. The present study therefore substantiates such concerns surrounding a lack of monitoring of end user security behaviour in organisations.

Second, findings showed that security managers described the legitimate use of monitoring and enforcement as dependent upon the existence of effective supporting security controls such as security policies and SETA programmes. Concern towards the legitimate use of monitoring and enforcement practices has been raised elsewhere by Lowery (2002). Lowery argued monitoring and enforcement of end user security behaviour should not take place until end users have been properly made aware of the existence of security policies with which they must comply and are sufficiently trained/educated on information security. Again, of note, this argument was not empirically supported. Hence, the present study substantiates this argument.

Next, findings showed that security managers described many organisations as failing to consistently enforce security behaviour. Previously, security practitioners have argued the monitoring and enforcement of security policies must be consistent, which means the equal application to all members of an organisation, including upper management (David, 2002; Wood, 1997). Therefore, the present study provides much needed empirical evidence to support this. This is an important finding because if an organisation does not consistently enforce security behaviour, then security policies may be considered unimportant by end users, which will potentially reduce their effectiveness in managing information security. Indeed, the findings suggest that monitoring and enforcement practices may prove counterproductive if the necessary supporting security controls are not in place and if certain members of organisations are perceived to be receiving favourable treatment compared to end users.

Lastly, a new finding was that security mangers described the overuse of punishment as potentially increasing the likelihood that end users would fail to report security incidents. This is an important finding and suggests that too much emphasis on punishment may create problematic situations for organisations as end users may try to cover up security incidents which may have potentially serious consequences.

Thus, overall, the major findings relating to monitoring and enforcement practices which emphasise the use of punishments suggest that this may not always be the best approach for managing security behaviour in organisations due to several practical challenges. Such findings are significant because a major outcome of previous studies in information security management has been the endorsement of monitoring and enforcement practices and the use of punishment to improve end user security behaviour. While the findings of this study somewhat support this argument, by showing a fear of monitoring and punishment for non-compliance may influence end user willingness, such benefits should be weighed against the numerous challenges that may be experienced by security managers when trying to implement such an approach and the potential costs this might have to an organisation's information security.

In practice, if organisations decide to use monitoring and enforcement practices as a means to manage the security behaviour of end users, then it is highly recommended they ensure security policies are properly communicated and that end users have properly understood them, and can realistically comply with them (which means they must be digestible and feasible); as well as making sure SETA programmes have been effectively developed and implemented in organisations to ensure that end users are fully capable towards performing those security actions outlined in security policies and that they are willing to do so. In addition, organisations must make sure that all organisational members are monitored and enforced and avoid differential treatment surrounding failure to adhere to security policies. This means that upper management must be treated with equal measure.

8.5.2 The possible alternatives to punishment-based approaches

Findings from interviews with security managers showed that the use of rewards may be a useful alternative to using punishments to manage security behaviour of end users or could be effectively used as part of a mixed method approach in organisations. This supports recent studies which have advocated the use of rewards to complement punishments-based approaches (Bulgrucu et al, 2010; Chen et al, 2012).

Therefore, in practice, it is recommended that organisations try to incorporate the use of rewards systems when managing end user security behaviour. This can be done in relation to the use of SETA programmes. While many organisations may not have the resources to implement complex reward systems, the findings of the present study suggest that even simple acknowledgement from security managers and/or upper management may prove to have a significant boost to the levels of willingness of end users to protect information.

Interestingly, the findings also showed that security managers incorporated aspects of gamification into reward systems to help improve the effectiveness of using rewards to incentivise end users to protect information. Previous studies have highlighted the potential benefits of using gamification in relation to information security. This may include the use of *point systems*, which provide measures to track the progress of end users; *badges* or *trophies*, which provide end users achievement tokens towards various security goals; and *leader boards*, which provide different rankings of end users (Gjertsen et al, 2017; Thornton, 2014). Again, this connects with previous findings relating to SETA programmes and highlights another potential way for organisations to improve the levels of engagement of SETA programmes for end users.

Importantly, while findings from interviews with security managers suggested that rewards systems and the concept of gamification may be useful for managing end user security behaviour, interviews with security managers and end users showed that the use of rewards was not described as common practice in organisations. Again, this highlights an area of managing security behaviour which organisations may be overlooking, where some organisations may not be achieving the highest levels of willingness and capability of end users as a result. Of course, this could potentially be explained by a lack of security funding or because organisations are adopting an ad-hoc approach to SETA programmes, where the focus is more towards ticking boxes than achieving high levels of engagement (as discussed above).

Lastly, the findings from interviews with end users showed that despite there being a lack of monitoring and enforcement of security behaviour, end users still described having a strong willingness to protect information due to experiencing a moral responsibility to protect information. This is especially interesting because many studies have argued that insecure behaviour is largely caused by a lack of fear of punishment. However, the present findings challenge this assumption towards end user security behaviour, where end users automatically behave insecurely if they do not perceive severe and certain punishments for non-compliance. This is because those end users interviewed described also considering the moral implications of their behaviour, which influenced whether they behaved securely. Thus, the findings of this study are consistent with more recent studies which have argued moral beliefs of end users often have an equal or more powerful influence on security behaviour than that of punishment or reward (D'Arcy and Devaraj, 2012; D'Arcy and Hovav, 2009; Li et al, 2014; Son, 2011; Workman and Cathegi, 2007). This means in practice organisations may benefit by highlighting to end users both their legal and moral responsibility towards protecting information alongside their organisational responsibility to protect information. This can be done via both security policies and SETA programmes.

8.6 The influence of usability of technical security controls on end user capability

Findings from interviews with end users showed that the usability of technical security controls was also described as an important socio-organisational important factor when managing information security in organisations. Findings showed that end users often described struggling to manage passwords during their everyday work routines due to having to remember numerous passwords for different systems and applications which also had to be regularly changed, as well as having to remember numerous non-work-related passwords, which often interfered with their ability to remember passwords during their work. Thus, many end users interviewed described behaving insecurely as a result, such as creating weak passwords and reusing weak passwords on multiple systems and applications.

The problems that end users may experience with managing passwords has been a major focus in usability research, where previous studies have shown end users regularly create and use weak passwords, write passwords down, and share their passwords, due to having to remember multiple passwords, use different passwords for different applications and systems, and/or change their passwords regularly (Adams and Sasse, 1999; Payne and Edwards, 2008).

A major cause of the password problem has been argued to be the inherent limitations of end users to remember such high numbers of secure passwords. For example, previous studies have argued the problem with end users remembering numerous complex passwords occurs because security requirements run contrary to the properties of human memory and overlook certain fundamental principles of what people are physically and mentally able to achieve. (Yan et al, 2004; Benenson et al, 2015)

Thus, the findings of this study suggest that organisations may need to improve the levels of support to end users with managing passwords, whether this is through encouraging end users to use passphrases or pass-algorithms (Payne and Edwards, 2008); by allowing the use of graphical passwords or biometrics (Faith and Garfinkel, 2004); or by implementing password managers, which store and enter end user passwords automatically (Stobert and Biddle, 2014).

In addition to findings relating to remembering passwords, findings showed that various processes and procedures surrounding the use of passwords were also described by end users as influencing their capability and willingness to protect information. Due to slow processes surrounding usernames and passwords end users described being more likely to create weak passwords and reuse them on multiple systems, as well as writing passwords down and sharing them, to ensure they were able to effectively and efficiently perform their primary job roles.

Therefore, in practice, organisations should try to ensure that the working practices of end users are taking into consideration when implementing various technical security controls and the processes and procedures surrounding them must also have attention paid towards the impact these controls may have upon end users daily work routines.

8.7 The importance of security testing in information security management

As mentioned in the previous chapter on the experiences of security testers, during interviews security testers generally referred to network-based penetration testing simply as penetration testing and physical-based penetration testing a social engineering testing. Therefore, such usage of the terms will continue here when discussing the major findings relating to security testing.

8.7.1 The nature of penetration and social engineering testing

Findings from interviews with security testers showed that both penetration testing and social engineering testing were generally described by security testers as simulating real world attacks against organisations to enable organisations to prevent and/or reduce the likelihood and impact of cybercriminal attacks in the real-world. Further, security testers described both penetration testing and social engineering testing as comprising three main elements: (1) identifying vulnerabilities, (2) exploiting vulnerabilities, and (3) fixing vulnerabilities. Further, penetration testing was described as primarily focusing on technical vulnerabilities while social engineering testing was described as primarily focusing on human vulnerabilities.

These findings are supported by previous studies that have argued the value of security testing derives from performing an authorised and controlled attempt to identify and exploit vulnerabilities to penetrate an organisation's security defences, to enable organisations to develop and implement appropriate security controls to eliminate those vulnerabilities before they are exploited in the real-world (Bertoglio and Zorzo, 2016; Bishop, 2007; Luo, 2011; Shah and Metre; 2015; Workman, 2008).

However, importantly, the findings showed that security testers described several limitations, where penetration testing and social engineering testing did not guarantee that an organisation was secure in the real-world. First, security testers described how security testing only provided a static image of the level of protection of information within an organisation, which may change over time following any changes to organisational functions or acquisition of new technology; second, security testers described security testing as only assessing an organisation's level of protection against the skillset of security tester(s) involved, which may be more or less advanced than real-world threat actors; and third, certain types of social engineering attacks may not be allowed during social engineering testing due to potential risks to individual targets.

These findings relating to the nature of penetration testing and social engineering testing are important because they highlight the potential contributions that penetration and social engineering testing can have toward improving the level of protection of information in organisations. The findings suggest that investigating penetration testing and social engineering testing may prove useful towards improving our understanding of how cybercriminals may operate when attacking organisations, which in turn may prove useful during the development and implementation of various security controls, as this will provide organisations and security managers invaluable insight into how attackers are likely to exploit certain vulnerabilities in information security, such as those caused by the security behaviour of security managers and end users. However, findings also suggest that while security testing may help us better understand real world attacks against organisations, there may still be certain 'blind spots' in our understanding relating to how certain attacks are conducted in the real world, due to certain inherent limitations of security testers and penetration testing and social engineering testing.

- The findings of this study suggest that organisations must try harder to help end users with managing secure passwords. Previous studies have shown that improvements can be made to end user password behaviour via the use of things like passphrases; pass-algorithms; graphical passwords; biometrics; and password managers. Therefore, it is recommended that organisations make efforts to implement such measures to help alleviate some of the difficulty of working with numerous passwords and/or numerous applications and systems.

8.7.2 The different types of penetration and social engineering testing

Findings showed that security testers described three main types of penetration tests, which were labelled black-box, white-box, and grey-box. Further, each were described as simulating the real-world location of the attacker in relation to the organisation. Breaking down penetration tests into different types of box tests is consistent with previous studies on security testing (Bertoglio and Zorzo, 2016; Bavisi, 2009).

Another interesting finding was the emerging concept of red teaming. Red teaming exercises were described by security testers as very different from standard types of penetration tests (i.e., black box or white box) because there were no rules surrounding the types of attacks security testers could perform against an organisation and security testers were required to conduct their attacks without being detected. This is an interesting finding as previous studies have tended to use the term red teaming as somewhat interchangeable with penetration testing (e.g., Brooks, 2008; Kraemer et al, 2004; Chowdappa et al, 2014). Yet, the present study suggests that red teaming, in practice, may refer specifically to a more advanced kind of penetration testing and so should be considered separate.

With regards to social engineering testing, security testers described breaking down social engineering tests into phishing, vishing, smishing, and impersonation attacks. Again, previous studies have similarly broken social engineering tests down into these attack vectors (Ivaturi and Janczewski, 2011).

The findings relating to different types of security testing are important because they highlight potential avenues for the use of the crime script approach. The Rational Choice Perspective states that when investigating crime, researchers should adopt a crime-specific approach because different crimes will serve different needs, and different situations will provide different opportunities for criminals to satisfy those needs (Cornish and Clarke, 2014; 2017). The findings relating to the different types of security testing therefore highlight the potential suitability of the crime script approach when investigating different types of security testing and how certain organisational settings may provide more or less opportunities for cybercriminals to successfully attack and steal information, which again may help security managers develop various opportunity-reducing techniques to try and reduce such opportunities being exploited in the real-world.

8.7.3 The tools and tactics used by security testers

During interviews, security testers described how penetration testing and social engineering testing would be performed by either an individual security tester or by a team of security testers.

Regarding penetration testing, this was described as being determined by the types of attacks conducted and the size of the organisation and kinds of technical infrastructure. For social engineering tests, security testers described how the overall effectiveness of using pretexting was influenced by the various factors relating to end users' expectations connected to various pretexts; which required security testers to then use various tools or props to make sure the pretext closely aligned with those expectations; and security testers also described how the use of team play would enable them to better perform certain pretexts or how having teams of security testers meant they were better enabled to align their chosen pretexts with the expectations of those targeted during their attacks.

These findings are particularly interesting as the Rational Choice Perspective states that criminal offenses will have various 'choice-structuring properties' attached to them (Cornish and Clarke, 1987; 1989), which will help criminals distinguish one criminal activity from another, such as the amount of effort or risk involved. These properties, in turn, will generate specific requirements in terms of who is suitable for performing that criminal offense. Thus, the present findings suggest that performing certain types of attacks against organisations will likewise have various choice structuring properties which determine who is potentially most suitable for an attack, or who is potentially the most suitable target, and how best to perform that attack.

In addition to findings relating to casting and prop requirements, interviews with security testers about penetration testing showed that although performing certain actions would place various constraints on which security tester could perform them (which connects to the choice structuring properties discussed above), security testers described technology (both hardware and software) as an important factor towards reducing the influence they would have on security testers because; (1) it drastically reduced the level of effort of performing certain tasks, and (2), it enabled security testers to multitask during the penetration test. This is important finding because RCP states a major determinant of committing crime is the required time and effort to perform certain criminal acts. Further, as explained above, certain attacks may place constraint upon how many people can commit a certain type of crime. However, the findings of the present study suggest that technology may be used to help reduce this or to overcome certain situational constraints.

Although, importantly, the findings also showed that while security testers described automated technology as providing two major advantages, they stressed that the use of automated technology did not necessarily mean that the security tester fully understood how to use such technology. Therefore, these findings further suggest that while automation may help perform certain tests, there will still be a requirement towards having certain levels of skill and ability; therefore, in practice, technology may not overcome all choice structuring properties connected to performing certain types of attack.

8.7.4 Performing Security tests

Interviews with security testers showed that both penetration testing and social engineering testing was performed in a sequential manner, where each test would comprise a number of different stages which had accompanying goals and objectives, which then determined the course of later actions. Such findings are consistent with RCP and the notion of event decisions, which refers to the decisions made by offenders prior to, during, and after the commission of a crime (Cornish and Clarke, 2014; 2017).

Overall, the findings are important because they help to improve our understanding of how attacks may be conducted against organisations and the organisational settings of their attacks. Previous studies have argued there is currently a lack of insight into the relationship between cybercriminals and the organisational settings of their attacks; where such insight would greatly assist security mangers in mitigating the risks to information (Willison, 2006).

8.8 Developing a cybersecurity Standard

In conjunction with the current research project, I have worked extensively with an organisation called *Polish Platform for Homeland Security* located in Poznan, Poland. My primary role within the organisation was to help a team of security experts develop a cybersecurity standard suitable for SMEs across Poland.

The cybersecurity standard comprises four main stages, namely asset management, risk management, security control selection, development and implementation, and security testing and auditing. Each stage is further broken down into essential steps in order to guide SMEs through each stage. For example, stage three, risk management, instructs SMEs how to perform risk identification, risk analysis, risk evaluation, and risk treatment.

Importantly, when developing the cybersecurity standard, many of the findings of this research project were incorporated into the development process, such as those relating to the development and implementation of security policies and SETA programmes (which shaped the development of stage four, security control selection, development and implementation). Thus, the major findings of this study have proven instrumental during the development of the cybersecurity standard.

While the development of the cybersecurity standard is still in its infancy, it fully demonstrates the direct applicability of the current findings and may prove an important avenue for future research to further support the current findings with regards their impact upon practice.

8.9 Summary

Chapter 8 has provided a critical discussion and synthesis of the findings with previous studies to answer the research question.

9 Conclusion

9.1 Introduction

This chapter summarises the main contributions to research, the theoretical implications of the study findings, the limitations of the present study, and recommendations for future research.

9.2 Contributions to research

This study significantly contributes to research in three main areas. First, this study significantly contributes towards our understanding of how socio-organisational factors influence information security management and the level of protection of information in organisations. The findings showed that the level of protection of information in organisations may be influenced by factors relating to upper management support; the effective development and implementation of security policies and SETA programmes; the proper use of monitoring and enforcement practices, including the use of rewards and consideration towards moral beliefs; and having usable technical security controls.

Second**,** this study significantly contributes towards improving our understanding of guardianship and makes significant advancements towards developing a 'guardianology'. The study empirically developed a conceptual framework for understanding guardianship as comprising two main dimensions, the willingness to perform protective actions and the capability to perform protective actions. Further, in the context of information security management, the study showed how both the willingness and capability of end users to protect information may be influenced by the various socio-organisational factors.

Third, this study is the first to use the crime script approach to understand how external attacks against organisations may be conducted by cybercriminals through investigating the practice of security testing. Therefore, this study both extends the reach of the crime script approach towards cybercrimes such as malicious hacking and social engineering and improves our understanding of how best to prevent and/or reduce the likelihood that organisations will become victimised by cybercriminals.

9.3 Theoretical Implications

There are numerous theoretical implications based upon the findings of this study, which are as follows:

- With regards to guardianship theory, this study incorporated and expanded the concept of guardianship. The findings showed how willingness and capability were important dimensions of guardianship, where both dimensions were required to ensure guardians actively engaged in protective actions. Further, this study broke new grounds by applying the concept of guardianship to the field of information security management and showed how each dimension of guardianship was influenced by various socio-organisational factors in information security management. Thus, the findings may be of interest to scholars connected to both the Routine Activity Approach and guardianship research.
- This study marks the first use of the crime script approach to understand how external threat actors might conduct their attacks against organisations. Therefore, the findings of this study may be of interest to those currently conducting research via the crime script approach. Further, while crime scripts have become more popular in recent years, there have been far less published use of crime scripts in the realm of cybercrime. Hence, this study supports the use of crime scripts when investigating various cybercrimes, such as malicious hacking and social engineering.
- Those working in the area of environmental criminology may also find the findings of this study particularly interesting due to their focusing on how various situational factors shape the decision-making during crime commission. A common critique of RCP is whether criminal offenses can/should be understood as a logical sequence of stages, where each stage is goal oriented, and whether research can properly unveil such aspects of criminal offenses.

This study therefore provides important insights into these aspects of offender behaviour and its routinised nature.

- The findings relating to upper management support may be of interest to those researchers who investigate the influence of upper management in information security management and/or social norms. Previous studies which have investigated how the concept of social norms influence security behaviour have generally not included the behaviour and expectations of upper management. Further, previous studies have argued we need to understand how upper management come to influence social norms. Thus, this study helps improve our understanding in this area by showing how upper management may shape social norms via their involvement in the development and implementation of various security controls and the promotion of information security to end users.
- The findings relating to digestibility and feasibility of security policies may prove interesting to those investigating security policies and how they influence security behaviour in organisations. Previous studies which have utilised Theory of Planned Behaviour when investigating security policies have tended to argue end users with negative attitudes towards information security or complying with security policies are less likely to demonstrate secure behaviour. However, a limitation with previous studies is they have not fully explored why end users might develop a negative attitude towards performing certain actions or complying with security policies. Therefore, the findings of this study may be of interest to TPB-based scholars due to insights into how security policies may influence security behaviour and how security policies can be properly developed and implemented to maximise their effectiveness. In other words, the concepts of digestibility and feasibility of security policies provide insight into the possible determinants of end users developing positive or negative attitudes towards performing certain actions or towards complying with security policies.
- The findings relating to SETA programmes and the importance of end user engagement, along with the various factors which influenced this, will be of interest to researchers which utilise either Protection Motivation Theory or

Theory of Planned Behaviour to investigate SETA programmes. Such studies have tended to describe end users as behaving insecurely due to low levels of threat or coping appraisal (in the case of PMT) or because end users have a negative attitude and/or low perceived behavioural control (in the case of TPB) towards performing certain security actions, and therefore often recommend that organisations provide SETA programmes to end users. While the findings of this study showed that SETA programmes can indeed influence such constructs of perceived threats/vulnerabilities/impacts in information security, the findings also highlighted that this is largely dependent upon various factors relating to how SETA programmes are developed and implemented in organisations. Therefore, whether SETA programmes succeed in improving security behaviour via impacting upon the various constructs connected to either PMT or TPB, may rest upon the effective development and implementation of SETA programmes.

- Findings relating to monitoring and enforcement practices have several important implications for theory. The present study suggests that end user compliance behaviour is a complex process involving numerous factors which may influence their decisions to behave insecurely. First, the findings of this study showed that monitoring and enforcement practices may have a desirable influence on security behaviour (which is generally supportive towards General Deterrence Theory-based studies). However, the findings also showed that monitoring and enforcement of security behaviour may not always be feasible due to major practical difficulties. Second, the findings showed that rewards may have a positive influence upon security behaviour of end users which adds new insights into the current debate surrounding the use of rewards to encourage end users to behave more securely. Third, the findings showed that moral beliefs of end users may also be very influential towards improving security behaviour, which supports morality-based studies and challenges the basic assumption of GDT-based studies that a lack of fear of punishment necessarily leads to non-compliance with security policies.
- With regards to findings relating to the usability of technical security controls, the present study adds to our understanding of why end users might behave

insecurely and how unusable technical security controls may be part of the reasons for this. While the findings aren't exactly novel in this area, they nevertheless may be of interest to usability researchers as they suggest the so-called 'password problem' continues to be a major stumbling block for many organisations.

9.4 Limitations

When conducting any piece of research there will always be some inherent limitations. The following are the major limitations connected to this study.

9.4.1 Theoretical limitations

While the present study adopted an induction approach to allow the emergence of unanticipated socio-organisational factors which influence information security management, there was a general focus towards those highlighted in previous studies, which were further viewed through the lens of guardianship. Thus, while there were numerous socio-organisational factors considered to influence security behaviour in organisations, other potential theories and concepts were excluded, which could have potentially explained certain aspects of how socio-organisational factors come into play when managing information security in organisations.

9.4.2 Methodological limitations

There were several methodological limitations with the present study. The first methodological limitation was trying to gain access for data collection. The original plan for this study was to perform an ethnographic study of security testing. The reason for this was it would allow the research to get as close as possible to the performing of either a penetration or social engineering test. However, it was not possible to perform this due to the security concerns of client organisations, where they considered the presence of the researcher to potentially undermine both the security test and the level of security surrounding information. Therefore, it was decided that performing in-depth interviews would be a suitable alternative.

The second methodological limitation is it is not possible to generalise from qualitative studies due to the low numbers of participants. Further, end users from organisations from different sectors may have different experiences given the differences between various legal/regulatory requirements attached to those sectors. Also, organisations of different sizes and who vary in terms of resources will also influence the managing of information security in those organisations and ultimately the experiences of end users, which again limits the ability to generalise from the findings. Therefore, attempts towards generalisation from the present study should be treated with caution.

The third methodological limitation is, the value of conducting qualitative research derives from the richness of the data and the ability of participants to provide truthful and comprehensive accounts of their experiences of the phenomenon under investigation. A limitation with this study was many end users did not have experiences with various aspects of information security management due to a lack of security policies, SETA programmes, and/or monitoring and enforcement practices within their respective organisations. Therefore, many end users were not able to provide 'rich description' *per* se, directly relating to these areas of information security management. Although they nevertheless were able to provide an in-depth understanding toward their own experiences of how such a lack of managing information security influenced their overall security behaviour in organisations.

Further, due to a lack of managing information security in some organisations, end users may have misunderstood various aspects relating to information security management which may then have influenced how they responded to various questions during interviewing. For example, when discussing security policies, some end users considered security policies to be equivalent to the Data Protection Act and so when describing their experiences of security policies, they may have been describing their experiences of reading the Data Protection Act.

The fourth methodological limitation was, although the presence of the researcher in this study proved useful towards filtering out and clarifying certain areas during interviews, there will still be certain biases of the interviewer which will feed into the analysis and presentations of findings. Of course, confirmation of the researchers understanding was exercised regularly during data analysis to try to reduce this as much as possible.

9.5 Future Research

Based upon the findings of this study there are numerous areas which may prove fertile grounds for future research.

Given the importance of upper management support and the possible problem of how to effectively communicate to them, future studies could look at the different ways in which security managers communicate with upper management when trying to secure their support. Further, studies could investigate whether the recommendations described in this study to improve upper management support are effective in practice.

A major finding of this study was the effectiveness of security policies may be reduced by the level of digestibility and feasibility of security policies. However, due to the limitations of this study (e.g., the low numbers of participants) these findings cannot be generalised to other organisations. Therefore, future studies could quantitatively investigate the influence of digestibility and feasibility towards the effectiveness of security policies, which would further support the argument that when properly developed and implemented, security policies are an effective security control; rather than being inherently useless at managing security behaviour.

The concept of engagement was shown to be a useful way to measure the level of influence of SETA programmes towards end user security behaviour. Again, due to the present study being qualitative – where the findings cannot be generalised – future studies may wish to quantitatively investigate the influence that end user engagement has on the overall effectiveness of SETA programmes. Further, having a focus towards the What, the Why, and the How aspects of information security and how they subsequently influence the level of end user engagement may also prove worthwhile.

A major finding relating to monitoring and enforcement practices was that many organisations may not be monitoring and enforcing security behaviour in organisations due to numerous practical issues. Therefore, future studies might want to investigate whether such practical issues are widespread and how they can potentially be managed in organisations.

The usability of technical security controls is now a well-established area of research, thus there aren't many recommendations to be made here. However, it may prove useful to investigate why some organisations are not providing end users with compensatory controls to help them manage passwords.

As mentioned above, the initial plan was to perform an ethnographic study of security testing to allow the researcher to 'get closer to the crime scene' during penetration and social engineering testing, but due to security concerns this was not possible. Thus, future studies may want to try and perform an ethnographic study where security testing is performed and mapped using the universal crime script, followed by the selection of suitable opportunity-reducing techniques, which can then be followed by the retesting of an organisation's information security (which can again be mapped using the crime script approach) to determine whether they have effectively eliminated or reduced the level of vulnerability of information. This would further support both the crime script approach as well as the theoretical basis of RCP and situational crime prevention.

10 References

Abawajy, J. (2014) ‘User preference of cyber security awareness delivery methods’, *Behaviour & Information Technology*, 33(3), pp. 236–247. doi.org/10.1080/0144929X.2012.708787

Adams, A. and Sasse, A. (1999) ‘Users Are Not the Enemy: Why users compromise computer security mechanisms and how to take remedial measures’, *Communications of the ACM*, 45(12), pp. 41-46

Ajzen, I. and Madden, T. (1986) ‘Prediction of Goal-Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control’, *Journal of Experimental Social Psychology*, 22, pp. 453-474

Albrechtsen, E. (2007) ‘A qualitative study of users’ view on information security’, *Computers and Security*, 26, pp. 276-289

Alshaikh, M., Maynard, S., Ahmad, A. and Chang, S. (2018) ‘An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations’, *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 5085-5094

Alzamil, Z. A. (2012) ‘Information Security Awareness at Saudi Arabians’ Organizations: An Information Technology Employee’s Perspective’, *International Journal of Information Security and Privacy*, 6(3), pp. 38-55

Amankwa, E., Loock, M. and Kritzinger, E. (2014) ‘A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions’, *The 9th International Conference for Internet Technology and Secured Transactions*, pp. 248-252

Arbas, C., Maloney-Krichmar, D. and Preece, J. (2004) ‘User-Centered Design. In Bainbridge, W. (ed) *Encyclopaedia of Human-Computer Interaction*. Thousand Oaks: Sage Publications.

Ashenden, D. (2008) ‘Information Security management: A human challenge?’, *Information Security Technical Report*, 13, pp. 195-201

Bada, M., Sasse, A. M. and Nurse, J. R. C. (2015) Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, *International Conference on Cyber Security for Sustainable Society 2015*, pp. 118-131

Balfanz, D., Durfee, G., Smetters, D. K. and Grinter, R. E. (2004) ‘In Search of Usable Security: Five Lessons from the Field’, *IEEE Security & Privacy*, 2(5), pp. 19-24

Baskerville, R. and Siponen, M. (2002) ‘An information security meta-policy for emergent organizations’, *Logistics Information Management*, 15(5/6), pp. 337-346

Bauer, A., Bernroider, E. W. N. and Chudzikowski, K. (2017) ‘Prevention is better than cure! Designing information security awareness programmes to overcome users’ non-compliance with information security policies in banks’, *Computers and Security*, 68, pp. 145-159. doi.org/10.1016/j.cose.2017.04.009

Beautement, A., Sasse, A. M. and Wonham, M. (2008) ‘The Compliance Budget: Managing Security Behaviour in Organisations’, *Proceedings of the 2008 New Security Paradigms Workshop*, pp. 47-58

Beebe, N. L. and Rao, V. S. (2010) ‘Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process’, *Communications of the Association for Information Systems*, 26(17), pp. 329-358

Beck, L. and Ajzen, I. (1991) ‘Predicting Dishonest Actions Using the Theory of Planned Behavior’, *Journal of Research in Personality*, (25), pp. 285-301

Berezina, K., Cobanoglu, C., Miller, B. L. and Kwansa, F. A. (2012) ‘The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth’, *International Journal of Contemporary Hospitality Management*, 24(7) pp. 991-1010

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009) ‘If someone is watching, I’ll do what I’m asked: mandatoriness, control, and information security’, *European Journal of Information Systems*, 18, pp. 151–164

Bryman, A. (2012) *Social Research Methods*. Oxford University Press: Oxford

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) ‘Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness’, *MIS Quarterly*, 34(3), pp. 523-548

Bunker, G. (2012) ‘Technology is not enough: Taking a holistic view for information assurance’, *Infomration Security Technical Report*, 17, pp. 19-25

Caldwell, T. (2014) ‘The true cost of being hacked’, *Computer Fraud and Security*, June, pp. 8-13

Chan, H. and Mubarek, S. (2012) ‘Significance of Information Security Awareness in the Higher Education Sector’, *International Journal of Computer Applications*, 60(10), pp. 23-31

Chang, S. E. and Ho, C. B. (2006) ‘Organizational factors to the effectiveness of implementing information security management’, *Industrial Management & Data Systems*, 106(3), pp. 345-361

Chang, S. E. and Lin, C. (2007) ‘Exploring organizational culture for information security management’, *Industrial Management & Data Systems*, 107(3), pp. 438-458

Cheng, L., Li, L., Li, W., Holm, E. and 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(B), pp. 447-459

Choi, N., Kim, D., Goo, J. and Whitmore, A. (2008) ‘Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action’, *Information Management & Computer Security*, 16(5), pp. 484-501

Clarke, R. V. (2017) ‘Situational Crime Prevention’, in Wortley, R. and Townsley, M. (ed.) *Environmental Criminology and Crime Analysis*. London: Routledge, pp. 286-303

Clarke, R. V. and Cornish, D. (1985) ‘Modeling Offenders' Decisions: A Framework for Research and Policy’, *Crime and Justice,* 6, pp. 147-185

Clarke, R. V. (2010) *Situational Crime Prevention: Successful Case Studies*. London: Lynne Reinner Publishers

Cleary, M., Horsfall, J. and Hayter, M. (2014) ‘Data collection and sampling in qualitative research: does size matter?’, *Journal of Advanced Nursing*, 70, pp. 473-475.

Cohen, L. E. and Felson, M. (1979) ‘Social Change and Crime Rate Trends: A Routine Activity Approach’, *American Sociological Review*, 44, p. 588-608

Cohen, L. E. and Felson, M. (1980) ‘Human Ecology and Crime: A Routine Activity Approach’, *Human Ecology*, 8(4), pp. 389-406

Cornish, D. and Clarke, R. V. (2014) *The Reasoning Criminal: Rational Choice Perspective on Offending*. London: Transaction Publishers

Cornish, D. and Clarke, R. V. (2017) ‘The Rational Choice Perspective’, in Wortley, R. and Townsley, M. (ed.) Environmental Criminology and Crime Analysis. London: Routledge, pp. 29-61

Cornish, D. (1994) ‘The Procedural Analysis of Offending and its Relevance for Situational Prevention’, In Clarke, R. V. (ed) *Crime Prevention Studies, Volume 3*, Monsey: Criminal Justice Press, pp. 151-196

Cornish, D. and Clarke, R. V. (1987) ‘Understanding Crime Displacement: An Application of Rational Choice Theory’, *Criminology*, 25(4), pp. 933-947

Cornish, D. and Clarke, R. V. (1989) ‘Crime Specialisation, Crime Displacement and Rational Choice Theory’, In Wegener, H., Losel, F. and Maisch, J. (ed) *Criminal behavior and the Justice System*. Berlin: Springer

Cox, J. (2012) ‘Information systems user security: A structured model of the knowing–doing gap’, *Computers in Human Behavior*, 28(5), pp. 1849-1858

Coyne, I. T. (1997) ‘Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries?’, *Journal of Advanced Nursing*, 26(3), pp. 623–630

Creswell (2007) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. London: Sage Publications

D’Arcy and 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), pp. 643–658

Darcy, J. and Devaraj, S. (2012) 'Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model', *Decision Sciences*, 43(6), pp. 1091-1124

Darcy, J., Hovav, A. and Galletta, D. (2008) 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach', *Information Systems Research*, 20(1), pp. 1-20

David, J. (2002) 'Policy enforcement in the workplace', *Computers and Security*, 21(6), pp. 506-513

Department for Digital, Culture, Media and Sport (2019) *Cyber Security Breaches Survey 2019: Statistical Release*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf (Accessed: 02 October 2019)

Desman, M. B. (2003) 'The Ten Commandments of Information Security Awareness Training', *Information Systems Security*, 11(6), pp. 39-44

Dhillon, G. and Backhouse, J. (2001) 'Information System Security Management in the New Millennium', *Communications of the ACM*, 43(7), pp. 125-128

DiCicco-Bloom, D. and Crabtree, B. F. (2006) 'The qualitative interview', *Medical Education*, 40, pp. 314–321

Dinev, T. and Hu, Q. (2007) 'The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies', *Journal for the Association of Information* Systems, 8(7), pp. 386-408

Dixon-Woods, M., Shaw, R. L., Agarwal, S. and Smith, J. A. (2004) 'The problem of appraising qualitative research, *BMJ Quality & Safety*, 13, pp. 223-225.

Dlamini, M.T. Dlamini, Eloff, J. H. P. and Eloff, M. M. (2009) ‘Information security: The moving target’, *Computers & Security*, 28(3-4), pp. 189-198

Doherty, N. F., Anastasakisa, L. and Fulford, H. (2009) ‘The information security policy unpacked: A critical study of the content of university policies’, *International Journal of Information Management,* 29(6), pp. 449-457

Doherty, N. F., Anastasakisa, L. and Fulford, H. (2011) ‘Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy’, *International Journal of Information Management*, 31(3), pp. 201-209

Doherty, N.F. & Fulford, H., (2005) ‘Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis’, *Information Resources Management Journal*, 18 (4), pp. 21-38

Dominguez, C. M. F., Ramaswamy, M., Martinez, E. M. and Cleal, M. G. (2010) ‘A Framework for Information Security Awareness Programmes’, *Issues in Information Systems*, 11(1), pp. 402-409

Eminagaoglu, M., Ucar, E. and Eren, S. (2009) ‘The positive outcomes of information security awareness training in companies – A case study’, *Information Security Technical Report*, 14(4), pp. 223-229

Cranor, L. F. and and Garfinkel, S. (2004) ‘Usable or Secure?’, *IEEE Security & Privacy*, pp. 16-18

Felson, M. (1995) ‘Those Who Discourage Crime’, In Eck, J. E. and Weisburd, D., (ed) *Crime and Place: Crime Prevention Studies. Vol. 4*, Monsey, NY: Criminal Justice Press. pp. 53-66

Felson (2006) *Crime and Nature*. Thousand Oaks, CA: Sage

Fidas, C. A., Voyiatzis, A. G. and Avouris, N. M. (2010) ‘When Security Meets Usability: A User-Centric Approach on a Crossroads Priority Problem’, *2010 14th Panhellenic Conference on Informatics*, pp. 112-117

Ajzen, I. and Fishbein, F. (1970) ‘The Prediction of Behavior from Attitudinal and Normative Variables’, *Journal of Experimental Social Psychology*, 6(4), pp. 466-487
Flechais, I., Sasse, M. A. and Hailes, S. M. V. (2004) ‘Bringing Security Home: A process for developing secure and usable systems’, *New Security Paradigms Workshop 2003*, pp. 49-57

Florencio, D. and Herley, C. (2007) ‘A Large-Scale Study of Web Password Habits’. *International World Wide Web Conference Committee (IW3C2)*, pp. 657-665

Flowerday, S. V. and Tuyikeze, T. (2016) ‘Information security policy development and implementation: The what, how and who’, *Computers & Security*, 61, pp. 169-183

Floyd, D. L., Prentice-Dunn, S. and Rogers, R. W. (2000) ‘A Meta-Analysis of Research on Protection Motivation Theory’, *Journal of Applied Social Psychology*, 30(2), pp. 407-429

Fulford, H. and Doherty, N. F. (2003) ‘The application of information security policies in large UK-based organizations: an exploratory investigation’, *Information Management & Computer Security*, 11(3), pp. 106-114

Furnell, S. (2005) ‘Why users cannot use security’, *Computers & Security*, 24(4), pp. 274-279

Furnell, S. and Clarke, N. (2012) ‘Power to the people? The evolving recognition of human aspects of security’, *Computers and Security*, 31(8), pp. 983-988

Furnell, S., Jusoh, A. and katsabas, D. (2006) ‘The challenges of understanding and using security: A survey of end-users’, *Computers and Security*, 25(1), pp. 27-35

Gartner Inc. (2018) ‘Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019’. Available at: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 (Accessed: 30 June 2019)

Gaunt, N. (2000) ‘Practical approaches to creating a security culture’, *International Journal of Medical Informatics*, 60(2), pp. 151-157

Goel, S. and Chengalur-Smith, I. N. (2010) ‘Metrics for characterizing the form of security policies’, *The Journal of Strategic Information Systems*, 19(4), pp. 281-295

Goo, J., Yim, M. S. and Kim, D. J. (2013) ‘A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate’, *Proceedings 2013 46th Hawaii International Conference on System Sciences*, pp. 2959-2968

Guba, E. G. and Lincoln, Y. S. (1994). ‘Competing paradigms in qualitative research’, In Denzin, N. K. and Lincoln, Y. S. (ed.) *Handbook of qualitative research*. Thousand Oaks, CA, US: Sage Publications, Inc. pp. 105-117

Haelterman, H. (2016) *Crime Script Analysis: Preventing Crimes Against Business*. London: Palgrave MacMillan

Hagen, J. E. and Albrechtsen, E. (2009) ‘Effects on employees' information security abilities by e-learning’, *Information Management & Computer Security*, 17(5), pp. 388-407, doi:10.1108/09685220911006687

Hansch, N. and Benenson, Z. (2014) ‘Specifying IT security awareness’, *25th International Workshop on Database and Expert Systems Applications*, pp. 326-330

Hansche, S. (2001a) ‘Designing a Security Awareness Programme: Part 1’, *Information Systems Security*, 9(6), pp. 1-9 DOI: 10.1201/1086/43298.9.6.20010102/30985.4

Hansche, S. (2001b) ‘Information System Security Training: Making it Happen, Part 2’, *Information Systems Security*, 10(3), pp. 1-20 DOI: 10.1201/1086/43316.10.3.20010701/31727.6

Hazari, S. William Hargrave, W. and Clenney, B. (2008) ‘An Empirical Investigation of Factors Influencing Information Security Behavior’, *Journal of Information Privacy and Security*, 4(4), pp. 3-20 DOI: 10.1080/2333696X.2008.10855849

Herath, T. and Rao, H. R. (2009a) ‘Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness’, *Decision Support Systems*, 47(2), pp. 154-165

Herath, T. and Rao, H. R. (2009b) ‘Protection motivation and deterrence: a framework for security policy compliance in organisations’, *European Journal of Information Systems*, 18(2), pp. 106–125

Herley, C. (2014) ‘More Is Not The Answer’, *IEEE Security & Privacy*, 12(1), pp. 14-19

Hollis-Peel, M. H., Reynald, D. M, Bavel, M., Elffers, H. and Welsh, B. C. (2011) ‘Guardianship for crime prevention: a critical review of the literature’, *Crime, Law and Social Change*, 56(1), pp. 53-57 doi.org/10.1007/s10611-011-9309-2

Holloway, I. and Wheeler, S. (2002) *Qualitative Research in Nursing* (2nd ed.) Oxford: Blackwell Publishing

Hone, K. and Eloff, J. H. P. (2002a) ‘Information security policy — what do international information security standards say?’, *Computers & Security*, 21(5), pp. 402-409

Hone, K. and Eloff, J. H. P. (2002b) ‘What Makes an Effective Information Security Policy’, *Network Security*, 6(1), pp. 14-16

Hong, K., Chi, Y. Chao, L. R. and Tang, J. (2006) ‘An empirical study of information security policy on information security elevation in Taiwan’, *Information Management & Computer Security*, 14(2), pp. 104-11 doi.org/10.1108/09685220610655861

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) ‘Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture’, *Decision Sciences*, 43(4), pp. 615-659

Ifinedo, P. (2012) ‘Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory’, *Computers & Security*, 31(1), pp. 83-95

Ifinedo, P. (2014) ‘Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition’, *Information & Management*, 51(1), pp. 69-79

Jacobs, B. A. (2010) ‘Deterrence and Deterrability’, *Criminology*, 48(2), pp. 417-441 https://doi.org/10.1111/j.1745-9125.2010.00191.x

J. Johnston, J., Eloff, J. H. P. and Labuschagne, L. (2003) ‘Security and human computer interfaces’, *Computers & Security*, 22(8), pp. 675-684

Kainda, R., Fléchais, I. and Roscoe, A. W. (2010) ‘Security and Usability: Analysis and Evaluation’, *2010 International Conference on Availability, Reliability and Security*, pp. 1-8

Kajava J., Anttila J., Varonen R., Savola, R. and Röning J. (2006) ‘Senior Executives Commitment to Information Security – from Motivation to Responsibility’. In Wang Y., Cheung Y., Liu H. (eds) *Computational Intelligence and Security*. *International Conference, CIS 2006*. Berlin, Heidelberg: Springer

Kankanhalli, A., Hock-Hai, T., Tan, B. C. Y. and Kwok-Kee, W. (2003) ‘An integrative study of information systems security effectiveness’, *International Journal of Information Management*, 23(2), pp. 139-154

Karlsson, F., Karin Hedström, K. and Goldkuhl, G. (2017) ‘Practice-based discourse analysis of information security policies’, *Computers & Security*, 67, pp. 267-279

Karyda et al, (2005) ‘Information systems security policies: a contextual perspective’, *Computers & Security*, 24(3), pp. 246-260

Katsikas, S. K. (2000) ‘Health care management and information systems security: awareness, training or education?’, *International Journal of Medical Informatics*, 60(2), pp. 129-135

Kayworth, T. and Whitten, D. (2012) ‘Effective Information Security Requires a Balance of Social and Technology Factors’, *MIS Quarterly Executive*, 9(3), pp. 163-175

Kruger, H. A. and Kearney, W. D. (2008) ‘Consensus ranking – An ICT security awareness case study’, *Computers & Security*, 27(7–8), pp. 254-259

Kilman, D. and Stamp, J. (2005) ‘Framework for SCADA security policy’, *Sandia National Laboratories report SAND2005-1002C*, pp. 1-6

Kirlappos, I. and Sasse, M. A. (2014) ‘What Usable Security Really Means: Trusting and Engaging Users’. In Tryfonas, T. and Askoxylakis, I. (eds) *Human Aspects of Information Security, Privacy, and Trust*. *HAS 2014*. Ney York: Springer

Kirlappos, I., Beautement, A., Sasse, M. A. (2013) ‘“Comply or die” is dead: Long live security-aware principal agents’. In Adams A. A., Brenner M., Smith M. (eds) *Financial Cryptography and Data Security*. Berlin: Springer

Knapp, K. J. and Ferrante, C. J. (2012) ‘Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations’, *Journal of Management Policy and Practice*, 13(5), pp. 66-80

Knapp, K. J., Marshall, T. E., Rainer, R. K. and Morrow, D. W. (2006) ‘The Top Information Security Issues Facing Organizations: What Can Government do to Help?’, *The EDP Audit, Control, and Security Newsletter*, 34(4), pp. 1-10, DOI: 10.1201/1079.07366981/46351.34.4.20061001/95104.1

Knapp, K. J., Morris, R. F., Marshall, T. E. and Byrd, T. A. (2009) ‘Information security policy: An organizational-level process model’, *Computers &* Security, 28(7), pp. 493-508

Leach, J. (2003) ‘Improving user security behaviour’, *Computers & Security*, 22(8), pp. 685-692

Leclerc, B. and Wortley, R. (2014) *Cognition and Crime: Offender Decision Making and Script Analyses*. London: Routledge

Leech, N. L. and Onwuegbuzie, A. J. (2011) ‘Beyond Constant Comparison Qualitative Data Analysis: Using NVivo’, *School Psychology Quarterly*, 26(1), pp. 70–84

Leung, L. (2015) ‘Validity, reliability, and generalizability in qualitative research’, *Research and Audit*, 4(3) pp. 324-327

Lincoln, Y. S. and Guba, E. G. (1985) *Naturalistic Inquiry*. London: Sage Publications

Lowery, C. (2002) ‘Developing Effective Security Policies’, *Dell Power solutions*, pp. 77-79 Available at http://www.craiglowery.com/publications/

Manke, S. and Winkler, I. (2012) ‘The Habits of Highly Successful Security Awareness Programmes: A Cross-Company Comparison’, Available at https://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf

Maqousi, Balikhina, T. and Mackay, M. (2013) ‘An Effective Method for Information Security Awareness Raising Initiatives’, *International Journal of Computer Science & Information Technology*, 5(2), pp. 63-72

Marshall, B., Cardon, P., Poddar A. and Fontenot, R. (2013) ‘Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in IS Research’, *Journal of Computer Information Systems*, 54(1), pp. 11-22, DOI:10.1080/08874417.2013.11645667

Martins, A. D. and Veiga, N. (2015) ‘Improving the information security culture through monitoring and implementation actions illustrated through a case study’, *Computer &* Security, 49, pp. 162-176

Merhi, M. I. and Ahluwalia, P. (2015) ‘Top Management Can Lower Resistance toward Information Security Compliance’, *Thirty Sixth International Conference on Information Systems, Fort Worth 2015*, pp. 1-11

Metalidoua, E., Marinagic, C., Trivellasc, P., Eberhagen, N., Skourlasd, C. and Giannakopoulos, G. (2014) ‘The Human Factor of Information Security:

Unintentional Damage Perspective', *Procedia - Social and Behavioral Sciences*, 147, pp. 424-428

Milne, S., Sheeran, P. and Orbell, S. (2000) 'Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory', *Journal of Applied Social Psychology*, 30(1), pp. 106-143

Miro, F. (2014) 'Routine Activity Theory', In Miller, J. M. (eds) *The Encyclopedia of Theoretical Criminology*, West Sussex: Blackwell Publishing https://doi.org/10.1002/9781118517390.wbetc198

Moustakas, C. (1994) *Phenomenological Research Methods*. London: SAGE Publications

Nurse, J. R. C., Creese, S., Goldsmith, M. and Lamberts, K. (2011) 'Guidelines for Usable Cybersecurity: Past and Present', *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, DOI: 10.1109/CSS.2011.6058566

Onwuegbuzie, A. J., and Leech, N. L. (2007) 'Sampling Designs in Qualitative Research: Making the Sampling Process More Public', *The Qualitative Report*, 12(2), pp. 238-254

Pahnila, S., Siponen, M. and Mahmood, A. (2007) 'Employees' Behavior towards IS Security Policy Compliance', *40th Annual Hawaii International Conference on System Sciences (HICSS'07)*

Payne, B. D. and Edwards, W. K. (2008) 'A Brief Introduction to Usable Security', *IEEE Internet Computing archive*, 12(3), pp. 13-21

Peltier, T. R. (2005) 'Implementing an Information Security Awareness Programme', *Information Systems Security*, 14(2), pp. 37-49, DOI: 10.1201/1086/45241.14.2.20050501/88292.6

Posey, C., Roberts, T. L., Lowry, P. B., Courtney, J. and Bennett, R. J. (2011) 'Motivating the Insider to Protect Organizational Information Assets: Evidence from Protection Motivation Theory and Rival Explanations', *Dewald Roode Workshop in Information Systems Security 2011*, pp. 1-51

Posey, C., Roberts, T. L., Lowry, P. B. and Hightower, R. T. (2014) 'Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders', *Information & Management*, 51(5), pp. 551-567

Puhakainen, P. and Siponen, M. (2010) 'Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study', *MIS Quarterly*, 34(4), pp. 757-778

Renaud, K. (2012) 'Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches?', *IEEE Security & Privacy*, 10(3), pp. 57-63

Renaud, K. and Flowerday, S. (2017) 'Contemplating human-centred security & privacy research: Suggesting future directions', *Journal of Information Security and Applications*, 34(1), pp. 76-81

Reynald, D. M. (2009) 'Guardianship in action: Developing a new tool for measurement', *Crime Prevention and Community Safety*, 11(1), pp. 1-20

Reynald, D. M. (2010) 'Guardians on Guardianship: Factors Affecting the Willingness to Supervise, the Ability to Detect Potential Offenders, and the Willingness to Intervene', *Journal of Research in Crime and Delinquency*, 47(3), pp. 358-390

Reyns, B. W., Henson, B. and Fisher, B. S. (2016). Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept From Routine

Activity Theory as It Applies to Online Forms of Victimization', *Journal of Contemporary Criminal Justice*, 32(2), pp. 148-168

Rezgui, Y. and Marks, A. (2008) 'Information security awareness in higher education: An exploratory study', *Computers & Security,* 27(7–8), pp. 241-253

Robinson, O. C. (2014) 'Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide', *Qualitative Research in Psychology*, 11(1), pp. 25-41, DOI: 10.1080/14780887.2013.801543

Ruoti, S. Andersen, J., Zappala, D. and Seamons, K. (2015) 'Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client', Available at arXiv:1510.08555

Safa, N. S., Sookhak, M., von Solms, R., Furnell, S. Ghani, N. A. and Herawan, T. (2015) 'Information security conscious care behaviour formation in organizations', *Computers & Security*, 53, pp. 65-78

Sampson, R., Ecl, J. E. and Dunham, J. (2010) 'Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure', *Security Journal*, 23(1), pp. 37-51

Sasse, M. A. and Flechias, I. (2005) 'Usable Security: Why Do We Need it? How Do We Get It?, in Cranor, L. F. and Garfinkel, S. (ed.) *Security and Usability: Designing Secure Systems That People Can Use*. Cambridge: O'Reilly

Saunders, M., Lewis, P. and Thornhill, A. (2007) *Research Methods for Business Students*. Essex: Pearson Education Limited

Schatz, D. and Bashroush, R. (2016) 'The impact of repeated data breach events on organisations' market value', *Information & Computer Security*, 24(1), pp.73-92, https://doi.org/10.1108/ICS-03-2014-0020

Shaw, R. S., Chen, C. C., Harris, A. L. Huang, H. (2009) 'The impact of information richness on information security awareness training effectiveness', *Computers &* Education, 52(1), pp. 92-100

Siponen, M. and Vance, A. (2010) 'Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations', *MIS Quarterly*, 34(3), pp. 487-502

Siponen, M., Pahnila S. and Mahmood, A. (2007) 'Employees' Adherence to Information Security Policies: An Empirical Study'. In Venter, H., Eloff, M., Labuschagne, L., Eloff J., and von Solms, R. (eds) *New Approaches for Security, Privacy and Trust in Complex Environments. SEC 2007. IFIP International Federation for Information Processing*, vol 232. Boston: Springer

Siponen, M., Mahmoodb, M. A. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information & Management*, 51(2), pp. 217-224

Son, J. (2011) 'Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies', *Information & Management*, 48(7), pp. 296-302

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management*, 36(2), pp. 215-225

Spanos, G. and Angelis, L. (2016) 'The impact of information security events to the stock market: A systematic literature review', *Computers & Security*, 58, pp. 216-229

Stahl, B. C., Doherty, N. F. and Shaw, M. (2012) ‘Information security policies in the UK healthcare sector: a critical evaluation’, *Information Systems Journal*, 22(1), pp. 77-94

Stewart, G. and Lacey, D. (2012) ‘Death by a thousand facts: Criticising the technocratic approach to information security awareness’, *Information Management & Computer Security*, 20(1), pp.29-38, https://doi.org/10.1108/09685221211219182

Stobert and Biddle (2014) ‘The Password Life Cycle: User Behaviour in Managing Passwords’, *Symposium on Usable Privacy and Security (SOUPS 2014) July 9-11, 2014*

Sutton, D. (2016) *Information Risk Management: A Practitioner’s Guide*. India: Viva

Thanh, N. C. and Thanh, T. T. L. (2015) ‘The Interconnection Between Interpretivist Paradigm and Qualitative Methods in Education’, *American Journal of Educational Science,* 1(2), pp. 24-27

Thomson, K. and von Solms, R. (2005) ‘Information security obedience: a definition’, *Computers & Security*, 24(1), pp. 69-75

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008) ‘Investigating Information Security Awareness: Research and Practice Gaps’, *Information Security Journal: A Global Perspective*, 17(5-6), pp. 207-227, DOI: 10.1080/19393550802492487

Turner, D. W. (2010). ‘Qualitative Interview Design: A Practical Guide for Novice Investigators’, *The Qualitative Report*, 15(3), pp. 754-760.

Valentine, (2006) ‘Enhancing the employee security awareness model’, *Computer Fraud & Security*, 2006(6), pp. 17-19

Vance, A. and Siponen, M. (2012) ‘IS Security Policy Violations: A Rational Choice Perspective’, *Journal of Organizational and End User Computing*, 24(1), pp. 21-41

Vance, A., Siponen, M. and Pahnila, S. (2012) ‘Motivating IS security compliance: Insights from Habit and Protection Motivation Theory’, *Information & Management*, 49(3–4), pp. 190-198

von Solms, R. and von Solms, B. (2004a) ‘From policies to culture’*, Computers & Security*, 23(4), pp. 275-279

von Solms, R. and von Solms, B. (2004b) ‘The 10 deadly sins of information security management’, *Computers & Security*, 23(5), pp. 371-376

von Solms, S. H. and von Solms, R. (2009) *Information Security Governance*. New York: Springer

Vroom, C. and von Solms, R. (2004) ‘Towards information security behavioural compliance’, *Computers & Security*, 23(3), pp. 191-198

Vroom, C. and von Solms R. (2002) ‘A Practical Approach to Information Security Awareness in the Organization’, in Ghonaimy, M. A., El-Hadidi, M. T. and Aslan, H. K. (eds) *Security in the Information Society. IFIP Advances in Information and Communication Technology, vol 86*, Boston: Springer

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) ‘An integrated view of human, organizational, and technological challenges of IT security management’, *Information Management & Computer Security,* 17(1), pp. 4-19

Whitten, A. and Tygar, J. D. (2005) ‘Why Johnny Can’t Encrypt’, in Cranor, L. F. and Garfinkel, S. (ed.) Security and Usability: Designing Secure Systems That People Can Use. Cambridge: O’Reilly

Willison, R. and Backhouse, J. (2006) ‘Opportunities for computer crime: considering systems risk from a criminological perspective’, *European Journal of Information Systems*, 15(4), pp. 403–414

Willison, R. (2006) ‘Understanding the perpetration of employee computer crime in the organisational context’, *Information and Organization*, 16(4), 2006, pp. 304-324

Wilson, M. and Hash, J. (2003) ‘Building an Information Technology Security Awareness and Training Programme’, Computer Security Division
Information Technology Laboratory, National Institute of Standards and Technology, Available at: https://www.nist.gov/publications/building-information-technology-security-awareness-and-training-programme (Accessed: 30th June 2019)

Wood, C. C. (1995) Writing InfoSec Policies, *Computers and Security*, 14(8), pp. 667-674

Wood, C. C. (1997) ‘Policies Alone Do Not Constitute a
Sufficient Awareness Effort’, *Computer Fraud & Security*, 1997(12), pp. 14-19

Yanus, R. and Shin, N. (2007) ‘Critical Success Factors for Managing an Information Security Awareness Programme’, *Technical Report Number 238,* Pace University, School of Computer Science and Information Systems

Yar, M. (2005) ‘The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory’, *European Journal of Criminology, 2*(4), pp. 407–427

Zhang, J., Reithel, B. J. and Li, H. (2009) ‘Impact of perceived technical protection on security behaviors’, *Information Management & Computer Security*, 17(4), pp.330-340, doi:10.1108/09685220910993980

11 Appendices

11.1 Appendix A: Information sheet (security managers)

UNIVERSITY of ABERTAY DUNDEE

School of Social and Health Sciences
University of Abertay Dundee
Bell Street
Dundee
DD1 1HG
Telephone + 44 (0) 1382 308700

PARTICIPANT INFORMATION SHEET

Project title: The socio-organisational factors which shape guardianship experience of information security management in organisations

What is the study about?

You are invited to participate in an interview in order to explore the managing of information security in organisations. In particular, the use of non-technical security controls such as security policies and security education, training, and awareness programmes.

Who is carrying out the study?

The study is being conducted by Jason Johnstone and will form the basis of a PhD at Abertay Dundee, under the primary supervision of Dr Stefano De Paoli.

What does the study involve?

The interview involves the following:

- The recording of conversation between the researcher and participant.
- The study should last roughly 60 minutes.

- Participants can expect to be asked questions about their personal experiences surrounding the managing of information security; questions *will not* be directed towards your current or previous employer.
- There will be no risk of harm coming to any of the participants.

Do I have to take part?

No. It is entirely up to you to decide whether or not to take part. If you decide to take part you will be given this information sheet to keep and be asked to sign a consent form to confirm that you understand what is involved when taking part in this study.

Can I withdraw from the study?

Yes. Being in this study is completely voluntary. You are not under any obligation to consent and if you do consent you can still withdraw at any time without affecting your relationship with the University of Abertay Dundee. Interviews may be stopped at any time if you do not wish to continue, the audio recording will be erased and the information provided will not be included in the study.

Will anyone else know the results?

All aspects of the study, including results, will be strictly confidential and anonymised, only the researcher will have access to information on participants. A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report.

What if I require further information about the study or my involvement in it?

When you have finished reading this information, Jason Johnstone will discuss it with you further and answer any questions you may have. If you would like to know more at any stage, feel free to contact Jason Johnstone on Telephone: 07984444040 or E-mail: [redacted].abertay.ac.uk

What if I have a complaint or any concerns?

Any concerns or complaints can be forwarded to the School of Social and Health sciences. *See above for contact details*.

11.2 Appendix B: Information sheet (end users)

UNIVERSITY of ABERTAY DUNDEE

School of Social and Health Sciences
University of Abertay Dundee
Bell Street
Dundee
DD1 1HG
Telephone + 44 (0) 1382 308700

PARTICIPANT INFORMATION SHEET

Project title: The socio-organisational factors which shape guardianship experience of information security management in organisations

What is the study about?

You are invited to participate in an interview in order to explore how certain non-technical factor influence the security behaviour of end users in organisations.

Who is carrying out the study?

The study is being conducted by Jason Johnstone and will form the basis of a PhD at Abertay Dundee, under the primary supervision of Dr Stefano De Paoli.

What does the study involve?

The interview involves the following:

- The recording of conversation between the researcher and participant.
- The study will last roughly 60 minutes.
- Participants can expect to be asked questions about their personal experiences surrounding the use and protection of information as part of their job role; questions *will not* be directed toward your current or previous employer.
- There will be no risk of harm coming to any of the participants.

Do I have to take part?

No. It is entirely up to you to decide whether or not to take part. If you decide to take part you will be given this information sheet to keep and be asked to sign a consent form to confirm that you understand what is involved when taking part in this study.

Can I withdraw from the study?

Yes. Being in this study is completely voluntary. You are not under any obligation to consent and if you do consent you can still withdraw at any time without affecting your relationship with the University of Abertay Dundee. Interviews may be stopped at any time if you do not wish to continue, the audio recording will be erased and the information provided will not be included in the study.

Will anyone else know the results?

All aspects of the study, including results, will be strictly confidential and anonymised, only the researcher will have access to information on participants. A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report.

What if I require further information about the study or my involvement in it?

When you have finished reading this information, Jason Johnstone will discuss it with you further and answer any questions you may have. If you would like to know more at any stage, feel free to contact Jason Johnstone on Telephone: 07984444040 or E-mail: [redacted]abertay.ac.uk

What if I have a complaint or any concerns?

Any concerns or complaints can be forwarded to the School of Social and Health sciences. *See above for contact details*.

11.3 Appendix C: Information sheet (security testers)

School of Social and Health Sciences
University of Abertay Dundee
Bell Street
Dundee
DD1 1HG
Telephone + 44 (0) 1382 308700

PARTICIPANT INFORMATION SHEET

Project title: The socio-organisational factors which shape guardianship experience of information security management in organisations

What is the study about?

You are invited to participate in a questionnaire in order to explore the practice of security testing in organisations.

Who is carrying out the study?

The study is being conducted by Jason Johnstone and will form the basis of a PhD at Abertay Dundee, under the primary supervision of Dr Stefano De Paoli.

What does the study involve?

The interview involves the following:

- The recording of conversation between the researcher and participant.
- The study will last roughly 60 minutes.
- Participants can expect to be asked questions about their personal experiences surrounding the practice of either network-based or physical-based penetration testing; questions *will not* be directed toward your current or previous employer.
- There will be no risk of harm coming to any of the participants.

Do I have to take part?

No. It is entirely up to you to decide whether or not to take part. If you decide to take part you will be given this information sheet to keep and be asked to sign a consent form to confirm that you understand what is involved when taking part in this study.

Can I withdraw from the study?

Yes. Being in this study is completely voluntary. You are not under any obligation to consent and if you do consent you can still withdraw at any time without affecting your relationship with the University of Abertay Dundee. Questionnaires may be stopped at any time if you do not wish to continue, all answers given will be erased and the information provided will not be included in the study.

Will anyone else know the results?

All aspects of the study, including results, will be strictly confidential and anonymised, only the researcher will have access to information on participants. A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report.

What if I require further information about the study or my involvement in it?

When you have finished reading this information, Jason Johnstone will discuss it with you further and answer any questions you may have. If you would like to know more at any stage, feel free to contact Jason Johnstone on Telephone: 07984444040 or E-mail: [redacted].abertay.ac.uk

What if I have a complaint or any concerns?

Any concerns or complaints can be forwarded to the School of Social and Health sciences. *See above for contact details*.

11.4 Appendix D: Participant Consent Form

School of Social and Health Sciences
University of Abertay Dundee
Bell Street
Dundee
DD1 1HG
Telephone + 44 (0) 1382 308700
PARTICIPANT CONSENT FORM

I, ...[PRINT NAME], give my consent to participate in the following research project:

Project Title: The socio-organisational factors which shape guardianship experience of information security management in organisations

In giving my consent I acknowledge that:

1. The procedures required for the project and the time involved have been explained to me, and any questions I have about the project have been answered to my satisfaction.

2. I have read the Participant Information Statement and have been given the opportunity to discuss the information and my involvement in the project with the researcher.

3. I understand that being in this study is completely voluntary – I am not under any obligation to consent.

4. I understand that my involvement is strictly confidential. I understand that any research data gathered from the results of the study may be published however no information about me will be used in any way that is identifiable.

5. I understand that I can withdraw from the study at any time, without affecting my relationship with the researcher or the University of Abertay Dundee now or in the future.

(By typing my name below, I am electronically signing this consent form)

....
Signature

....
Please PRINT name

....
Date

11.5 Appendix E: Interview Guide (Security Managers)

1. Can you describe your job role?
2. In your own words, what is information security?
    a. How does this differ from cybersecurity?
3. How important is information security in organisations?
    a. How supportive/involved are upper management towards information security?
4. What are the main threats in information security?
    a. External?
    b. Internal?
5. Can you describe how information security is managed within an organisation?
    a. Technological factors?
    b. Organisational factors?
    c. Role of end users?
6. Can you explain the role of risk management?
7. Can you describe the development and implementation of security policies in organisations?
    a. Can you describe the effectiveness of security policies?
    b. Why might end users demonstrate non-compliance with security policies?
8. Can you describe the development and implementation of SETA programmes in organisations?
    a. Can you describe the effectiveness of SETA programmes? Both computer-based and face-to-face?
9. Can you describe the monitoring and enforcement of security behaviour in organisations?
10. Can you describe the effectiveness of monitoring and enforcement towards managing security behaviour in organisations?
11. Is there anything you would like to add that we haven’t discussed?

11.6 Appendix F: Interview guide (end users)

1. Can you describe your job role?
2. What sorts of information do you handle?
3. What is your understanding of information security?
4. Why do you think information security might be important for organisations/individuals?
5. In your opinion, what might be the main threats to information security?
    a. External?
    b. Internal?
6. What is your experience of using technical security controls in your everyday work routine?
    a. Do you have to use encrypted devices, such as USBs? Encrypted emails?
    b. How might designers of technology enable users to be more secure?
7. How important is information security in your organisation?
8. How would you describe your level of awareness regarding information security policies?
    a. Does your organisation have a security policy which you must follow?
    b. How would you describe your experiences of information security policies?
    c. How would you describe your ability to manage security guidelines alongside normal work procedures?
9. What are your experiences regarding information security training?
    a. How is information security training delivered within your organisation?
    b. How regularly do you receive security training?
    c. How did this shape your understanding of the importance of information security?
10. What are your experiences of monitoring and enforcement practices in organisations?
11. Can you describe a situation where you, or a colleague, were confronted with either adhering to security policy or transgressing?
    a. What were your reasons for potentially transgressing?

    b. What was the outcome?
    c. How did this shape your overall perception regarding information security?
    d. Why might other employees not comply with security requirements?

12. How might employers improve the level of security compliance among their employees?

11.7 Appendix G: Interview schedule (penetration testers)

1. Can you describe your job role?
2. In your own words, what is penetration testing?
3. Why is it important for an organisation to have a penetration test?
    a. How does penetration-testing improve security beyond common IT security measures?
4. What are some of the common threats to organisations?
    a. External?
    b. Internal?
5. Are there different kinds of penetration tests?
    a. Advantages?
    b. Disadvantages?
6. Can you describe the process of doing a penetration test?
7. Do you work alone or in a team?
    a. Advantages?
    b. Disadvantages?
8. Can you describe for me the role of technology in carrying out a penetration test?
    a. What technologies might you use? (including both software/hardware)
    b. What about the technologies you are trying to penetrate? (including both software/hardware)
9. What are your views surrounding the general level of security within organisations prior to them having a penetration test?
10. Can you describe for me an example in which you were successful in identifying a vulnerability?
11. What was the root cause of the vulnerability? (i.e., technical/non-technical)
12. Can you describe for me the role of end users in security?
    a. How might they affect security?
13. How are the results generated from a penetration test presented to the client?

11.8 Appendix H: Interview schedule (social engineers)

1. Can you describe your job role?
2. In your own words, what is social engineering?
    a. How does social engineering relate to ‘hacking’?
3. Why is it important for an organisation to have a social engineering test?
4. What are some of the common threats to organisations?
    a. External?
    b. Internal?
5. Are there different kinds of tests? (advantages/disadvantages)
6. Can you describe the process of doing a social engineering test?
7. Do you work alone or in a team?
    a. Advantages?
    b. Disadvantages?
8. Can you describe for me the tools and tactics used during a social engineering test?
9. What are your views surrounding the general level of security within organisations prior to them having a social engineering test?
10. Can you describe for me an example in which you were successful in identifying a security vulnerability?
11. Can you describe for me the role of end users in security?
12. How are the results generated from a social engineering test presented to the client?