Risk Understanding is not enough: Identifying and leveraging emotional drivers of security behaviour via the 'Behavioural Security Grid'

Odette Nicole Beris

A THESIS SUBMITTED FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

AT

UNIVERSITY COLLEGE LONDON

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY COLLEGE LONDON

FEBRUARY 2017

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

ABSTRACT

In recent years, organisations have been exposed to unprecedented levels of security breaches leading to significant data losses in many cases. In order to mitigate the risks associated with these threats, standards such as ISO 27001 have been devised to ensure organisations have adequate risk management processes in place. Employee non-compliance render these measures ineffective. The results of this research suggest that focusing on improving employee perception of security risks in order to increase security compliance within organisations is not sufficient to improve security behaviour. Identifying and leveraging positive affective drivers may also be relevance in improving employee security compliance behaviour. The three case studies use a novel methodological approach referred to as the Behavioural Security Grid (BSG) to classify employee security behaviour in relation to four quadrants. The BSG is a revised version of the *Johari Window* originally developed by Luft and Ingham, using the dimensions of *Affective Security* and *Risk Understanding* to better understand security behaviour. The findings demonstrate that positive affective responses towards security coupled with positive understanding of security risks imply improved security behaviour. Case Study 1 compares two organisations Company A and B, where Company B demonstrated significantly positive levels of both *Affective Security* and *Risk Understanding*, indicating positive organisational security behaviours. Case Study 2, conducted within Organisation C, a Government department, suggests that *Positive Risk Understanding* is not sufficient to improve security compliance and that *Negative Affective Security* indicates dissatisfaction with

the security provision within the organisation and may signal possible circumvention. Case Study 3 conducted within Organisation D, across Government departments, suggests that employees demonstrating *Positive Risk Understanding* and *Positive Affective Security* imply improved levels of security compliance. The validation survey (Study 4) used as a method to triangulate the results for Case Study 3, supports the findings that Organisation D demonstrates a predominantly positive security culture. Overall, the findings indicate that creating cultures demonstrating *Positive Affective Security* as well as *Positive Risk Understanding* may be the missing link to increasing employee participation in improving organisational security behaviours.

IMPACT STATEMENT

The impact of this research is primarily focused on the development of new knowledge in relation to employee security behaviour within organisations. In particular, it highlights the importance of affect, as well as cyber risk understanding in the drive to improve employee security behaviour. This is of particular relevance to both security and organisational development practitioners as they can use these insights to shape employee security interventions such as security messages for instance. The results from the three case studies presented within this dissertation suggest harnessing positive attitudes, feelings and behavioural preferences towards security may be a driver in improving employee security behaviour.

It is useful for organisations to note however that this research concurred with other findings in the information security literature which indicate that *security hygiene* (Kirlappos and Sasse, 2014) needs to be in place, before affect can be leveraged in the drive to improve security culture.

The other major impact of this research is the adoption of a novel methodological approach referred to as the Behavioural Security Grid (BSG) (Beris et al., 2015) designed to assist organisations explore and diagnose employee security behaviour. The BSG, a framework developed from the revised Johari Window (Luft and Ingham, 1955) explores the interplay between affective attitudes, feelings and behavioural preferences towards security, operationalized as *Affective Security* (AS), and understanding of cyber risks, operationalized as *Risk Understanding* (RU). These two dimensions, *AS* and *RU*, form the axes of the BSG (Beris et al., 2015) to suggest four modes of security behaviour which imply different organisational interventions. Further research is required to develop this methodological approach.

ACKNOWLEDGEMENTS

This thesis would not have been completed without the help and support of others. I would like to thank M. Angela Sasse for generously sharing her knowledge and expertise as well as her helpful feedback on the draft. I would also like to thank members of the Information Security Research Group, in particular Adam Beautement and Anthony Morton for their insights and encouragement. Thanks also go to my sponsor for supporting this research and the partner organisations who generously agreed to participate.

A special thank you to Thelma Beris, Michele Barker and Graham Parker for all your support. Sincere thanks is also due to my husband Steve for being stalwart throughout.

This dissertation is dedicated to my late father Albert Beris, with gratitude.

CONTENTS

TABLES

FIGURES

CHAPTER 1: INTRODUCTION

1.1 General background: information security threat landscape

Organisations seek to maintain the confidentiality, integrity and authenticity of their information assets by using a variety of security policies and mechanisms to mitigate the risks (Sasse & Flechais, 2005). However, as the frequency of cyber security incidents within organisations ever increases, it is evident that those risks are difficult to manage effectively.

In a survey focused specifically on the UK commissioned by the Department for Business, Innovation and Skills (PwC, 2015), PwC report that 90% of large businesses and 74% of small businesses have experienced a security breach. In terms of quantifying the losses, the "*worst security breach*" of the year has cost an average of between £1.46m - £3.14m and £75k - £311k for large organisations and small businesses respectively. Clearly, the figures suggest that it is imperative for UK organisations to ensure their strategy encompasses the mitigation and management of cyber security risks.

1.2 Human Factors: The importance of security hygiene

In relation to the types of data breaches that occur in organisations, PwC reported that 75% of breaches in large organisations and 31% of breaches small businesses are staff-related (PwC, 2015). Figures also suggest that over 50% of the worst breaches are staff-related in that they have been attributed to "*inadvertent human error*", an increase of 31% since 2014 (PwC, 2015).

This high percentage of employee non-compliance *notionally* adds support to the idea that people are the "*weakest link*" (Schneier, 2004). Certainly the majority of literature on managing security behaviour has advocated a "*fix the human"* approach: the assumption is that if only people recognised the risks, they would follow the behaviour mandated by the policy, and, security would be assured. However, staff may breach security policy for many reasons. One reason for non-compliance is lack of *security hygiene*; the fact that staff may struggle to comply with security policy even if they actually want to (Kirlappos, Beautement, & Sasse, 2013). *Security hygiene* aligns security processes with employees' job roles enabling employees to work productively minimising onerous security requirements without breaking security rules (Kirlappos et al., 2013). When security tasks present themselves as a burden or obstacle to the user, it is perhaps unsurprising that they may choose to circumvent official security processes. In particular, Kirlappos et al., (2013) highlighted that the time and cognitive or physical effort that is required by security mechanisms can lead to circumvention of policy when employees are focused on completion of their primary task, not the secondary task of being secure.

Most security non-compliance is not necessarily a result of malicious intent or lack of risk awareness. Instead, it might be reframed as an employee's rational response to the sometimes onerous security requirements that are placed on them (Herley, 2009) when *security hygiene* is not observed (Kirlappos et al., 2013). In such cases, employees may engage in "*shadow security*" (Kirlappos, Parkin, & Sasse, 2014). Organisations that do not have an effective security policy in place or else require users to grapple with unusable security mechanisms that lead to circumvention and by extension, create new security risks. It is therefore incumbent on the organisation to ensure *security hygiene* is in place within the organisation, which aligns security mechanisms and processes with the employee's primary tasks, to encourage security compliance (Sasse, Brostoff, & Weirich, 2001). Thus, the first step in improving employee security compliance is addressing *security hygiene* issues in order to reduce the number of security breaches. What this means in practice for organisations is that employees not only need to be able to recognise security risks, but also be able to comply with security policy to manage those risks.

1.2.1 A participatory approach: Employees as principal agents

As discussed, organisations need to manage the human element to mitigate security risks, nevertheless how they achieve this aim is of relevance since the traditional approach "*command and control*" approach has not been wholly effective to date (Kirlappos et al., 2013). Indeed, this traditional discourse has been challenged by researchers who suggest it is counter-productive to treat users as the enemy (Adams & Sasse, 1999), encouraging organisations instead to adopt a *participatory* approach in managing employees attitude and behaviour towards security.

Recent research repositions humans as active collaborators (Kirlappos et al., 2013), or "*principal agents*" (Pallas, 2009) in helping the organisation manage security risks is a more effective and sustainable strategy. For instance, Kirlappos & Sasse (2014) emphasise that a participatory approach is likely to engender an improved security culture where individuals play a role in complying with policy. Nevertheless, if security processes make it difficult for users to complete their primary roles, they may be more inclined to engender a negative affective response towards security and withdraw participatory engagement in following policy. This negative *affect* as it is referred to in the psychological literature (Slovic, Finucane, Peters, & MacGregor, 2007) may also impact on user perception of security risks and negatively influence compliance behaviour.

1.2.2 The importance of employee security risk awareness

Once organisations have ensured there is sufficient *security hygiene* within the organisation, they also need to ensure employees understand security risks and modify their behaviour where appropriate and also recognise the implications of areas of institutionalised non-compliance or "*shadow security"* within the organisation (Kirlappos et al., 2014).

For instance, if employees regularly circumvent security processes to get their tasks done, despite being aware of the security risks, it is important for them to feel comfortable enough to explain to their managers how security impacts on their primary job role, and identify friction. *Friction* is created when there is a misalignment between the employee's primary task (*job associated tasks*) and the overheads derived from the security task (*time, cognitive effort, ease of use*), which may interfere with the employee's goal of completing their main task.

Specific feedback on why employees are creating workarounds given to those responsible for designing security processes can lead to better processes and policies to reduce circumvention in the longer-term. Conversely, employees who are supportive of organisational security policies but do not recognise the risks of circumvention will likely benefit from security awareness training. Employee risk perception then is clearly a key part in reducing non-compliance or at least, allowing employees to recognise the implication of the risks that may arise from acts of non-compliance.

1.3. Conclusions from the literature review

This section will now turn to considering the research gap in the literature between risk perception, affect and information security compliance behaviour. Affect and risk perception has been extensively explored within the psychological literature (Slovic, Finucane, Peters, & MacGregor, 2004) but it is less prevalent within the information security literature, where cognitive explanations for risk perception tend to be emphasised (Farahmand, Atallah, & Spafford, 2013).

As discussed in the literature review, Farahmand, Atallah & Konsynski (2008) revised an existing framework based on a psychometric model, using two main dimensions to better understand risk perception which are concerned with i) *understanding* and ii) *consequences of an event*. It is argued that the BSG is different from this model in that whilst the Farahmand et al. (2008) model does seek to gather information from both cognitive and affective aspects via a set of questions, it does not explicitly measure positive and negative *affective* attitudes towards security which is a key component of the BSG.

Another point of difference between Farahmand et al's model and the BSG framework is the way in which each model categorises security. For instance, Farahmand et al., (2008) presents five levels relating to the impact of the *consequence*s dimension, and six levels relating to the *understanding* dimension. The BSG categorises security behavior into four distinct areas referred to as *Open*, *Hidden*, *Blind* and *Unknown* have been adopted from the Johari Window (Luft & Ingham, 1955), which has been revised to consider modes of security behaviour as a consequence of both *Strong* and *Weak Positive* and *Strong* and *Weak Negative* for both *Risk Understanding* (RU) and *Affective* Security (AS). This thesis aims to bridge this gap by developing a framework to map employee understanding of security risks as well as affective responses to security.

As discussed above, the BSG builds on Farahmand et al.'s work (2008) to some degree, as it aims to capture both affective and cognitive stakeholder perceptions of information security risks within a revised framework. But - rather than focusing explicitly on the misalignment of organisational incentives - the BSG aims to categorise individual differences in terms of their understanding of cyber risks and affective attitudes towards security in the form of security behavioural quadrants.

Another security framework which was developed by Alfawaz et al., (Alfawaz, Nelson, & Mohannak, 2010) categorises information security behaviour according to four modes reflecting individual knowledge, skills and awareness. However, it doesn't specifically account for risk perception or understanding of risks, nor emotional responses to security. The BSG builds on the work of Alfawaz et al., (2010) by developing an organisational security framework but also explores levels of employee risk competence, referred to as *Risk Understanding* and affective attitudes, feelings and behavioural preferences towards security, referred to as *Affective Security*, in relation to security behaviour.

Massie and Morris' model (Massie & Morris, 2011) has inspired this research because they revised the Johari Window (Luft & Ingham, 1955) to express *known* and *unknown* risks for NASA's Constellation Program. Their model also incorporated personality traits, specifically how different types responded to what they were or were not aware of. However, their model did not explicitly use affective and understanding of cyber risks as drivers of security behavior. The BSG will build on the framework developed by Alfawaz et al., (2010) and Massie and Morris' model (2011) but explicitly examine two dimensions; *Risk Understanding* and *Affective Security* in relation to employee security behaviour.

Security paradigms influenced by economics which present employee compliance behaviour as a function of a cost-benefit analysis have also shaped the development of the BSG. For instance, work relating to the "*compliance* *budget*", where individuals make an active choice as to whether they wish to comply (Beautement, Sasse, & Wonham, 2009) help explicate behaviour in the *Hidden* quadrant in particular, where employees understand the risks but may hold negative attitudes, feelings and preferences towards security which in turn impacts on their security behaviour. It should be noted however that the researchers did not *explicitly* consider risk understanding in relation to compliance behaviour which the current study seeks to address. Herley (2009) also highlights that security advice often does not take into account the amount of effort that is required to complete security tasks and given its low cost-benefit is rejected.

Kirlappos et al. identified three distinct drivers for non-compliance which included "*high costs*" associated with compliance: "*lack of understanding*" of security risks and an "*inability"* to comply due to deficiencies within the technical implementation (Kirlappos et al., 2013). They do not explicitly consider these compliance drivers in relation to the impact on stakeholder risk perception, although they acknowledge that risk perception played a role in determining behavioural responses to security policy. The BSG seeks to address this gap by mapping employee risk perceptions in relation to information security policy.

The BSG could be used as a diagnostic framework for organisations to explore employee risk perceptions and affective attitudes to security in the form of i) their position on the grid, ii) behavioural responses that may be inferred from "*security stories*". As far as I am aware this is a novel approach to categorising security behavior into quadrants, in relation to risk and affect operationalised via the dimensions *Affective Security* and *Risk Understanding* (Beris et al, 2015).

Case Study 1 culminated in a co-authored paper; written by myself, as the first author, UCL colleague Adam Beautement and my supervisor M. Angela Sasse which I presented at the New Security Paradigms conference in the Netherlands in 2015 (Beris et al., 2015). This paper outlined the BSG framework which included the two dimensions of *Affective Security (AS)* and *Risk Understanding (RU*).

1.4 Research focus

The research presented in this thesis maps out how different levels of recognition and awareness of security risks and affective feelings, attitudes and behavioural preferences towards security imply different types of employee security modes.

For the purposes of this research, affect is used broadly to refer to positive and negative attitudes, emotional feelings (Fishbein & Ajzen, 1975) as well as affective responses that may imply preferences and choices related to security behavior (Van der Pligt, Zeelenberg, Van Dijk, de Vries & Richards, 1998) (see *Chapter 3* for further discussion). It is relevant to mention here that the role of affect as a motivator towards behaviour has been documented in the literature. For instance, within the field of consumer behaviour, affective states are explicitly linked with '*affective behaviour'*, i.e. a state of 'dissatisfaction' may engender ‘complaining behaviour’ in relation to the target stimulus (Santos & Boote, 2003). Custers and Aarts (2005) suggest that positive affect can lead to “*non-conscious goal pursuits*”. In other words, individuals are more likely to be motivated towards a given behavioural state when it is associated with positive affect, since it indicates the goal is worth pursuing (p.129). This is noteworthy, as it suggests positive affect can potentially motivate individuals towards certain behaviours. This insight can be applied to the domain of security behavior.

To explore the interplay between these dimensions, employees’ security risk competence (*RU*) and feelings and attitudes in relation to security and security behaviour *(AS*) are captured within a framework referred to as the *Behavioural Security Grid* (BSG). The methodological approach will be outlined in greater detail in *Chapter 5.4*; however briefly the BSG is a revision of the *Johari Window* (Luft and Ingham, 1955) incorporating the two key themes of *Affective Security* and *Risk Understanding*, derived from analysis of the transcripts – independently analysed by two coders - as two separate axes.

This dissertation primarily uses a qualitative analytic technique called *Applied Thematic Analysis* (ATA) to firstly explore the interview data and then secondly, generate qualitative codes to guide the research questions and derive hypotheses across three case studies. Following this, a “*confirmatory approach”* has been adopted to test the relevant hypotheses based on the initial exploratory analysis (Guest, MacQueen & Namey, 2012). The hypotheses are tested using quantitative analysis to explore where the employee population resides within the four quadrants of the BSG framework.

Case Study 1 used applied thematic analysis (ATA), a qualitative technique to code and analyse 93 interview transcripts across two organisations, a utility company and a telecommunications company referred to as Company A and B respectively. The BSG framework was developed from this initial case study (Beris et al, 2015) where *AS* and *RU* were used as the two main axes of the framework. This framework was used to explore four modes of security behaviour; delineated as *Open, Blind, Hidden* and *Unknown,* reflecting the terms from the Johari Window construct (Luft & Ingham, 1955). Case Study 2 involved conducting and analysing 20 interviews across a UK Government department. The same methodological approach to coding was used as in Case Study 1 in order to maintain consistency across case studies. Interviews were analysed and coded using ATA and quantitative analysis was used to score the dimensions of *AS* and *RU* in order to locate employees within the content of the BSG framework. Case Study 3 was carried out across various UK Government departments of which the participants were all Senior Information Risk Owners/Managers (SIROs) or incorporated aspects of the SIRO role into their primary job. The same methodological approach was applied as in Case Study 2 using both qualitative and quantitative techniques analysing 11 interviews using ATA to explore the qualitative themes, and then quantify the key dimensions *AS* and *RU* to locate within the BSG framework. A 16-item survey, which included items that were designed to reflect the four

BSG quadrants, was administered within Organisation D for the purpose of triangulating the results with Case Study 3.

1.4.1 Research questions

The main research aim was to better understand the drivers of security behaviour, by delineating *affective* feelings, attitudes and behavioural preferences towards security (*Affective Security*) and security risk competence, or *understanding of security risks (Risk Understanding)* derived from employee interviews on the topic. These two dimensions of *AS* and *RU* were used to imply different types of security modes across cohorts using the BSG framework.

Q1. What can be learned from delineating affective feelings, attitudes and behavioural preferences towards security (Affective Security) and security risk competence, or understanding of security risks (Risk Understanding) from employee interviews on security behaviour?

Q2.How can these two key dimensions - i) knowledge of security risks (RU) and ii) affective feelings, attitudes and behavioural preferences towards security (AS) - assist security practitioners/O.D. managers in understanding more about employee security behaviour within organisations?

Q3. How might the Behavioural Security Grid (BSG) framework help represent these differences between organisational security cultures as well as individual teams/groups?

Q4.What can be gleaned from the cohorts interviewed about affective attitudes, feelings and behavioural preferences towards security (AS) and knowledge of security risks (RU)?

In relation to each case study, the propositions are as follows:

Case Study 1: *It is expected that affective attitudes, feelings and behavioural preferences towards security (Affective Security) and security risk understanding (Risk Understanding) will differ across organisations, i.e. Company A and B.*

Case Study 2: *It is expected the sampled cohort within Organisation C will demonstrate Positive Risk Understanding due to the security context of the work environment.*

Case Study 3: *It is expected that the cohort of SIROs from Organisation D is likely to demonstrate both Positive Risk Understanding and Positive Affective Security due to the nature of job role i.e. vested interest in information security risk management as well as the context (Government agencies).*

1.5. Summary of contribution: Substantive and methodological

This thesis aims to improve understanding of employee security behaviour by utilising two main dimensions; affective feelings, attitudes and behavioural preferences towards security, referred to as *Affective Security (AS)* and understanding and recognition of security risks referred to as *Risk Understanding (RU)* (Beris et al, 2015). This research draws from the existing body of psychological and decision-making literature on risk and uses empirical data to check whether these insights apply within the domain of information security. In particular, the relationship between risk and affect are prevalent in the psychological literature, where affective explanations for risk perception are emphasised (Slovic et al., 2004).

The substantive contribution of this thesis offers new knowledge about the importance of *AS* and *RU* in security behaviour, where *AS* is perceived as a potential '*motivating*' factor in driving security behaviour. *RU* is a necessary competence of staff to recognise the risks, but results suggest that *RU* alone is not sufficient to improve security behaviour in much the same way as ensuring *security hygiene* is in place to allow employees to comply with policy. This can be compared to Herzberg's two-factor theory (1966) which delineated between job *motivators* and *hygiene* factors; the former was required to improve performance whereas the latter was a basic requirement for performance. This is of particular relevance to industry and practitioners who could explore the impact of harnessing *Positive AS* to improve security cultures within their organisation.

Therefore, one of the novel contributions of this research is identifying *AS* as a measureable component of security behaviour and creating a framework, the BSG, to map employee levels of *AS* and *RU*. The purpose of the BSG is to enable organisations to diagnose both positive and negative issues within the organisational security culture, by creating a deeper understanding of employee security behaviour using *AS* and *RU*. Each one of the quadrants imply different organisational interventions and depending on the security map for each organisation, these interventions can be informed by using the BSG as a diagnostic tool (see *Chapter 9.4.1:Contribution to Practice*).

Another key substantive contribution of this thesis to the information security domain is the generation of new knowledge about the drivers of risk perception and security behaviour in populations hitherto unsurveyed - both Organisation C and employees from various Government departments referred to as 'Organisation D'. Getting access to this group of individuals is generally difficult and therefore are novel cohorts for a study of this nature. The participants in both Organisation C and D are expected to be knowledgeable about security risks - Organisation C is in the security sector, and members of the 'Organisation D cohort' held posts that include responsibility for information security risk management. In particular, the cohort of SIROs which constituted the Organisation D population sample, offered an opportunity to glean unique insights about security risks and behaviours from the point of view of a Senior Risk holder in the organisation.

Hence, these two populations are unique in that they offer a particular view of employee security behaviour in an eco-system where one would expect its employees to be i) highly aware and respond appropriately to security risks and ii) demonstrate a positive attitude and behavioural preferences towards security which can incorporate being *critical* of the policy to improve *security hygiene*. This substantive contribution offering insights into this novel cohort within the IS domain is likely to be of interest to academic researchers as well as security practitioners within industry to compare the differing perspectives.

In relation to the methodological contribution, the BSG offers an innovative methodological approach, building on an existing psychological paradigm referred to as the *Johari Window* (Luft & Ingham, 1955) but using the two dimensions of *Risk Understanding* and *Affective Security* for axes x and y respectively. Thus, this is a novel approach applied to an security-oriented cohort in order to provide a new framework to better understand government employees' security behaviour, by delineating the dimensions of *RU* and *AS*, within a security context (see Beris et al, 2015).

1.6. Structure of thesis

Chapter 1 is an introduction to the research topic, locating it within the domain of information security and specifically, the human aspects associated with organisational security behaviour. It emphasises the role of the employee in relation to security compliance behaviour including the importance of employee risk awareness.

Chapter 2 presents an overview of the relevant literature which includes a summary of the psychological and decision-making research on risk perception and affect. A summary of heuristics and biases are also presented in relation to risk perception.

Chapter 3 focuses on the interplay between affect and risk perception in relation to employee security behaviour. It explores how the employee weighs up the risks and benefits associated with security compliance and how affective attitudes towards security imply different types of security behaviour.

Chapter 4 summarises the methodological approaches and research design decisions adopted for this thesis. This includes an overview of the qualitative research and quantitative methods i.e. a mixed methods approach and issues relating to validity and reliability.

Chapter 5 describes Case Study 1, which involved the analysis of employee interview data on security behaviour drawn from two organisations, a utility and a telecommunications company referred to as Company A and B respectively. A mixed methods approach incorporating qualitative and quantitative analysis was adopted in order to i) measure affective security feelings, attitudes and behavioural preferences (*AS*) and recognition of security risks (*RU*) across both organisational cultures, ii) classify employee security behaviour, using *AS* and *RU*, within a framework referred to as the Behavioural Security Grid (BSG).

Chapter 6 describes Case Study 2, which involved the collection and analysis of interview data on security behaviour, where the participants were employees from Organisation C, a Government department. The same methodological mixed methods approach was adopted as in case study 1. The study demonstrated that understanding of cyber risks is not sufficient for employee security compliance behaviour and that positive affective attitudes towards security may be an important factor in improving employee security compliance behaviour.

Chapter 7 describes Case Study 3, which involved the collection and analysis of interview data from Organisation D, which referred to various Government departments. The participants were all Senior Information Risk Managers/Owners (SIROs) who were across Government departments. The same mixed methods approach was applied, consistent with Case Study 2. This suggested that employees who demonstrated *Positive AS* towards security and knowledge of security risks were more likely to demonstrate compliant security behaviour that was aligned with organisational security policy.

Chapter 8 is comprised of a validation study conducted with randomly selected employees at Organisation D. Study 4 was a survey, designed to triangulate the interview data from Case Study 2. The results offered an alternative data source, using a different cohort that was drawn from one of the Government departments at Organisation D demonstrating that about two-thirds of the participants sampled demonstrate *Positive AS* towards security and *Positive RU*.

Chapter 9 reviews the research and synthesises conclusions from the three case studies and validation survey.

CHAPTER 2: LITERATURE REVIEW

2.1.Introduction

Jonathan Evans, former Director General of MI5, has suggested that cyber crime is as much of a security threat to the UK as terrorism, citing one cyber attack that cost a UK business more than £800 million in intellectual property losses (‘British Intelligence Speaks Out On Cyber Threats | GRT’, 2012). Clearly, the risk posed to UK business is a major issue and needs to be effectively mitigated. According to the ISO27005 standards, information security risk is defined as the “*potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation*” (Calder & Watkins, 2010, p.16). Given it is not possible to mitigate against all risks (not all risks are known in advance, and resources for mitigation are finite), part of the challenge for any organisation is to i) define what they deem as *acceptable* risk, and ii) how to manage that risk on a strategic level (Bodin, Gordon, & Loeb, 2008).

Once the organisation defines its risk appetite, or security posture, industry standards such as the ISO27001 advocate that the organisation’s information security risk management policies should be aligned with the “*organisational risk management context*” (Calder & Watkins, 2010). If organisational perspectives and definitions of security risk emphasise the alignment of policies with strategy, employee perspectives on risk may differ in their interpretation and subsequent response to risk. For instance, employees may perceive some aspects of information security policies more important to follow than others depending on their understanding of the risk. Thus, *individual* risk perception is different from the organisation's security posture. Nevertheless, organisational decisions about risk inevitably depend on *human perception* of the potential security risks. The subjective way risk is interpreted means security policies and behaviour may be based on misperceptions of the threat; indeed research has demonstrated that individual risk perception is often subject to errors due to cognitive biases (Johnson & Tversky, 1983) as well as emotional processing of information (Slovic, Peters, Finucane, & MacGregor, 2005).

Exploring how to measure and influence individual risk perception within information security is of relevance therefore because individual and organisational perception of security risk and the associated threat directly informs how they respond. Employees may, for instance, underestimate the security risks associated with non-compliance of information security policy and therefore may be more likely to circumvent policies (Kirlappos et al., 2013). This may be not due to employees' lack of technical awareness, but - as Kirlappos et al. (2013) note - because of deficiencies in the organisational technical infrastructure, which can frustrate attempts to comply with policy. Employees may also blur personal and work boundaries in relation to use of BYOD policies which may contribute to increased "*risky*" security behaviour in the workplace (Blythe, Coventry, & Little, 2015).

Research has suggested that employees are behaving *rationally* by rejecting security policy: they may consider that the effort involved in following security policy burdensome are simply not worth their effort (Herley, 2009). These factors may, in turn, play a part in shaping and influencing employee information security risk perceptions, where threats may be downplayed due to the difficulties associated with compliance.

Schneier argues that one of the problems of risk perception is when the "*feeling*" of security is not aligned with the "*reality*" of the security risk; in other words humans can sometimes miscalculate the security trade-off due to systematic biases (Schneier, 2008). Schneier suggests that risk perception can become distorted because we evaluate risks "*intuitively*" which impacts on how accurately we try to evaluate the severity and probability of the risk, the magnitude of the cost, the efficacy of the risk mitigation versus the cost trade-off (Schneier, 2008). In evaluating Schneier's contribution here, it should be highlighted that his views are a synthesis of research within the psychological risk decision-making domain, rather than original research.

To better understand risk perception, lessons can be drawn from cognitive psychology identifying the factors that influence and govern *how* individuals judge and make decisions about risk is clearly relevant. In particular, two modes of thinking, derived from cognitive psychology, are likely to offer some insight into how individuals perceive risks associated with information security. These two modes of thinking are referred to as *System 1* and *System 2* (Stanovich & West, 2000). *System 1* is an automatic and therefore fast processing system which is characterised by its intuitive, associative properties whereas *System 2* is more effortful and therefore slower, but considered more rational and analytical (Stanovich & West, 2000). Kahneman suggests that although individuals may *feel* that it is their conscious *System 2* selves that controls their perceptions and decisions, it is actually the automatic associative operations of *System 1* which may have a more pervasive influence over how perception of risk are formed (Kahneman, 2012). Although researchers have identified the importance of these two systems in forming security risk perceptions (Schneier, 2008) there has been limited empirical research in the information security literature. This thesis attempts to fill this gap in the research by exploring and measuring employee affective feelings, attitudes and behavioural preferences towards security and risk awareness and understanding in relation to security behaviour.

Conducting a study focused on measuring and influencing employee perceptions of information security risk is challenging for two reasons: 1) Teasing out the factors that actually influenced their risk perception might be difficult to isolate given that they may present as an instinctive and unconscious response via *System 1*, 2) Employees do not always necessarily recognise security risks in the workplace, and measuring something that is abstract and (in some cases) undetectable to the perceiver is difficult because it is essentially an "*unknown unknown".* Therefore one of the principles underpinning this research project is to examine employee security *behaviour,* or their analysis of the security behavior of colleagues in relation to risk, rather than simply asking users about how risky they think a given security behaviour is.

2.2 Literature review structure

This literature review will present a brief overview of general definitions of risk rooted mainly in the psychological literature, followed by a summary of information security risk and risk perception. Non-compliance of security policy and risk perception will be discussed and possible impacts on information security risk perception will also be referred to. A brief section identifying some of the differing organisational stakeholders and their perspectives on information security risk will be covered within the literature review. An overview of the information security risk literature will also be briefly presented, in particular exploring how risk perception has been investigated in a security context. The impact of affect, within the context of the heuristics and biases literature, will be discussed particularly in relation to *System 1* (Stanovich & West, 2000) and misperceptions of information security risk. How the psychological literature can help illuminate and better understand employees' perception in relation information security risk will be referred to. Limitations associated with the literature will be briefly referred to followed by a summary of the proposed research gap this dissertation aims to address.

2.3 Definitions of risk

A discussion relating to *perceptions* of information security risk should be prefaced by a discussion of what risk actually is. Renn & Benighaus suggest that the scientific conceptualisations of risk refers to the "*probability distribution of adverse effect*", whilst lay definitions generally characterise risk as the "*likelihood of an adverse event*" and the possibility that an event is will have a negative impact on something they "*value*" (Renn & Benighaus, 2013, p.295).

What is interesting in most of these definitions is that risk is typically framed as a *loss* in both conceptualisations, rather than explicitly associating risk with behaviour that also brings the prospect of possible *reward*. In addition, the scientific construction of risk refers to probability models designed to calculate the odds implying some degree of objectivity perhaps, whereas general definitions are more focused around how humans perceive risk and in turn, evaluate the consequence of potential losses. Notwithstanding, Aven for instance, challenges the assertion that definitions of risk should be framed purely in relation to loss; suggesting that anticipated losses as an inherent part of risk may bias the risk perceiver (Aven, 2012). Furthermore, Aven argues that probability models of risk are not comprehensive in that all the "*uncertainties*" cannot be known, therefore the "*unknown unknowns"* cannot be estimated (Aven, 2012).

Aven and Renn present risk as a broader concept characterising it as: "*uncertainty about and severity of the events and consequences of an activity with respect to something that humans value*" (Aven & Renn, 2009, p.587).

They note that "*severity*" reflects the magnitude of the risk, such as its perceived size, and that it should be understood in relation to what people value, so it needs to take into account losses or gains (Aven & Renn, 2009). They also emphasise that "*uncertainty*" relates to both the event (or risk itself) and the consequences, whereas the "*severity*" says something about the anticipated consequences. Other technical definitions of risk suggest it is the "*probability of events and the magnitude of specific consequences*" (Kasperson, Renn, Slovic, Brown, Emel, Goble, Kasperson & Ratick, 1988, p.177).

2.4. Definitions of information security risk – Industry standards

General definitions, types and perceptions of risk have been presented, this section will now consider specific definitions of *information security risk.*

In terms of the industry standards governing information security risk, the guidelines operationalise risk in relation to a process or function, breaking it down into each component part; for instance, the acceptance of a risk, how it is analysed, assessed, evaluated, managed and treated is referred to (ISO/IEC 27001, 2005). In this way, ISO27001 defines information security risk in relation to "*risk-related activities*" rather than as a stand-alone definition (Calder & Watkins, 2010). The ISO27000 standards define risk as the "*combination of the probability of an event and its occurrence*" (Calder & Watkins, 2010). This definition implies that the probability of the risk occurring can be calculated in an *objective* manner, which of course is problematic since many risks are unknown and therefore cannot be calculated (Taleb, 2010).

What is particularly interesting about the ISO guidelines suggests that information security risks are "*always present*" as assets are open to threats via the vulnerabilities that can occur within "*processes, systems, network and people*" (BS ISO/IEC 27002:2013). It also suggests that any changes to business processes may lead to new security risks (BS ISO/IEC 27002:2013). This is interesting as it positions risk as an ongoing *reality* to be managed within the information security process which should be aligned with business objectives.

Within the academic information security literature, as with much of the general risk literature, the concept of risk appears to be explicitly framed in terms of loss; for instance Bodin, Gordon and Loeb (2008) identify three measures associated with security risk which include:

> *"…the expected loss, the expected severe loss and the standard deviation of the loss." (Bodin et al., 2008, p.2 in 'working paper' version).*

In information security, it seems intuitive that the risks associated with security breaches are inevitably linked with losses, and, perceptions of the magnitude of the loss. Other researchers suggest that information security risk is the product of security incidents and financial losses as well as the probability that they will occur (Sommestad, Ekstedt, & Johnson, 2010). For instance, in relation to online security risks, Wang & Nyshadham (2011) note that the literature suggests that consumers calculate risk according to expected utility analysis, that is:

> *"... the subjective probability of a loss" and "the subjective magnitude of consequences of the loss, and compute an expectation of loss" (Wang & Nyshadham, 2011,p.1).*

Wang et al. suggest this approach is not explicit enough because consumers do not necessarily know what many of the online risks are nor what their predicted outcomes are likely to be (Wang & Nyshadham, 2011). In addition, they suggest that this is not just a problem for non-experts: experts do not necessarily know the probability of a credit card fraud either (Wang & Nyshadham, 2011). Likewise, Rhee, Ryu & Kim highlight that standard definitions of risk that relate to the multiplication of the probability of an incident versus the anticipated extent of the consequences does not necessarily lend itself to measuring information security risk, since many security incidents are either unknown or simply not reported (Rhee, Ryu & Kim, 2012, p.222).

This viewpoint echoes other researchers (e.g. Aven & Renn, 2009) who position risk as something that relates to uncertain outcomes and the consequences of those outcomes. Relating this to the information security domain, it is important to remember that security threats may appear invisible unless the consequences of the security incident becomes apparent and therefore perceived risks may be invisible or downplayed. The risk is invisible until it becomes an incident which is then experienced viscerally in general, as a loss which can be measured and is therefore concrete.

In summary, there are two perspectives on framing and conceptualising information security risk, with the industry standards on the one hand placing risk as an inherent part of the information management system, whereas the academic information security literature emphasises risk as a loss in many cases. This is important to note from a psychological perspective as framing constructs within a specific context, such as a *loss frame*, has potential implication for risk perception where individuals may be inclined to take a more risk-taking approach (Kahneman & Tversky, 1979). The (ISO 270001) definition of information security risk and the general risk literature is similar in that both refer to a probabilistic approach which arguably does not take into account the risks that are not yet known, and therefore cannot be predicted.

2.5. Types of risk

One way of interpreting risk is to frame it in relation to feelings and analysis (Kahneman, 2012). Slovic et al. (2004) suggest that there is an evolutionary basis in using emotion or instinct to guide perceptions about risk, whereas more analytical approaches to risk assessment such as probability theory for instance, rely on a more reason-based approach. As such, individual perceptions of risk may be directly affected by two modes of feeling and thinking; hence *System 1* and *System 2* (Kahneman, 2012). Information security risk management definitions such as ISO20007 emphasise the alignment of organisational strategic risk strategy with its information security policy (Calder & Watkins, 2010). Clearly then, risk is a nebulous concept with multiple, overlapping definitions ranging from probabilistic interpretations, organisational perspectives to more affectively, subjectively influenced constructions.

As previously discussed, as well as probabilistic interpretations of risk there are also more subjective interpretations (Aven, 2012). Kahneman refers to Slovic's comment that effectively the idea of an "*objective risk*" does not exist "*outside our minds and culture*" but rather that it is developed by humans to manage potential hazards (Kahneman, 2012). In a similar vein, John Adams defines risk as a concept that is ultimately subjective stating:

> "*risk is defined, by most of those who seek to measure it, as the product of probability and utility of some future event. This future is uncertain and inescapably subjective; it does not exist except in the minds of people attempting to anticipate it…"* (Adams, 1995, p.30).

In Adams' conceptualisation, risk is *unknowable,* in that the event to which it refers has not yet occurred and therefore risk is more about *perceptions* of the anticipated future impact of an event. Given that the previous definitions associate risk with loss, incorporating the notion of subjectivity in his model of risk is different (Adams, 2002). In the context of information security, the consequences of risk are inevitability associated with loss because effective security is when nothing damaging occurs, in other words, when nothing happens (West, 2008). Indeed, the industry standards (i.e. ISO 270001) define information risk as a potential threat that will "*exploit vulnerabilities*" (Calder & Watkins, 2010) which does not focus on reward but instead highlights the "*potential harm*" that the exploitation of vulnerabilities can cause the organisation.

Adams notes that inevitably loss or *accidents* may occur as a result of risk taking, but on the other hand, to eliminate the risk of adverse events effectively means that no risks can be taken at all. In his *Risk Thermostat* model, Adams postulates that risk-taking is analogous to a *cost-benefit analysis* in that the more rewards an individual may associate with a given risk, the more likely she is to engage in the said *risky* behaviour and as a consequence, the thermostat setting increases (Adams, 2002). In addition, the model hypothesises that when the level or "*propensity*" to take risks and the perception of the threat becomes misaligned, some sort of behavioural response or "*balancing behaviour*" needs to occur (Adams, 2002).

One central aspect of the risk thermostat, according to Adams, is that individuals will tend to gravitate back to a level of risk they are comfortable with. For example, if someone who manages comfortably with a high level of risk is required to adhere to various safety behaviours, they may compensate by taking additional risks (Adams, 1999). In the context of information security, an example of this might be an individual who regularly updates their anti-virus software when prompted, but then downloads files from non-mainstream download sites. They may *feel* they are "*secure enough*" since they have done it before without apparent event and moreover, *feel* they can rely on the anti-virus software although it could be argued that downloading files from unverified sites carries more of a risk from as yet unclassified viruses infecting the machine. As Slovic et al. (2004) indicates, "*risk as feeling"* can, in some instances, overwhelm the individual and lead to errors of judgement where feelings conflate the consequences of the risk. In relation to

Adams' risk thermostat framework, it is intuitive and offers face-validity in understanding risks although as far as I am aware, it is empirically untested.

Adams also distinguishes between different types of risk; risk which is *perceived directly*, risk that is *perceived through science* and *virtual risk*. Directly perceived risk is viscerally experienced by individuals, and assessed intuitively. Risks perceived through science can be quantified formally, and in many cases the probability associated with certain events occurring can be assessed (Adams, 1999). Adams (1999) makes the point that if individuals do not trust science and scientists however, they may dismiss official Government statistics for instance, and over-exaggerate the risk. The third category, virtual risks, are uncertain risks where the event may or may not be real. I would argue that cyber risks are located within this category since such risks are uncertain, the individual is not necessarily aware whether their computer has been infected with a virus for example, or whether a *man-in-the-middle* attack has compromised their communication paths.

Adams acknowledges the differences in approaches to risk and draws on cultural theory, linking risk *archetypes* – i) *hierarchist, ii) egalitarian,*
iii) individualist and iv) *fatalist*, to explain risk perception; i) hierarchism refers to individuals who recognises social boundaries and hierarchies, ii) egalitarians see themselves as being more loyal to the group than external constraints, iii) individualists see themselves as more self-reliant, seeking to exert control over their immediate environment and iv) fatalists feel they have little control over the circumstance (Adams, 1995, p.36).

Adams suggests that that people may have a particular preference for not only the level of risk they are prepared to tolerate, but are also affected by a cultural lens through which they perceive and evaluate risks (Adams, 1995). Recent research within the domain of information security has shown that in terms of security behaviour age is a factor (Beautement, Becker, Parkin, Krol, & Sasse, 2016). For instance, Beautement et al. found that older individuals may demonstrate more fatalistic attitudes towards security, where they feel they have less control over their outcomes, whereas younger individuals are more likely to embody hierarchically-oriented attitudes, relying on technologies for instance to help solve problems. These risk archetypes are relevant to mention here, since this thesis also explores the classification of security behaviour, but specifically in relation to two axes based on understanding of cyber risks and affective attitudes, feelings and behavioural preferences towards security.

2.6. Risk perceptions

I will now briefly consider *perceptions* of risk. As discussed, given the lack of consensus in the literature regarding definitions of risk, it follows that risk perceptions are inherently subjective, and therefore subject to bias. Aven delineates between the concept of risk and *perceptions* of risk stating that risk perception may encompass: "*personal feelings and affections about the possible events, the consequences of these events and about the uncertainties and probabilities*" associated with these events, but that these aspects associated with perception do not represent risk per se (Aven, 2012, p.34). Slovic et al. (2004) delineate between "*risk as feelings*" and "*risk as analysis*", but argue that "*intuitive feelings*" are the main way that individuals assess risk. Other researchers define risk perception as the product of the *subjective* assessment of the risk and its magnitude (Knowles, Prince, & Hutchison, 2012). This is a useful distinction to make in relation to risk perception, as Aven suggests that risk perceptions may be our *subjective* reality but which are nevertheless separate from actual risk itself (Aven, 2012).

2.7 Information security: non-compliance and risk perception

In some cases, employees may fail to comply with information security policy because they have a different perception of risk: the main risk as far they are concerned is failing to perform their job, referred to as the *primary task*, a human factors term (see *Glossary*), (Ka Ping, 2004). This argument is echoed by industry expert Schneier (2008) who suggests that employees do not necessarily fail to comply with security policies because they do not *understand* the risk - they just conceive it differently in that the organisational risks for them are less salient, whereas getting their job done takes precedence. Therefore investigating the factors that influence non-compliance may be fruitful in providing insights into the factors that influence employees and managers' perception of information security risks.

Padayachee compiled a taxonomy summarising the factors that drive individual security behaviour, as a tool for organisations seeking to manage it (Padayachee, 2012). In particular, the author identified *organisational commitment*, defined as the psychological state of the employee attachment to the organisation and *awareness,* as factors that impact on security behavior. It is suggested that these factors may colour how employees perceive the risk, which in turn, may influence security behaviour. Certainly, organisational commitment and the related concept of *affective commitment* (Meyer, Stanley, Herscovitch, & Topolnytsky, 2002) - where feelings of attachment to the organisation has been demonstrated to positively influence employee behaviour - may influence security risk perceptions as well as security behaviour itself. A potential strength of Padayachee's research is that the taxonomy is based on empirical findings, rather than derived from studies which are less ecologically valid such as studies that not conducted "*in the wild*" (Shepherd, Archibald, & Ferguson, 2013). Affective attachment to the organisation is thus a promising factor to explore in understanding security behaviour.

Other examples of empirical research include Kirlappos et al.'s paper on security non-compliance, which identified various real-world security problems that present difficulties for organisations (Kirlappos et al., 2013). The authors note that one of the key problems in relation to organisational approaches to information security is that policies and procedures do not take into account the employee's perspective and often end up burdening the employee with more audit checks etc.. This may have implications for risk assessment as research has indicated that there is an inverse relation between *risk* and *benefit* (Finucane, Alhakami, Slovic, & Johnson, 2000). Applying this to information security suggests that a high-benefit option for the individual (such as circumventing onerous security tasks in order to maximize primary task performance) may lead to downplaying the associated security risks.

Kirlappos et al., (2013) also identify a number of common misconceptions about information security risks amongst employees : i) that using a personal USB stick is unlikely to cause any harm, ii) that deleted data can not be recovered from computer drives and iii) that protecting sensitive files with a password, that is actually related to access control, is sufficiently secure (Kirlappos et al., 2013). An individual's lack of security awareness may imply a lack of awareness around the security risks associated with their actions.

Lack of knowledge often underlies misconceptions around security risks; for instance, Kritzinger & von Solms found that home computer users are "*vulnerable*" to cyber security crime as they do not have sufficient knowledge around information security to protect their personal data on their machines and as a consequence, are unable to make effective risk assessments (Kritzinger & von Solms, 2010). Moreover, they suggest that individuals may be unaware of threats and therefore are not going to perceive them as risks (Kritzinger & von Solms, 2010).

Another issue that may encourage employees to adhere to information security policy is to clearly identify "*risky security behaviour*" as such. Shepherd, Archibald and Ferguson argue that users may develop a "*knowledge-based trust*" relationship with their device, which means that even if the performance of their device seems to change, their trust remains intact (Shepherd et al., 2013).

Kirlappos et al. (2013) identified *lack of organisational infrastructure* to be another driver of non-compliance. Employees reported i) copying files to their laptops because it was difficult to access them whilst travelling, or because there was not enough space on network drives for all the files, ii) using unencrypted USBs or emailing files instead and iii) writing down their passwords because they had too many to manage.

Based on these observations, Kirlappos et al. argue that the company was *"tacitly complicit"* in employees' workarounds, driven by the belief that work would "*grind to a halt*" if they followed the rules (Kirlappos et al., 2013).

It could be argued that in some cases, the *consequences* of security compliance for employees may be perceived to be more detrimental to the smooth running of the organisation than the non-compliant or "*risky*" behaviour (Kirlappos et al., 2013). In other words, if the process for security compliance is sufficiently onerous, non-compliance is a reasonable trade-off for efficiency and justifies a downplaying of risks. As discussed, the inverse relationship between risk and benefit (Alhakami & Slovic, 1994) may mean that easier options lead to perceptions of lower risk. The authors did not explicitly investigate the relationship between risk awareness and information security however, nor did they seek to measure risk perception within the scope of their study.

Takemura (2011) examined the relationship between employee information security awareness, risk perception and compliance (Takemura, 2011). They found that risk perception directly influences "*problematic behaviours*" concerning information security. They demonstrated that individuals whose workplace satisfaction is low might be likely to engage in non-compliance behaviour. One of the limitations of this study, which they acknowledge, is the source of data. They collected their responses via a web-based questionnaire survey that asked respondents questions about their awareness and behaviours related to information security measures. One particular weakness of the study is the use of hypothetical questions which could elicit answers that are not necessarily representative of what the participant might do when faced with the actual situation.

2.8. Stakeholder perspectives on information security risk

2.8.1 Expert and non-expert: probability vs. consequences

I will now present a brief overview of how different perspectives shape and influence individuals' perception of risk. Firstly, I will consider the perspectives of *experts* and *non-experts* in the general risk literature, and then turn to how different stakeholder roles influence risk perception as explored in the information security literature.

Risk perception can be impacted by whether an individual is an expert or a non-expert. For example, Slovic et al. highlight that "*risk means different things to different people*" (p.85) and note that whilst experts and non-experts may evaluate risk similarly, non-experts views may be more likely to be affected by the fear of a "*dread*" event for instance, possibly due to its emotional impact (Slovic, Fischhoff, & Lichtenstein, 1982). Other researchers have noted that whilst there may be differences in terms of risk perception between experts within the same field, their assessments tend to be more accurate than non-experts (Knowles et al., 2012).

In one study, (Savadori, Savio, Nicotra, Rumiati, Finuane & Slovic, 2004) experts were shown to perceive the risks associated with biotechnology as less of a threat compared with the public. One possible reason for the experts' lower risk assessment may relate to the knowledge and expertise associated with making risk assessments in specialised areas (Savadori et al., 2004).

Sjöberg (2002) investigated the factors accounting for experts' risk perception, and found that - assuming similar levels of technical knowledge - risk perceptions were "*comparable*" between experts and non-experts. He argues that his results challenge the literature that experts evaluate risk differently since they are subject to the same psychological influences. Savadori et al., (2004), however, found negative correlations for risks based on harm and benefit for both the expert and non-expert sample groups, and they argue that it is possible that both experts and non-experts make risk assessments based on the *affect heuristic*. This runs counter to the notion that scientific risks are evaluated any differently from directly perceived or virtual risks, since affective responses to risk may mean that all types of risks are evaluated, to a lesser or greater extent, via the affect heuristic. In relation to public trust and acceptance of scientific evaluation of risks, Savadori et al. (2004) found that there was a surprisingly low correlation between trust in the source of information and individual risk perception.

Albrechtsen & Hovden (2009) highlight that risk research suggests that experts tend to focus on *probability,* whereas non-experts are more likely to consider *consequences.* In the general risk literature, looking at risk mitigation in transport for instance, studies found that experts place greater emphasis on probability estimates more than politicians and the general public (Rundmo & Moen, 2006). Similarly, Sjöberg (2000) found that a sample of home insurance customers considered the seriousness of the *consequences* of the risk - rather than the probability of the event - to be a more predictive factor in relation to risk mitigation. Applying these findings to the domain of information security suggests that employees who are not security experts may be more likely to be influenced by the *consequences* of security incidents than considering the likelihood of such an occurrence.

2.8.2. Security managers and employees' risk perception

As previously discussed, there is a difference in view in the general risk literature around the risk perception of experts and non-experts with some researchers such as Sjöberg challenging the established idea that experts evaluate risk differently (Sjöberg, 2002). Within the information security risk literature, the picture is slightly more complex. For instance, Albrechtsen & Hovden (2009) highlight that information security managers tend to evaluate risks associated with user behaviour more highly than the users themselves. They connect this with Slovic et al.'s (2007) affect heuristic and the inverse relationship between risk and benefits (Finucane et al., 2000), suggesting that security managers may have a low level of confidence in evaluating employees' security behaviour and therefore may consider them a high risk group (Albrechtsen & Hovden, 2009).

Albrechtsen & Hovden (2009) hypothesised - perhaps not surprisingly - that there are differing levels of risk assessment depending on whether you are a security manager or a user. They identified fourteen information security risks that employees may face and have differing degrees of awareness of. They asked participants to rate each potential threat on a five-point scale from no risk to high risk to the ongoing running of the organisation including: "*human error, virus infections, carelessness, misuse of sensitive information, loss of sensitive information, incautious use of email, software vulnerability, incautious use of the internet, use private purposes, social engineering, spam, hacking, theft of hard/software, use for illegal purposes*" (Albrechtsen & Hovden, 2009, p.10).

They found no significant difference between the security managers and users in terms of risk perception in half the threats which included "*software vulnerabilities, virus infections and treatment of sensitive information*" (Albrechtsen & Hovden, 2009). In relation to the other seven perceived threats there was a different pattern of responses with security managers rating four of the threats to be less risky than the users. These included "*incautious use of the internet*", "*spam mail*", "*use of the organisation's IT resources for illegal purposes*" and "*hacking*". The security managers ranked the other three threats i.e "*IT-related human error*", "*user carelessness*" and "*social engineering attempts*" as more risky, which the authors indicated might be linked to the managers' perception of lower levels of employee security awareness (Albrechtsen & Hovden, 2009). Albrechtsen & Hovden (2009) demonstrated that security managers ranked these threats as higher risk, as they pertain to users' knowledge about security issues. Moreover, their results showed a disparity between the targets of threat between the two groups in that security managers rated *human error* related to security to be the biggest risk, whereas users or employees considered that social engineering threats, which might involve scamming individuals to reveal data, was the lowest risk (Albrechtsen & Hovden, 2009). In relation to these results, security managers considered employees to be a greater risk than the employees themselves. The impact of affect or emotional processing on the assessment of risk was not considered.

McFadzean, Ezingeard & Birchall's research sampled a population of company directors and identified risk perception as a key variable in influencing directors' level of engagement in their management of information security (McFadzean, Ezingeard, & Birchall, 2007). Specifically, they developed a perception of risk grid, which, in brief, mapped high risk perceptions across conditions of operational and strategic uncertainty, whereas they mapped low risk perception across conditions of operational and strategic stability (McFadzean et al., 2007). However, they didn't consider the impact of affect in shaping risk perception.

From this review of the literature, we can conclude that i) an individual's awareness and knowledge of information security, ii) their perception of expertise in relation to estimating associated security risks and iii) position as a stakeholder in the organisation may all play a defining factor in determining assessments of risk. Affective responses to risk are also potential areas for exploration. Therefore, it is important to consider the *perspective* of the stakeholder in relation to understanding the factors which may influence individual's perception of risk.

2.8.3. Individual differences and information security risks

Information security research has identified that specific groups may be more vulnerable to threats – such as phishing - than others; if correct, this has implications for understanding how demographics affect perceived security risks. Sheng, Holbrook, Kumaraguru, Cranor & Downs (2010) examined the variables predicting vulnerability to phishing attacks and found that women between the ages of eighteen to twenty-five years old were more likely to be vulnerable to phishing than men. Sheng et al. also found that risk aversion is negatively related to phishing vulnerability as one might expect.

It is worth noting that there are various limitations with this study; the population sample was drawn from Amazon Mechanical Turk, which - as the authors acknowledge – has a population that is quite different from organisational populations. Participants also faced no actual risk in this web-based task, which may have skewed the participants' risk judgments (Sheng et al., 2010). This is a weakness in the study because consequences influence risk perception, and whilst cyber risks might not always be visible, an awareness of potential consequences influences risk perception.

2.9 Affect and risk perception

Renn & Benighaus postulate that "*feelings*, *values* and *knowledge"* are key variables likely to play a role in influencing individuals' evaluation of the severity and acceptability trade-off of risks (Renn & Benighaus, 2013. p.295). They argue that these broad constructs are potentially important antecedents to explore in attempting to measure the extent to which they influence individuals' risk assessments. Turning to the impact of feelings on risk perception, it is evident that affect for instance is a key driver in the formation of such perceptions. Indeed, the *"risk-as-feelings hypothesis"* (Loewenstein, Weber, Hsee, & Welch, 2001) postulates that affective responses to risk are often precursors to actual behaviour as opposed to cognitive appraisals of risk.

In judging the risks associated with an object, Slovic et al. (2004) suggest that people tend to be influenced by their *feelings*, as well as their thoughts. Specifically, they suggest that individuals are likely to perceive higher reward options as a *lower* risk, whereas if they are less disposed towards a given option an opposite effect is demonstrated, that is lower benefit can lead to an increase in perception of risk.

As well as observing the inverse relationship between risk and reward, Finucane et al. (2000) argued that a *halo effect* is present in relation to affectively influenced risk perception: a change on one variable - such as an increase in risk perception - will have an impact on the evaluation of the other variable, i.e. decreasing perception of reward or benefit. In a sense, Finucane et al. suggests that what we *like* intuitively seems less risky, whereas what we do not like or want may appear as more of a risk. (For further discussion on affect see *Chapter 3*).

Time has also been shown to strengthen the inverse relationship between risk perception and benefits, as it is hypothesised that *reduced time pressure* can lead to less reliance on analytic reasoning and more focus on the affect heuristic (Farahmand et al., 2008). This could be relevant to understanding more about employee perception of cyber risks where individuals create workarounds when they feel they have not got sufficient time to carry out their *primary task*.

Given the plethora of research suggesting that it is rational for individuals to prioritise their primary task over the secondary task of security (Herley, 2009), it may be useful to extend this to explore whether individuals become '*blind*' to evaluating security risks when they are focused on their primary task. It is anticipated that this theme may emerge from analysis of the interview transcripts where employees discuss how security fits into their primary job role and the security trade-offs they have to make to finish their work within set time-constraints.

Additionally, researchers have drawn attention to the impact of emotion on risk perceptions of cyber crime suggesting that anxiety for instance, might increase perceptions of cyber vulnerability as individuals may interpret "*ambiguous stimuli*" as potentially threatening (Jackson, Allum, Gaskell, & Trust, 2006). Jackson et al., also hypothesise that emotions are influenced by perceptions of "*control, consequences and perceived likelihood*" and important to examine in relation to cyber risk perceptions. It should be noted though that the Jackson paper is not an experimental study but rather a literature review suggesting avenues for further research.

2.9.1. Experiential mode and affect

"We favor the visible, the embedded, the personal, the narrated, and the tangible; we scorn the abstract." (Taleb, 2007, p.262)

Slovic et al. (2004) suggest that most people form risk assessments via the "*experiential mode of thinking*", rather than the "*analytical mode*". This former mode is thought to function automatically, driven by affect, where individuals are less "*consciously aware*" of evaluating the risk, whereas the later is based on logic and tends to be slower and requiring more cognitive effort. The experiential mode is characterised by "*encoding reality in concrete images, metaphors and narratives*" (Slovic et al., p.313).

They point out that - although intuitive responses to risk may be considered "*irrational*" - emotion can positively influence risk perception. Specifically, they argue that from an evolutionary perspective individuals tend to rely on the "*intuitive*" experiential system for its short-cuts known as heuristics, which allow people to make quick decisions about the risks they face based on an "*affective impression*" (Slovic et al., 2004). Slovic argues that affect is "*essential to rational action*" in this regard (Slovic, 2004, p.314). Hence, (Slovic & Peters, 2006) suggest that the so-called "*affect heuristic*" refers to using feelings to inform evaluations of risks for instance. Affect is defined here as a "*quality of goodness or badness*" which is "*experienced as a feeling state*" where the positive or negative associations with a given stimulus becomes salient (Slovic et al., 2004, p.312).

Following Slovic's argument, though the experiential system may be optimal in assessing risk in some situations, such as making a judgment about the safety of drinking water as per Slovic's example (Slovic et al., 2004), in other situations individuals may be deceived by their experiential system. For instance, Slovic cites two key ways that the experiential system may obscure perceptions of risk; firstly, that people's affective responses are subject to manipulation by mechanisms, advertising being an example of one such mechanism, and secondly, that not everything in the physical world can be adequately denoted via the "*affective system*" (Slovic et al., 2004). This echoes Schneier's argument that - although humans have evolved to make quick, intuitive decisions related to security-tradeoffs - in some instances we may erroneously inflate risk estimates whilst downplaying others (Schneier, 2008).

There are various biases which the experiential system is susceptible to which impact on risk perception, a few of which I will briefly summarise here. One such bias is the tendency to be influenced by the "*visceral*" where fundamental drivers such as emotion, hunger, desire etc. may have a strong, albeit temporary, impact on how an individual might feel at a given time (Slovic, 2004). It is suggested that the impact of this strong affective response may skew risk perceptions in that positive affect is linked with low perceptions of risk for instance (Slovic & Peters, 2006). Certainly, research has demonstrated that people have a tendency to overestimate the probability of events which elicit feelings of "*dread*" in the risk perception literature (Gigerenzer, 2004). These risks are described as "*low probability, high consequence*" events, which have been demonstrated to skew risk perception because of the strong emotions attached to them (Gigerenzer, 2004). Likewise, psychologists found probability neglect occurred when the outcome, such as kissing a film star, was related to emotional gain above other outcomes such as financial gains for example (Rottenstreich & Hsee, 2001). Further discussion of how affect is explored within this research is outlined in *Chapter 3*.

2.10. Time, hyperbolic discounting and risk perception

Time is another factor that may be problematic for the experiential system to evaluate since the experiential system is focused on the present and not oriented towards future outcomes**.** Slovic et al. note that in the literature, studies on *hyperbolic discounting* (Ainslie & Haslam, 1992) have demonstrated that people may alter their preferences in response to their perceptions of time (Slovic, Finucane, Peters, & MacGregor, 2002). For instance, they may opt for the bigger delayed prize when the given options are both further away in time, but may choose the smaller prize if both options are more immediately available . Indeed, individuals' tendency to discount future rewards in favour of smaller more immediate rewards may support the hypothesis that affective processing of options over-weights "*rewards today*".

Following this argument, it might be suggested that in relation to future risks, the experiential system or *System 1* (Stanovich & West, 2000) may be less likely to be evoked since it is present-oriented and switching to the more analytically-oriented *System 2* (Stanovich & West, 2000) might be optimal. Short-term smaller gains are valued over longer-term larger gains, individuals may be inclined to rate immediate risks as '*less risky'* because immediate rewards are preferable. In terms of a real-world example of how this translates to managing security risks, an employee might decide to delay updating software vulnerability patches despite being aware that they are necessary to maintain computer security. They choose the immediate rewards of more time and less cognitive effort over security.

The research reviewed here suggests that individuals make psychological attributions about temporal distance which are likely to have implications for the measurement and perception of information security risks. Temporal distance is defined here "*the actual distance between a reference point (typically today) and the point of occurrence of the event under consideration (e.g. tomorrow, next year)..."* (Chandran & Menon, 2004, p.376). Hence, they explored the psychological impacts of temporal distance on perceptions of risk, to identify whether an event that is expected to occur in the near future or the distant future impacts on subjective judgments of risk (Chandran & Menon, 2004). The researchers' results indicated that temporal framing *did* impact on risk perceptions such that hazards that were framed as occurring every day, as opposed to every year, were judged as more "*concrete and proximal*" which in turn increased risk perceptions.

Chandran et al.'s research on temporal framing and risk references Trope & Libermans' (2003) work on *construal level theory,* which postulates that individuals use different level *construals* to conceptualise information relating to events that are in the "*distant future*" compared with events that are in the "*near future*" (Chandran & Menon, 2004). Although individuals only directly experience the present, they conceptualise the future by developing "*abstract mental construals of distant objects*" (Trope & Liberman, 2010). Further, within the context of construal level theory, Trope and Liberman highlight that psychological distance is ultimately subjective since the reference point is the individual self. They also suggest that increases in psychological distance lead to the development of abstract constructs that capture the overall meaning of the object (known as "*higher level construals*"), whereas the closer the psychological distance, the more concrete and detailed the "*lower-level construal*" (Trope & Liberman, 2003).

This links to the economic concept of hyperbolic discounting where research has demonstrated individuals do not discount future and near events in the same way (Acquisti & Grossklags, 2007) in that they may be willing to trade-off short-term gain for larger longer-term gain (Anderson & Moore, 2009). In terms of security risk perception, it is likely that hyperbolic discounting may explain why people circumvent security policy such as delaying virus updates which offer longer-term protection against malware (larger gain), for a shorter term more immediately gratifying gain of completing one's primary task (smaller gain).

Applying this theme to information security, Garg and Camp (2012) found that time was the most significant predictor of online risk in their 4-dimensional model. Specifically, they found that "*temporal impact*" which they defined as consisting of "*newness*" and "*common dread*" was a significant factor in explaining most of the variance affecting online risk perception (Garg & Camp, 2012). Garg and Camps' results indicate that "*new"* and "*common dread*" risks are both related to time, in as much as a new risk is novel and therefore has not been encountered before, and a "*common dread*" risk relates to how widely known it is. Research has shown that when comparing risks which occur on a daily or yearly basis, participants tend to perceive the day frame as a higher risk because it is more immediate, proximate and represented via a lower-level construct (Chandran & Menon, 2004). In summary, they suggest that as risks get more familiar, or older, they become more concrete (Garg & Camp, 2012).

Garg and Camp (2012) have argued that risk communication about security might be improved if informed by the findings from construal level theory. Thus in particular they suggest that newer risks are likely to be represented as higher level constructs, whereas better known risks, become more concrete and lower level constructs. Therefore, leveraging mental models to impact on the internal representation of risk i.e. make it more concrete, is likely to enhance user understanding of the risk.

I would argue that drawing on construal level theory and hyperbolic discounting to investigate how information security risks are construed and framed in relation to time may be a fruitful line of enquiry in terms of investigating the relationship between psychological distance and perceptions of information security risks. It is suggested that in assessing near risks, individuals' risk perception is likely to be more influenced by the experiential mode (*System 1*) whereas in relation to future information security risks, individuals' may be more likely to switch to a more analytically-oriented approach (*System 2*).

2.11. Mental models of information security risk

Tam, Glassman & Vandenwauver (2010) have also drawn on construal level theory to inform their research in exploring the classic trade-off between security and convenience. They explicitly associate between higher level, abstract construals, or mental models, of the distant future and the tendency therefore to focus on the *"desirability"* of that event, compared to lower-level construals in the near future, which due to the emphasis on concrete details might imply "*feasibility"* issues. The researchers specifically examined the variables of feasibility (convenience) and desirability (security) in relation to password management via a web-based survey which required participants to elicit their motivation in relation to five password management actions or behaviours.

In relation to the time hypothesis, they found that giving participants more time resulted in stronger passwords (Tam et al., 2010) They also found that participants who favoured security above convenience are more likely to generate stronger passwords. The researchers hypothesised that those who preferred security above convenience and vice versa would demonstrate different individual risk-taking propensities. However, this hypothesis was not supported (Tam et al., 2010) suggesting that when it comes to evaluating the drivers that influence security behaviour, individual risk profiles may be less influential than usability.

Although Tam et al. explored the trade-off between convenience and security they did not explicitly consider perceptions of risk, aside from the risk propensity hypothesis (Tam et al., 2010). It would therefore be potentially fruitful to consider how employees' perceptions of information security risk and subsequent security behaviour manifests when time is a factor.

Asgharpour, Liu & Camp argue that to improve information security compliance, it is essential to reconsider approaches to risk communication using mental models in order to influence users' perception of risk (Asgharpour, Liu, & Camp, 2007). Asgharpour et al. posit that a mental model is an internal representation of how the individual conceptualises the way something works and can be leveraged to communicate risk more effectively. The benefit of mental models is that whilst they do not provide a complete picture of how something works they do offer a simplified version that can help enable the user better conceptualise and therefore identify and respond to information security risks (Asgharpour et al., 2007).

Asgharpour's research demonstrates that mental models found in the existing security literature suggest that non-experts and experts have developed different models of security. However, it is important to remember that although the authors looked at models relating to security it was not explicitly applied to *information security*. Nevertheless, generalising their findings to an information security context, Asgharpour et al. (2007) recommend that models should be based around non-expert representations of information security risk to improve the clarity of risk communication efforts.

Within the information technology literature - and specifically the context of online gaming - positive relationships have been demonstrated between *perceptions of risk* and *intangibility*. In particular, researchers have identified that making products and services more tangible enhances the users' risk perception by making the threats more discernable (Chen, Lee, & Wang, 2012). Developing mental models of information security risks for non-experts could therefore be perceived as a way to influence perceptions of security risk by making it more tangible and comprehensible. Further, it has been argued that users may not identify online risks at all and therefore steps to provide users with a more concrete model may be likely to better influence risk perception (Blythe, Camp, & Garg, 2011). They suggest that research has shown that users find physical mental models easier to recall, thus it could be reasoned that making information security risks more tangible i.e. more concrete, less abstract, is likely to enhance user understanding of cyber risks (Blythe et al., 2011).

2. 12. Measuring risk perception: psychometric approach

This section provides an overview of the psychometric approach of measuring risk perception. An influential approach to studying perceptions of risk is the psychometric paradigm which has been applied mainly to offline risks in the psychological literature. The development of the psychometric model was influenced by personality theory in that it was an attempt to delineate and measure factors associated with risk (Nyshadham & Minton, 2013). The model consists of various scales or dimension and within each scale participants were required to rate various hazards from technological to man-made risks (Sjöberg, 2000). Mean ratings were derived from each hazard, and the hazard and scale variables were then factor analysed to produce the key dimensions (Sjöberg, 2000). From this, Fischoff developed a 9-dimension framework which has been widely used, these included: "*voluntariness of risk", "immediacy of effect", "knowledge about risk to exposed individuals", "knowledge about risk to science", "control over risk", "newness", "chronic-catastrophic effect", "common-dread effect" and "severity of consequences*" (Fischoff, Slovic, & Lichtenstein, 1978).

This psychometric paradigm has been adapted for use to measure risk perception within the context of information security (Farahmand, Atallah, & Spafford, 2013). They presented their theoretical framework which they suggest explores the cognitive aspects of risk such as *consequences* and also the more affective aspects of risk which they associated with *understanding* (Farahmand et al. 2008) They condensed the nine dimensions, identified by Fischhoff et al. (1978), into two key clusters; *understanding* (comprised of familiarity and experience) and *consequences* (comprised of scope, duration and impact) reflecting the participants' experience of risk perception and security incidents. The understanding cluster was split into 6 levels of understanding with 6 being the lowest level of understanding and 1 the highest. What is of particular relevance about the model here, is that perception of risk is quantified by a higher score which occurs when understanding decreases but consequences increase (Farahmand et al., 2008). The emphasis on consequence is apposite since the impact of personal consequence on risk perception has been demonstrated in the literature (Sjöberg, 2000). The framework also includes a time element; which is of relevance since time has been shown to impact on risk perception as people may revert to *System 1*-type processing under time pressure.

Although Farahmand et al.'s (2008) conceptualisaton of risk perception encompasses consequence and understanding such that risk perception is presented as a function of these two variables, it does not explicitly measure the impact of affect on this relationship. They do attempt to integrate information from both the affective and cognitive aspects of risk perception however via gathering information through questions about understanding the risk event and perceiving the ramifications of consequences respectively.

Huang, Rau, & Salvendy (2010) attempted to investigate the factors that influence individuals' perception of twenty-one information security threats and identified six clusters which included knowledge, impact, severity, controllability, possibility and awareness. Out of these six, the "*most* *perceived overall danger of different threats*" included severity, impact and possibility. The researchers also found a significant result in terms of individual's perception of information security related to the "*types of loss*" or the particular consequences associated with the threat (Huang, Rau, & Salvendy, 2010). This widely-used framework has also been extended to incorporate online risks as demonstrated by Garg & Camp, who used this approach to inform their own 4-dimensional framework in the information security literature (Garg & Camp, 2012). They found that the most significant dimension was "*temporal impact*" which included new risks and dread. This finding echoes the framework developed by Farahmand et al. (2008) who included a temporal component to understanding employee risk perception. Garg & Camp (2012) acknowledge, nevertheless, that the study does not explore how the cognitive bias of availability and affect may impact on risk perception, which was beyond the scope of the research.

Nyshadham & Minton (2013) note that - although two dimensions explained most variation in the magnitude of the consequences of risk and unknown risks - the emphasis has moved to consider affect and *feelings* associated with *dread risk* which has since become more salient in understanding risk perception. Their findings support the idea that the affect heuristic may be an important driver in better understanding how risk perception is influenced. Clearly, the role of affect is a key factor to explore in relation to information security risks.

2.13. Factors that influence risk perception

2.13.1. Social Communication

This section will briefly summarise the impact of social communication on risk perception.

Intuitively, it seems highly probable that social discourse is likely to have an impact on how different stakeholders perceive risk. Research (Renn & Benighaus, 2013) indicates that in attempting to make a judgment about various broader technological risks, individuals are influenced by others' views which directly influences their evaluation of the risk. Renn et al. (2013, p.296) refers to Luhmann highlighting that risk is also influenced by aspects of "*social communication*" as well as personal experience (Luhmann, 1990). Weirich & Sasse (2001) showed that "*pretty good persuasion*" can improve passwords users choose, and argue that this finding could be applied to improve users' behaviour in terms of other security mechanisms (Weirich & Sasse, 2001).

Employees who do not have *personal experience* of problems associated with information security and are not exposed to discussions around information security however may not perceive the risks. Conversely, in an environment where an individual may have personal experience of information security risks, they are likely to have an increased awareness of such risks.

Another framework by which to understand risk perception is the *Social Amplification of Risk Framework* which postulates that "*hazardous events*" are influenced by social, psychological, cultural and institutional processes which in turn, impact on public perceptions of risk (Kasperson et al., 1988). Risk is represented as a signal which is "*amplified or attenuated"* by factors in the environment such as the media and also individual communication (Kasperson et al., 1988, p.177). Knowles et al. suggests that the impact of the media can enable perceptual factors such as the availability bias which, in turn, may distort individuals' risk judgements as they may conflate ease of retrieval with how important the recalled item of information is (Knowles et al., 2012).

2.13.2. Heuristics, biases and risk perception

Several perceptual factors that impact the subjective perceptions of risk have been shown to impact both experts and non-experts and will be summarised in the following section. These include loss aversion and descriptive theories of risk such as *prospect theory, representativeness, availability, familiarity* and *optimism biases*. These broad findings will be extrapolated to information security risk perception.

2.13.3. Normative and descriptive models of risk

Research has demonstrated individuals often don't necessarily behave according to normative, economic models in analytically evaluating risks according to criteria such as "*severity*", "*acceptability*" and "*likelihood*" (Song & Schwarz, 2009). Song & Schwarz (2009) note that empirical research has demonstrated that individuals' risk perception may not always consider probability fluctuations, for instance. One of the key findings from the later version of *prospect theory* (Tversky & Kahneman, 1992*)* that is salient to risk is that the “*decision weights*” that people attribute to outcomes are not the same as the probability of the event (Kahneman, 2012). So, for instance, events that are less likely to occur may be overweighed because of the *subjective* value an individual assigns to that event. Kahneman (2012) also notes that individuals tend to associate values of gains or losses with wealth fluctuations, rather than focusing on the actual amounts lost or gained. Hence, Tversky & Kahneman's suggested that individuals demonstrate a “*four-fold pattern of risk*” which predicts “*risk aversion for gains and risk seeking for losses of high probability*” and “*risk seeking for gains and risk aversion for losses of low probability*” (Tversky & Kahneman, 1992, p.297). In other words, perceptions of the gain or loss associated with the event as well as the decision weight assigned to the event outcome (or consequences) has been empirically demonstrated to skew risk preferences and influence behavioural responses to risk in specific ways. Schroeder notes however that the findings from prospect theory may not wholly describe the patterns of risk perception within an information security context since applying observations from prospect theory offline to online contexts may not be useful (Schroeder, 2005). They did report a modest finding nevertheless that negatively framed scenarios did imply an increase in risky behavior.

Framing effects have been systematically demonstrated when problems or scenarios that are equivalent to each other, but are presented within the context of a loss or gain frame, yield systematically different preferences (Tversky & Kahneman, 1981). For example, when equivalent options are framed positively, there is a tendency to prefer a risk averse approach, conversely when options are framed negatively the results suggested that individuals demonstrate a preference for risk taking (Tversky & Kahneman, 1981). Researchers indicate that framing effects may be less pervasive at the level of the individual, instead suggesting that *affect* may also influence risk perception and risk decisions (Seo, Goldfarb, & Barrett, 2010).

2.13.4 Representativeness and availability heuristics

Early research by Kahneman and Tversky (1972) identified a heuristic referred to as *representativeness* where individuals tend to make probability assessments based on the similarity of the event compared to the general category of the "*parent population*". The authors suggest that people ignore the "*base-rate information*" and tend instead to make risk judgements based on similarity (Kahneman & Tversky, 1972). The problem with this is that it may lead to misconceptions about the likelihood of events; that is, if an individual thinks an event is representative of something else they might conflate the two events which could skew their assessment of risk.

The *availability heuristic* is another cognitive shortcut, identified by Tversky and Kahneman (1973) that can potentially lead to misperceptions about probability and therefore risk estimates. They suggest that *availability*, which is the ease to which an example of something is brought to mind, may inflate perceptions of risk. For instance, if an event is recalled easily because it is 'front of mind', then the individual may unwittingly conflate ease of recall with estimates of risk (Tversky & Kahneman, 1973). The *availability heuristic* may be impacted by affect, as emotionally-laden events for instance may be distinctive and therefore easy to recall (Slovic et al., 2004).

In summary, the research is mixed in relation to availability effects on risk perception. Sjöberg and Engelberg have disputed the extent to which the availability heuristic is responsible for altering risk perceptions (Sjöberg & Engelberg, 2010) In their experimental study, they showed participants entertainment movies to test whether the availability heuristic would impact on risk perceptions, however they found no such effect (Sjöberg & Engelberg, 2010).

Notwithstanding, in relation to individual's perception of risk in particular, Jackson et al. (2006) highlighted how judgement biases such as availability and representativeness might be insightful to explore in terms of further research. In general, vivid events are easier to recall and retrieve (*availability*) which may have implications for assessments of probability, such as amplifying individuals' estimated likelihood for negative events. If the person thinks the consequences of an event is sufficiently impactful, they may find the event easier to recall which, in turn, may influence on perceptions of risk. A practical example of this within an information security context would be security messages disseminated in the workplace which may be 'front of mind' due to repeated exposure or impactful delivery. Certainly, other researchers within the information security literature have identified the availability heuristic as one of the most important factors influencing risk perception since exposure to negative events can inflate perception of threats (Knowles et al., 2012).

2.13.5. Familiarity and risk

Extending the literature on "*risk as affect*" Song & Schwarz (2009) explored the impact of familiarity on risk perceptions, specifically examining whether the fluency with which a stimuli might be processed impacts on lay perceptions of the level of risk. Interestingly, their research indicates that individuals are more likely to perceive unfamiliar or "*disfluently processed stimuli*" as posing a higher risk than "*fluently processed stimuli*" (Song & Schwarz, 2009, p.138). Moreover, Song et al. (2009) found that this effect was evident for both risks associated with positive and negative risks.

In considering perceptions of information security risks, Song & Schwarz (2009) research might be particularly useful to consider since the researcher highlight that "*disfluent*" material, i.e. material that is difficult to pronounce for instance or difficult to read, might serve as a warning to individuals perhaps to not install a piece of software that is unverified for instance. The unfamiliar quality of the stimuli may interrupt the automaticity associated with fluidity of the experiential judgment of risk. Conversely, it is suggested that the risks associated with employee security shortcuts may be downplayed if they are familiar and regularly performed

2.13.6. Optimism bias and information security risks

Optimism bias refers to an individual's tendency to underestimate the risk or likelihood of an adverse event happening to them (Slovic, 2004, p. 986). Weinstein highlights that optimism bias tends to be strongest for events that individuals' do not have much experience of, and for events that have a low probability of occurring (Weinstein, 1989). In his study on *unrealistic optimism* in relation to health issues, he found an optimism bias where individuals considered they were less likely to be vulnerable to health issues compared to their peers. This effect was demonstrated across age, gender and occupation. One of the key findings from this particular study was that in relation to hazards, individuals were inclined to believe that if the issue or potential threat had not yet surfaced, they were not susceptible to such risks in the future (Weinstein, 1987, p.496).

If an individual tends to base future prediction of risk on past personal experience, and their past experience is positive, then it is logical to suggest that they will discount any future risks. In relation to information security risks, this finding has relevant implications, especially if an individual within an organisation has not previously encountered particular problems or consequences associated with their security behaviours, this research suggests they may be inclined to downplay security risks.

As previously mentioned, *optimism bias* features in the general risk literature as a variable impacting on perceptions and assessments of threats, such that individuals have a tendency to minimise the risk of a negative event happening to them when compared with their peers (Weinstein, 1989). This bias might be usefully applied in exploring security managers and employees attitudes to information security risk, particularly when considering individuals' perception of their vulnerability to security threats. In line with the literature, it might be hypothesised that individuals with high optimism bias may consider they are less vulnerable to security risks than their peers for instance.

In their recent paper, Rhee, Ryu & Kim (2012) considered "*unrealistic optimism*" in relation to information security risk perceptions hypothesising that information security managers demonstrated an optimism bias in their perception of information security risks. They note that their research evolved out of an observed disconnect in the information security domain; they observed that whilst there was acknowledgement of potential risks there was little willingness to address the issue. They associated optimism bias with a "*perception of personal invulnerability*" which may act as a mechanism to distort assessments of personal and organisational risk. Their research incorporated social comparison theory and suggested that "*comparative optimism*", that is whether individuals considered themselves more or less vulnerable to information security risks when comparing themselves to others, was in evidence (Rhee et al., 2012).

2.13.7. Confirmation bias

Taleb argues that the tendency to confirm evidence, known as confirmation bias (Nickerson, 1998) rather than falsify in the Popperian tradition, leads them to make "*black swan"* type errors (Taleb, 2010). He finds further support for his argument by referring to the deductive abstract reasoning test known as the Wason selection test (Wason & Shapiro, 1971) demonstrated that when faced with a reasoning task, most individuals would seek to confirm the rule rather than *disconfirm* (Taleb, 2010).

Performance on the Wason task also been demonstrated to improve when the reasoning task is contextualised within a more concrete form. For instance, researchers have found that embedding the task within a realistic context with a rule such as *"if a letter is sealed than it has a 50 lire stamp on it"* elicited at least one answer that was correct from 22 out of 24 participants, compared to 7 out of 24 presented with the abstract version of the test (Johnson-Laird, Legrenzi, & Legrenzi, 1972). Similarly, Wason & Shapiro presented the task as a contextualised rule; they found that 10 out of 16 participants solved the reasoning task in the thematic group whereas 2 out of 16 participants terms was used to capture the hypothesis that context could have an impact on logical reasoning performance (Wason & Shapiro, 1971).

Extrapolating these general findings from cognitive science to information security may be beneficial in understanding more about security risk perceptions. Firstly, that people's natural tendency to look for evidence to confirm hypotheses may mean that security threats that have not occurred previously may not be considered or that there are no visible consequences of a security breach and therefore it is assumed that such a breach has not occurred. Secondly, the matching hypothesis may be useful for security managers to consider in relation to risk communication; employees may be looking for specific security vulnerabilities because they are primed to via security policy for instance, but understandably unaware of what is *not* mentioned on the policy. Thirdly, contextualising security information and information security policy from abstract language to a more concrete or realist style may potentially improve the efficacy of risk communication.

It should be borne in mind however, that these are lab-based experiments and are not situated within a real-world context which is one of the drawbacks of applying this research to other domains - such as employee perception of security risks in organisations (Chamberlain, Crabtree, Rodden, Jones, & Rogers, 2012). Conducting research and collecting empirical data within the context of an organisational culture and using employees in their work environment, rather than student participants in a lab setting, is likely to have an impact on employee risk perception and security behaviour. Consequently, it should *not* be assumed that these findings on psychological perceptions of risk will necessarily be replicable within an organisational setting.

2.13.8. Rare and unknown risks

Another challenge in relation to risk, is understanding how individuals perceive risks that relate to events that are highly unlikely to occur, indeed, that they may not even have been considered, nevertheless carry a severe consequence. Conversely, Taleb also refers to an event that is extremely likely and predictable, yet doesn't take place, as a "*black swan*" (Taleb, 2010). Major unexpected security breaches might be categorised in this way.

Elahi's research on risks may be usefully applied to security risks, since the author argues that the *unrecognised sources of ignorance* - signified on ancient maps as "*here be dragons"* - may be edited out by "*institutional frameworks*" and "*human psychology*" (Elahi, 2011). In other words, organisations and employees may be unaware of aspects of security behavior within the organization. Elahi's *unchartered territories* might be relevant here in distinguishing between employee, managerial and organisational perceptions of security threats and risks. The organisation may not know what employees know in relation to security policy and associated consequences and risks, equally employees may not know all of the security risks that executives are exposed to. Equally, employees and the organisation itself are also likely unaware of a range of external threats to the organisation that present unknown risks.

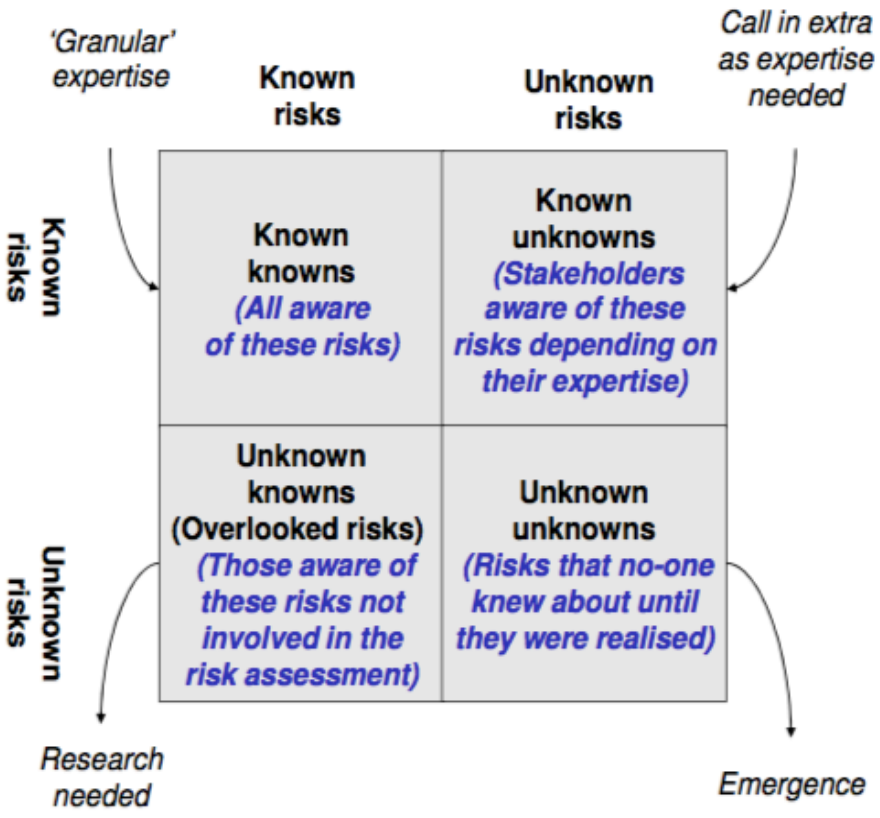
'Granular' expertise
Known risks
Unknown risks
Call in extra as expertise needed
Known risks
Unknown risks
Known knowns
(All aware of these risks)
Known unknowns
(Stakeholders aware of these risks depending on their expertise)
Unknown knowns
(Overlooked risks)
(Those aware of these risks not involved in the risk assessment)
Unknown unknowns
(Risks that no-one knew about until they were realised)
Research needed
Emergence

Figure 1: Risk Criteria – (*Figure by Danny Dresner)
(Figure reproduced from Danny Dresner's unpublished PhD thesis)

In order to explore how individuals respond to unknown online risks, Wang and Nyshadham identify four states to conceptualise uncertainty as a way of classifying levels of knowledge concerning online risks which include: "*known certainty*", "*known uncertainty*", "*unknowable uncertainty*" and "*unknown uncertainty*" (Wang & Nyshadham, 2011) which they developed from Chow and Sarin's framework (Chow & Sarin, 2002). Their assertion that "*unknowable uncertainty*" - which refers to missing information that can be accessed by another individual - is positioned in a hierarchy of preference between "*known and unknown uncertainty*". The researchers hypothesise that missing information, especially when it can be accessed by another, positively affects the perceived attractiveness of a given option or risk (Chow & Sarin, 2002).

Similarly, Alfawaz, Nelson and Mohannak (2010) classified four different states of information security behaviour, based on employee knowledge of the security rules and security skills which included i) *not knowing-not doing*, ii) *not knowing-doing*, iii) *knowing- not doing* and iv) *knowing-doing*.

As discussed, this research attempts to build on Alfawaz et al's framework by mapping the existence of security behavior that may not be visible to the organization. Alfawaz et al., (2010) did not examine risk perception in their study, but rather focused on the relationship between individual knowledge, values, skills, information security awareness and behaviour (Alfawaz et al., 2010).

2.13.9. Control

Ellen Langer's work on *illusion of control* relates to an individual's above-average expectation of success in situations dependent on chance (Langer, 1975). Rhee et al. explored "*perceived controllability*" in relation to information security threats arguing that the level of control an individual believes they have, is likely to influence their perception of the threat. They suggest that if an individual believes they have higher control to mitigate security threats they are likely to "*adjust down*" or minimise their perception of the risk (Rhee, Ryu, & Kim, 2005). This notion of adjusting down potentially links to Adams' (1995) risk thermostat, which postulates where individuals are to exhibit a "*balancing behaviour*" they adjust the risk experience to a level of risk tolerance that they find acceptable (see *Chapter 2.5: Types of Risk*) .

2.14. Limitations in the risk perception literature

As mentioned above, there is a plethora of literature on risk perception within the fields of psychology and decision-making, whereas research within the domains of the information security literature exploring risk perception and its relationship to information security behaviour is somewhat limited. This section will briefly outline some of those limitations.

2.14.1 Ecological validity

Firstly, as already mentioned, there are issues around applying the findings from psychological research on risk that has been carried out within an experimental, lab setting (Chamberlain et al., 2012). Certainly, the ecological validity of some of the psychological lab-based studies may be questionable as they are not conducted within an organisational setting (Chamberlain et al., 2012) and further, do not take into account the influence of organisational culture on security behaviour. This is a major flaw as understanding employee risk perception and information security behaviour necessarily needs to take into account context and organisational factors.

2.14.2. Web-based surveys

Another key drawback within the information security risk perception literature has been the use of web-based surveys rather than conducting research in the wild. For instance, one study collected data via a web-based survey using *hypothetical* questions about risk perception and security behaviour, which do not always reflect actual behaviour (Takemura & Komatsu, 2013). As Acquisti has identified there is often a "*dichotomy*" between actual behaviour and stated intention, which survey instruments that profile preference may not surface (Acquisti & Grossklags, 2003). For instance, (Sheng et al., 2010) used a web-based survey methodology incorporating a role-play to assess susceptibility to phishing behaviour. A key limitation of this and similar studies is that when the consequences measured are not personal to the participant, the results may not reflect how people actually respond in real-life situations.

Therefore, one of the key strengths of this thesis is that the interview data has been empirical in nature exploring actual security attitudes and behaviours, collected within organisational settings and using employees as participants, rather than students for instance. These research decisions have been taken in order to mitigate some of the weaknesses of lab-based or student-population oriented research.

CHAPTER 3: AFFECTIVE RESPONSES TO SECURITY AND UNDERSTANDING OF INFORMATION SECURITY RISKS

This chapter outlines the interplay between affect and risk perception in relation to information security behaviour. From the literature review on the psychological and decision-making risk literature, affect emerged as a key factor in driving perceptions of judgement and risk.

Firstly, it is necessary to define what is meant by affect. Defining affect is problematic as it is conceptualised in various ways in the literature. As discussed, Slovic et al. (2007) define affect partly as a "*feeling state"*, a quality of "*goodness*" or "*badness*" as well as a positive or negative response towards a given stimulus. Fishbein and Ajzen (1975) characterised affect in relation to a positive or negative dichotomy, and also used the term interchangeably with "*evaluation*" (Fishbein & Ajzen, 1975, p.11). Van der Pligt et al. (1998) considered affect as a component of attitude – behaviour models, suggesting that *anticipated* post-behavioural affective reactions influence future behavioural preferences. Similarly, researchers have found affective responses to be predictive of political preferences for instance (e.g. Abelson, Kinder, Peters & Fiske, 1982).

As discussed, in the literature review, the "*affect heuristic*", as it is referred to, is a cognitive process which acts as a shortcut in judgement and decision-making, where emotion is the guiding factor in the process (Slovic et al. 2004). This shortcut enables the individual to make risk assessments automatically for instance, based on how they *feel* about the stimulus. Similarly, the "*risk-as-feelings*" hypothesis, suggests that automatic, emotional responses to an event may influence estimates of risk more vividly than analytical evaluations (Loewenstein et al., 2001). Specifically, research has demonstrated that how individuals *feel* about events and their associated benefits directly influences their automatic risk assessments and reflects in their subsequent choice or behaviour.

In the context of this research exploring affect in relation to security behaviour, affect is considered broadly, encompassing; i) positive and negative attitudes towards a given stimulus (in this case security), ii) positive and negative feelings and/or emotional responses towards security that the individual may or may not be consciously aware of iii) positive and negative evaluations/behavioural preferences associated with security.

One insight from the research is that affect may be used to help people better understand the security risks. For instance, Shepherd et al. (2013) propose that in order to mitigate against incorrect risk assessments, *affective* feedback via online warnings may help users recognise the security risk and respond accordingly by changing their behaviour in some cases. Information security research has shown that warnings are generally ineffective in relation to changing users' behaviour in part because users become desensitised to warnings and fail to understand them (Felt, Ainslie, Reeder, Consolvo, Thyagaraja, Bettes, Harris & Grimes, 2015). *Affect* on the other hand has been demonstrated to influence individual risk perception, which in turn may impact security behaviour.

When considering information security risks for instance, individuals may downplay the likelihood of potential incidents and opt for the preferred choice when they perceive the benefits to be positive. For instance, an employee may download software from the internet because they judge a certain application may make their workload easier thereby eliciting a positive emotion. Conversely, where events are associated with negative affect individuals may see that option as risky and be less inclined to engage in that (Finucane et al., 2000). For instance, an employee may not adhere to a particular security task, such as accessing documents from a work repository, because it is low on usability in that it is complicated to use and takes too much time. The negative affective response from engaging with that particular security task may lead to the employee avoiding it in the future. As Finucane et al. (2000) suggests, feelings play an integral part in influencing risk assessments, in that preferences may be associated with lower risks. In this example, the employee may choose to downplay any risks associated with the easier option of emailing the document to their personal account because accessing the unusable repository gives rise to frustration (negative affect).

The *affect-as-information* hypothesis (Clore, Gasper, & Garvin, 2001) offers evidence that decision-making is *directly* impacted by what we do (positive affect) and do not like (negative affect). Clore et al. propose that "*emotional* *feelings are representations of unconscious appraisals, so that they are appropriately experienced as information about (one's view) of those appraisals*"(p.5). Hence, the experiential component of affect is central to this hypothesis or approach; it is not enough to *think* attributes related to a target are positive or negative, but that we *experience* them as such. The difference between the "*affect-as-information"* (Clore et al., 2001) hypothesis and other models linking affect and risk assessments, is this emphasis of the *direct* impact of affect on cognition, rather than being mediated by memory for instance.

Relating this to another real-world information security example, if an individual wants to download a particular file necessary for their work, but are aware that the security policy restricts downloading of files from the internet, they may rationalise their decision and downplay the risks by convincing themselves that the risk is minimal or that they are entitled to do it:

> *"I think work packages are restricted…but I've got admin rights. Yeah, I mean I've downloaded stuff …which I need as a tool…Yes, I can download stuff, that's fine because I draw up firewalls." (P.122, Company B)*

This action suggests a rationalisation or discounting of risks, where the positive benefits of circumventing policy overweight concerns about security risks. This example of a policy workaround is consistent with much of the information security literature which has emphasised that employees tend to prioritise their *primary task* at the expense of secondary tasks (Pfleeger et al., 2014) particularly if the security tasks are too burdensome or not aligned with the user's interests (Herley, 2009).

This example is relevant because it positions the user as a rational actor maximising their efforts (Herley, 2009) as opposed to characterising the user's judgement as being '*skewed*' by emotion or affect. Rather than affect being positioned as something that serves only to derail risk judgements, researchers argue that the concept of '*skewed'* risk perception is actually a flawed one because emotion plays a valuable role in informing risk perception. People may contravene security policy not because they like breaking the rules *per se*, but because security tasks may be viewed negatively due to clunky mechanisms and time-consuming processes (Kirlappos & Sasse, 2014). Indeed, in his book *Risk Savvy*, Gigerenzer (Gigerenzer, 2014) argues that the affect heuristic influence on decision-making is not necessarily irrational; emotions for instance have a role to play in risk perception that is *adaptive* for the individual. Integrating both the analytical and experiential modes of thought to form assessments of risk enables an individual to form a more balanced judgement integrating the costs and benefits of the decision.

3.1. Individual differences and the importance of context

It is useful to note that there are various facets of affect which include not only its valence (the degree of positivity or negativity associated with the stimulus) but also the extent or intensity of the arousal experienced by the risk perceiver which impacts on risk assessments. Certainly, these components of affect may be experienced differently across individuals, depending on how they experience and perceive security tasks as well as their level of understanding regarding security risks. Slovic et al. (2004) note that individuals vary in the degree to which they respond affectively to a stimulus depending on the task they are doing and their own individual characteristics. Since the affect heuristic relies on the experiential system (which is intuitive and draws on imagery and metaphors rather than logic and reason), there may be individual differences in relation to the affective salience of a given event. For instance, individuals who encountered a particular hazard are likely to base their risk assessment of that event on their subjective experience (Savadori et al. 2004). Similarly, studies have shown that the public may be more affected by the "*vividness*" or "*catastrophic potential*" of a potential event, whereas experts may consider the expected fatalities for instance (Fischoff et al., 1978).

Additionally, context is all important which is useful to consider in relation to assessments of security risk. Individuals' risk-taking behaviour is not necessarily generalisable across situations since the specific characteristics of that individual such as how they weight affective stimulus, the situation they encounter and the task at hand may all play a part in influencing their assessment of the risks (Blais & Weber, 2006). Blais and Weber (2006) note that according to risk-return models, risk-taking behaviour – an evaluation and also trade-off of benefits and risks – can be different depending on the context, although the individual's *attitude* to perceived risk may be stable across domains.

The DOSPERT questionnaire measuring risk attitudes and behaviour (Blais & Weber, 2006), demonstrates that there are differences in an individual's risk-taking behaviour, depending on their perception of the benefits and risks in a given situation. For instance, an instrument such as the DOSPERT (Blais &

Weber, 2006) may highlight that someone high in risk-taking behaviour on the domain of recreational risks may not demonstrate a similar risk behaviour where health and safety is concerned. An individual's attitude towards perceived risk may be stable across both domains, but behaviour depends on *their* evaluation of the risks and benefits.

Identifying the differences in employees in respect of whether they adopt positive or negative attitudes and behavioural preferences towards security tasks may be of benefit in understanding the relationship between affect and security behaviour. Additionally, it may be helpful to better understand not only the context in which the employees operate in relation to how security fits in with their job roles, but also explore their level of understanding in terms of security risks and how the individual conceptualises the costs and benefits associated with compliance.

There is a tendency for individuals to inversely correlate risk and benefits such that individual tend to down-play the risks for preferred choices and vice versa (Finucane et al., 2000). Similarly, John Adams suggests that individuals engage in a "*cost-benefit analysis*" - the more benefits an individual associates with a risky choice the more likely that individual is to select that option (Adams, 2002). I argue here that this pattern of behaviour has relevance in understanding how individuals perceive engaging in security tasks, which I refer to as a '*risk-benefit'* frame.

The economic argument for why individuals may rationally reject security tasks in favour of getting their job done (Herley, 2009) has been made. In addition, researchers conceptualising effort for security tasks in the form of a '*compliance budget'* (Beautement & Sasse, 2009) highlighted that individuals may have a limit to how much they are willing to invest in relation to security. This theme plays out in the transcripts analysed, for instance:

"P: ...connect it to what the people do every day, because right now people are getting by on the status quo of non-compliance, but if you could inform them that there's going to be changes and it'll be taken more seriously…
I: So ...
P: It's got to be communicated and a lot of people are busy, so you've got to make it worth their time." (P.25, Company A)

Similarly, one employee from Company B highlights the problem with working from home in relation to connecting to the VPN:

"*…if you are working from home…it takes, you know 45 minutes to an hour [to get the VPN to work] and drives my guys completely up the wall, absolutely up the wall because they are technical and they can figure out ways around it, they could set up much better processes and technical solutions to this. It just drives them up the wall."* (P.157, Company B)

This exemplar highlights several themes; i) that difficult technical mechanisms (the VPN) lead to ii) wasted productivity (time; "*45 minutes to an hour*") iii) negative emotion (frustration; "*drives my guys completely up the wall*") which may lead to iv) negative attitudes towards security ("*they could set up much better processes and technical solutions to this*") and v) circumvention or workarounds of security policy to prioritise job tasks over security processes ("*They can figure out ways around it*").

If an employee feels negatively towards security and may see investing time in security tasks as a loss in productivity, they may begin to consider compliance itself a risky option. If they do not see the immediate payback when they have work to do, it can waste time and lead to negative attitudes, feelings and behavioural preferences towards security. Therefore, in such cases, the employee may choose, not to risk their time and mood by engaging in such a security task. If, on the other hand, an employee feels *positively* towards security in the organisation and *security hygiene* is in place, they may therefore be willing to invest time and effort in engaging in security tasks.

Extending the idea that users are rational to reject the burden that security tasks places on them (Herley, 2009), I argue that the act of compliance is *itself* a risk for users. Security tasks can be burdensome and not related to the job-holder's primary task, therefore investing time in an activity that is not perceived as central to one's job can be regarded as a risky option for the user. Reservations towards security based on economic evaluations of security tasks are likely to be expressed affectively via employee narratives about security. These affective attitudes, feelings and behavioural preferences towards security expressed in the interview transcripts will be coded and analysed for the purpose of this research. The primary research aim of this thesis is to delineate *affective* responses to security, as well as an *understanding of the security risks* themselves across various cohorts, to better understand different modes of security behavior.

The following chapter (Chapter 4: *Methodology*) outlines the methodological approaches used to analyse affective responses to security and security risk competence within employees' accounts of organisational security policy/

behaviour. The qualitative and quantitative approaches used within this research will be discussed.

CHAPTER 4: METHODOLOGY

The gap in the information security literature (see *Chapter 1:3*) identified as the focus of this dissertation seeks to explore employee understanding and recognition of information security risks, referred to as *Risk Understanding (RU)*, and affective responses to security which include positive and negative attitudes, feelings and behavioural preferences towards security, referred to as *Affective Security (AS)*. For the purposes of this research, *RU* and *AS* are derived from employee interviews on security behaviour. As discussed in the literature review (*Chapter 2*), much of the research within the information security domain on security behavior uses student participants to inform the research. It is possible that students may not share the same level of concerns as an employee working within an organisation in relation to balancing their primary task with security requirements for instance.

This current research seeks to mitigate this gap by drawing on employee samples from four separate organisational settings and analysing *empirical* data, using a mixture of qualitative and quantitative methodologies. These constitute anonymised interviews conducted within two organisations Company A and B, a utility company and telecommunications company, interviews from two Government departments (Organisation C and D) and a short quantitative survey deployed at Organisation D.

One of the methodological challenges in conducting research of this kind is that people do not always behave as they intend. In particular, asking someone to rate their level of risk awareness associated with a security task for instance will not necessarily capture their assessment of the potential risk, nor does it necessarily predict their behaviour (Blais & Weber, 2006). Instead it may have a priming effect influencing their stated preferences. Moreover, employees may demonstrate a '*self-rating problem'* where they are unable to assess their level of competence regarding awareness and recognition of risks in the work environment, which may be due to lack of competence or else a desire to present themselves more positively (Ehrlinger, Johnson, Banner, Dunning, & Kruger, 2008).

Therefore, it is suggested that measuring espoused affective attitudes, feelings and behavioural preferences and levels of risk understanding derived from accounts of security behaviour within a real-world context is likely to be more accurate than hypothetical scenarios conducted in experimental laboratory conditions. This decision to examine security attitudes and behavior *in context* has informed my research strategy and consequently, I chose to use empirical real-world qualitative interview data to inductively generate research questions and propositions related to each case study. Additionally, I deployed a brief 16-item quantitative survey to validate my findings.

4.1. Case study design

My initial research goal was exploratory in nature to identify and explore the factors related to security risk perceptions from employee interviews on security behaviour, conducted within real-world organisational settings. Specifically, I had two broad (initial) research aims which was to i) understand more about *how* employees' perception of security risks drives security behavior and ii) identify *what* other factors may be of relevance in understanding security behaviour and risk perception. Since the use of case studies are considered to be appropriate in circumstances attempting to answer "*how*" and "*why*" research questions (Yin, 2003), particularly when the *contextual* situation is also relevant to the study, this method of inquiry fitted my research aims. Indeed, Yin defines a case study as " *an empirical inquiry that investigates a contemporary phenomenon with its real-life context, especially when the boundaries between phenomenon and context are not clearly evident"* (Yin, 2003, p.13) which reflects the approach adopted within this thesis.

Another factor in my decision to use the case study as my research approach was the fact I did not want to influence behaviour - as in an experimental laboratory study for instance - but instead identify the emergent factors described by employees when talking about security risks and security behaviour in a real-world setting. As Yin explicates; experimental researchers may seek to "*control*" the context, but the strength of case studies is that the uniqueness of each particular organisational setting is an integral part of the research (Yin, 2013).

As Yin's definition reflected my research aims, I adopted a case study approach to better understand what was happening in respect of affective responses to security and risk perception within the context of specific organisational settings. For the purposes of this research, I have analysed data from four different organisational settings, conducting the interviews personally from two of those organisations, which has allowed me to compare the security culture across these different eco-systems using a simple behavioural framework. The data sources have been primarily interview data from four organisations as well as a brief quantitative survey.

There are many benefits associated with case study research; it facilitates focused inquiry into a specific phenomenon within real-world settings, the relative advantage of this is that it supports the discovery of contextual factors that influence behaviour. There are criticisms associated with the use of case studies nevertheless which include validity issues in respect of external validity or generalisability, internal validity, construct validity and reliability associated with case-study research. I will briefly address each one in turn.

4.2. Generalisability/external validity

Firstly, establishing generalisability or external validity in research is usually framed within a positivist paradigm, where statistical significance denotes *causal* relationships with phenomenon that can be generalised across populations. As such, generalising from case study research has been considered problematic as critics have argued that it is not possible to generalise from single cases (Flyvbjerg, 2006). Flyvbjerg (2006) argues that this "*conventional wisdom*" around generalisability in relation to case studies is "*misleading*" suggesting that case studies can play a valuable role in developing new knowledge, provide critical evidence to reject existing paradigms for instance. Yin (2003) echoes this view, suggesting that case studies can demonstrate external validity via "*analytical generalisation*" rather than deriving generalisablity via statistical significance. It is argued that this research uses case study methodology, producing *analytical* generalisations which have been demonstrated across multiple case studies to produce novel insights to build theory. For instance, this research analyses interviews with SIROs about their affective responses and behavioural preferences to security (*AS*) and understanding and knowledge of cyber risks (*RU*) which could be used to develop existing theory on security behaviour.

4.3. Reliability

Establishing reliability in case studies can be difficult because an in-depth inquiry into a phenomenon within a naturalistic setting may not be replicable elsewhere. Yin (2003) explains however that the emphasis in establishing reliability is not finding the same results in another case study, but rather, to *reduce biases* within the study. To ensure reliability, I used a similar question set across all three case studies, with the exception of the additional SIRO-related questions included in Case Study 3 only. I also used the same methodology including the same two dimensions *AS* and *RU* within the context of the BSG. Therefore, I attempted to standardise the methodologies used by operationalising two key variables within the context of the BSG (Beris et al 2015), across all three case studies in order to maintain consistency of approach.

4.4. Internal validity

The concept of internal validity, although essential for experimental research, is not as appropriate to establish when working with case studies that are not explicitly dealing with causality. Yin (2003, p.36) states that "*internal validity is only a concern for causal (explanatory) case studies*". This research *describes* and *explores* the relationships between *AS, RU* in relation to security behaviour by positioning them within the context of the BSG but does not explicitly state that one event *causes* the other. Nevertheless, the *triangulation* of results, derived from a quantitative survey administered at Organisation D (Study 4), was used to increase internal validity (Barbour, 2001). The items within the survey reflected the four modes of security behavior within the BSG and provided another data source to integrate into the findings.

4.5. Construct validity

Construct validity refers to whether the measures used in the study are appropriate, in other words, whether they measure what they are supposed to measure (Baskarada, 2014). Yin (2003) suggests construct validity is difficult to establish in case study research especially given the potentially subjective nature of the data analysis. Yin (2003, p.36) argues that one of the ways to mitigate against this is to use "*multiple sources of evidence*", I have therefore incorporated this principle within this research. For instance, interview data was collected across four different organisations (Company A and B, Organisation C and D), using distinct employee cohorts but measuring the same two dimensions *AS* and *RU* within the context of the Behavioural Security Grid (BSG). In effect, this provides "*multiple sources of evidence of* *the same phenomenon*" as advocated by Yin (2003) analysing the same two dimensions (*AS* and *RU*) across multiple case studies.

It is important to recognise that the analysis of the interview data may be subject to bias. Specifically, researchers may be subject to confirmation bias (Nickerson, 1998) where they are looking to confirm a particular hypothesis. The BSG had been developed as a conceptual model, thus one of the ways to mitigate against this therefore was to create a coding framework that would guide the analysis. For instance, delineating the *AS* and *RU* dimensions and conducting coding checks between myself and coder 2 were practical steps taken to reduce bias. Further, I recognised that there would be potential biases associated with the interviews. In order to mitigate against the bias of the same interviewer conducting all the interviews, I analysed interview data that had been collected by other researchers as in Company A and B, but also included interview data where I had personally conducted the interviews as in Organisation C and D. In addition, other modes of investigation such as the use of surveys, as in the validation study (Study 4) (see *Chapter 8*), were used to triangulate the data to validate the framework. Further, utilising multiple coders (me and a second coder analysed the data for Case Studies 1 and 2) was a research decision made to potentially reduce the analytic bias of a single coder.

4.6. Interpretivist paradigm

This initial phase of the research, which consisted of *inductively* identifying themes and developing codes to express these themes, positions this qualitative phase within an *interpretivist* paradigm. This interpretivist paradigm draws on the subjective views of the participants to explore their perspectives of security within real-world settings (Wahyuni, 2012). It should noted that qualitative data, positioned within the interpretivist paradigm, can imply different conceptualisations associated with reliability and validity. For instance, in some qualitative research establishing reliability and validity is referred to as establishing "*trustworthiness*" (Lincoln & Guba, 1986). However, since this research uses a mixed method approach, where the *AS* and *RU* scores are quantified, I have chosen to refer to traditional terms in relation to reliability and validity with the appropriate caveats given the qualitative, interpretivist paradigm adopted in the first phase of the project (see *Chapter 5.1.1* for a fuller description of the coding process). This interpretivist paradigm is of relevance when considering issues of inter-rater reliability between coders, since the coders independently selected different aspects of texts and to some degree interpreted the coding protocols subjectively (see *Chapter 6.3.1* for further discussion on limitations of inter-rater reliability in this research paradigm).

4.7. Mixed Method Approach

This methodological approach is referred to as mixed methods since the first stage of this project adopted a qualitative approach in the analysis and coding of interview data and the subsequent development of a codebook. This exploratory phase led to development of codes relating to systems and processes and the identification of key themes; namely around employee competency associated with security risk and employee affective attitudes, feelings and behavioural preferences as drivers of security behaviour. This led to the operationalization of two key variables, *Affective Security* (*AS*) and *Risk Understanding* (*RU*) which were delineated into *Positive, Negative, Strong* and *Weak* sub-categories. (See *Chapter 5.1.1*).

The second stage of the methodological approach used a quantitative approach in developing a simple scoring system to classify the *Affective Security* and *Risk Understanding* dimensions as positive or negative for all three case studies. In Case Study 1 for instance, *AS* and *RU* scores across Company A and B were compared, using Mann-Whitney U tests, to demonstrate significant differences between the two organisations (see *Chapter 5*). Case Study 2 also incorporated both qualitative and quantitative techniques to i) classify the codes using the *AS* and *RU* dimensions and ii) score the *Strong, Weak, Positive* and *Negative* aspects for both the *AS* and *RU* dimensions (see Chapter 6). This process of analysing, coding and scoring allowed me to position the data within the quadrants of the BSG framework. Case study 3 employed the same methodological approach as Case Study 2 for consistency i.e. used a similar interview question set, with the addition of questions focused on the SIRO job role and the same methodological analytic approach (see Chapter 7). This approach took the form of using the existing codebook to code the process variables as well as coding the *Strong* and *Weak AS* and *RU* codes in order to cross validate the BSG results. As a triangulation method, a 16-item quantitative survey was deployed to add further insight to the qualitative data collected for Case Study 3 (see *Chapter 8*).

There are potential benefits to integrating the research findings from qualitative and quantitative strands, to allow for a richer appraisal of the research problem including contradictory findings. Venkatesh, Brown & Bala suggests that a critical realist approach is an appropriate paradigm for mixed methods research because it "*accepts the existence of different types of knowledge*" (p.37). For example, I have used Applied Thematic Analysis which is "*a type of inductive analysis of qualitative data that can involve multiple analytic techniques*" (Guest et al. 2012, p.4) in order to explore the empirical interview data. In addition, I have used basic quantitative approaches to compare *AS* and *RU* scores for instance. Thus, this research project has adopted a 'pragmatic' approach, which draws on abductive approaches i.e. moving between qualitative research (induction) and quantitative research (deduction) in order to offer a "*practical and applied*" methodological approach (Venkatesh, Brown, & Bala, 2013).

CHAPTER 5: CASE-STUDY 1- COMPANY A AND B

5.1. Interview Data Set

The first study I conducted was a qualitative analysis of an existing set of transcripts of interviews with employees from two multi-national organisations, a utility and telecommunications company, referred to as Company A and B respectively. The Productive Security project team at UCL which included Professor M.Angela Sasse, Dr. Adam Beautement, Dr. Simon Parkin and PhD students Iacovos Kirlappos and Kat Krol[1] conducted semi-structured interviews with from employees in Company A and B. The Productive Security team members had carried out a Grounded Theory (GT) analysis of the data, and published in Kirlappos, Parkin papers (i.e. Kirlappos et al., 2013, Kirlappos et al., 2014). However, my research questions (see Chapter 1.4.1) focused on exploring security risk awareness and affective responses to security and therefore I analysed the transcripts using a different methodological approach which expressly focused on these themes (see Chapter *5.1.1 Coding Methodology* below).

The aim of the interviews was to elicit from the employees their thoughts on how security fitted in to their daily jobs. The interviews effectively explored the security behaviour of employees within the organisations. The interview questions encouraged employees to reflect on why they exhibited certain security behaviours in relation to: attitude, culture, risk and security policy (see *Appendix 1: Interview Question set for case-study 1).* These interviews were conducted both face-to-face and in a small number of cases over the

[1] Productive Security Project is a UCL project focused on improving organisational security compliance https://www.riscs.org.uk/?page_id=15

telephone where the location was difficult to access. The interviews were transcribed by an external transcription company.

The semi-structured approach allowed the participant to explore the aspects of their security behaviour that they deemed relevant, since the questions were generally open-ended. For instance, the interviews included questions such as: "*How does security fit into your day*?" and "*what security implications, if any, are associated with you or your colleagues' work?"* which encouraged the participant to share their security experiences without being led into taking any particular perspective. The questions prompted employees to explain their attitudes, perceptions and behaviours towards i) *security policies* ii) *access control*, iii) *clear desks*, iv) *passwords*, v) *storage and removable media*, vi) *labelling of sensitive information and data classification*, and vi) *security communication and leadership*.

5.1.1 Coding methodology – Applied Thematic Analysis

I analysed 93 interview transcripts from Company A and B on employee security behaviour using a qualitative technique called applied thematic analysis (ATA). ATA, as defined by Guest et al. (2012), is a synthesis of "*grounded theory, positivism, interpretivism, and phenomenology*" which is integrated into one methodological approach. Guest et al., suggest that ATA is a practical approach of identifying themes inductively from textual data such an in-depth interview. One of the primary aspects of ATA that separates it from grounded theory (GT) is that it may include quantification of the codes whereas GT does not, hence the reference to positivism. This had the advantage of adding "*analytic breadth*" to the research rather than being purely qualitative in approach (Guest et al., 2012).

The qualitative analysis was carried out using a software package called Atlas.ti[2]. The approach was inductive in nature, where the coding led to identifying patterns in the data which enabled me to use the analysis to address specific research questions that were relevant to my project. Thus, I approached the data set with a set of research questions that related to how security risk perception was narrated by the employees interviewed. Specifically, codes that related to how the employees expressed their understanding of cyber risks as well as their affective attitudes, feelings and behavioural preferences towards security were integrated into the codebook. Saturation was reached fairly early on in the coding process, with similar codebook themes emerging from the transcripts checked by myself and coder 2. This was consistent with other coders who found emergent themes early on in the coding process; for instance, Guest et al. (2006) found that in analysing 66 interviews, the full-set of codes and over-arching themes emerged after coding only 12 interviews. Therefore, I decided to complete the analysis for Case Study 1 using 93 transcripts (out of a full data-set of about 200 transcripts) as the codes and over-arching themes were becoming stable within the codebook (see *Appendix 4*). Refinements were made to the coding and the subsequent development of a codebook emerged as a result of this iterative process. This iterative coding process involved several stages of coding which will be outlined below.

[2] http://atlasti.com/

Initially, I identified key themes in the interview text using ATA after which I re-coded the transcripts to refine the emergent codes. These codes related to technical processes and mechanisms as well as attitudinal and behavioural aspects of security such as affective statements about security and risk perception. The next stage required the input of one other researcher who coded the interview transcripts independently in order to provide a counter-check to my own approach[3]. This counter-check revealed some codes overlapped and attention needed to be paid to code definitions and labels. Subsequently, sessions were then set up to discuss various elements of the process. Firstly, the relevance of the codes and accuracy of the coding was discussed which led to changes being made across the transcripts. Secondly, attention was focused on overlapping codes where various names were used to refer to the same or related attribute, for instance, in the early stages of the coding '*USBs*' were referred to as a code name, this was later subsumed into the '*Data:Storage'* section. Consequently, codes names were revised so that there was consistency in the language used to describe the different themes and attributes. These sessions were held at regular intervals (every 3 to 4 weeks) to check consistency and merge the codes into one cohesive codebook. These sessions were carried out over a period of approximately 10 months. Examples of two codebooks which emerged over a period of 6 months (from June 2014 to October 2014) are included in *Appendix 4* to demonstrate the evolution of the coding process.

[3] A post-doctoral Productive Security researcher, Dr. Beautement performed the task of second coder to check consistency throughout.

The outcome of this process was a codebook of the refined codes. This was an iterative process, whereby new codes were added and removed as additional transcripts were coded. Approximately twenty codes were identified to encompass the key themes and were used as superordinate categories to provide a structure to organise the codes. Eighteen out of the twenty code families included references to processes and technologies and were as follows: *Data, Software, Technology, Laptops, Technical Control, System, Passwords, Remote Working, Clear Desk Policy, Communication, Regulatory Compliance, Education and Training, Access Control, Human Factor, Service, Physical Security, Authentication, Primary Task* (see Figure 2.).

The remaining two codes, from the set of twenty, were related to human behavioural issues such as the employee's competence in respect of risk awareness and recognition of security risks and their espoused affective attitudes, feelings and behavioural preferences towards security. These two codes were referred to as "*Risk Understanding*" (*RU*)*,* which is associated with the extent to which employees recognise and identify security risks in the environment and *"Affective Security" (AS)* which relates to the affective attitude, feelings and behavioural preferences towards security. Both of these two dimensions were developed to express the themes of affect and risk understanding in the text.

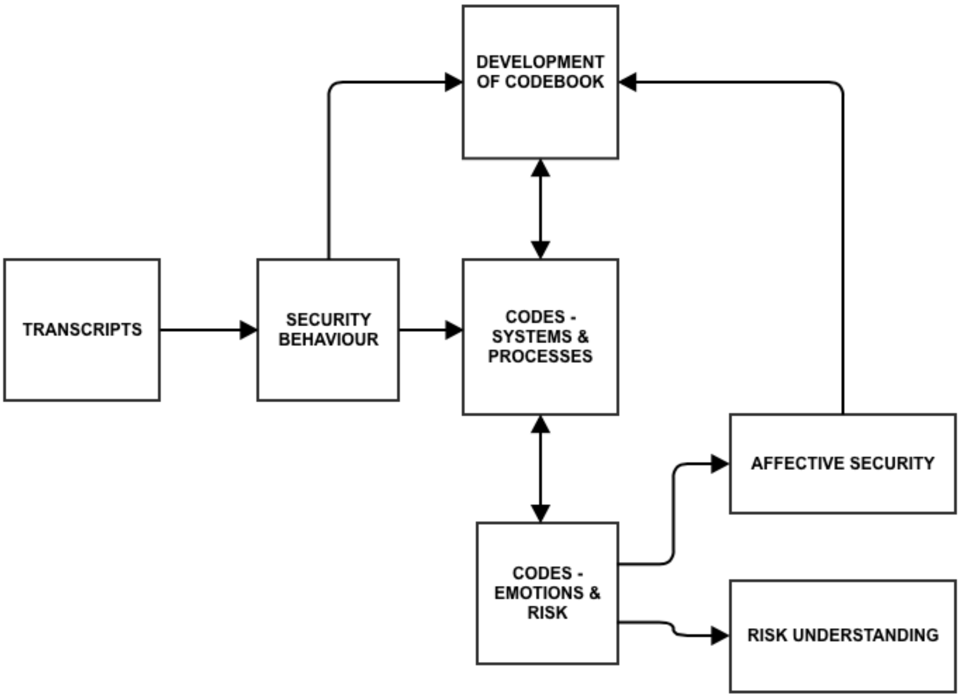

Figure 2: Coding Methodological Process

5.2. Patterns and Themes: Johari Window

As I coded the transcripts, a pattern emerged of the employees' descriptions of security behaviour that linked back to earlier work in the psychological domain, reflecting an existing psychological paradigm the *Johari Window*. Briefly, the *Johari Window* is a grid that highlights interpersonal differences relating to awareness between the self and others (Luft and Ingham, 1955) (See *Chapter 1.4* for a more detailed discussion). The quadrants within the *Johari Window* include *Open, Blind, Hidden* and *Unknown* and the relationship between the quadrants and the observed security behaviour will be outlined as follows.

The descriptions of security behaviour given by the employees were varied in attitude and behavioural preferences. There were instances that were generally positive in that there were aligned with security principles and aware of security risks as well as demonstrating support of organisational security policies. A typical instance reflecting behaviour in this quadrant might be that employees were aware of the risks of leaving their screen unlocked and always ensured they completed this action when they leave their desks. Another example related to physical security was an awareness of the risks associated with tailgating and individuals not being afraid to challenge others if they do not see a badge. These types behaviours could be described as *Open*, reflecting the *Open* quadrant in the *Johari Window* paradigm.

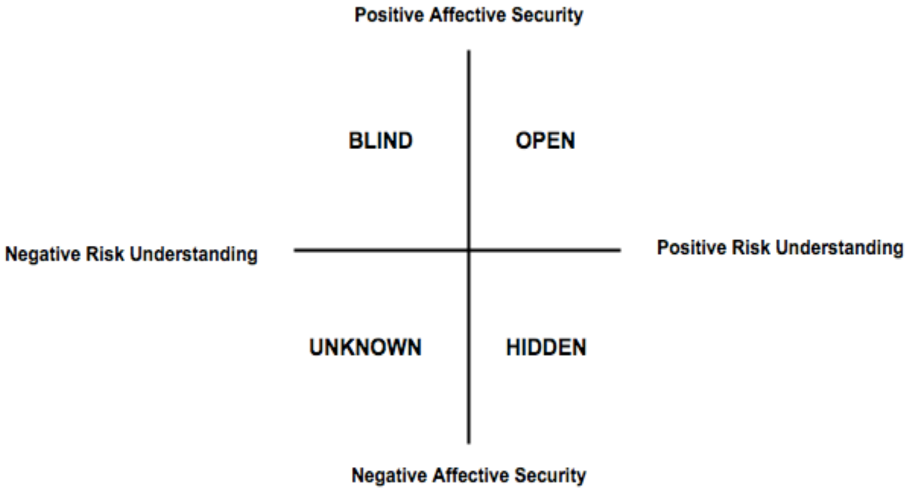
Positive Affective Security
BLIND
OPEN
Negative Risk Understanding
Positive Risk Understanding
UNKNOWN
HIDDEN
Negative Affective Security

Figure 3: Behaviourial Security Grid

Reproduced from Beris, Beautement & Sasse (2015)

This example reflects the *Open* quadrant where the individual is positive about the security provision or policy within the organisation and is mindful and aware of the specific security risks associated with the policy. In this instance, they are aware of the policies their team needs to be mindful of:

"when we're building a project plan, and we're, say we're setting up a relationship with a new vendor, we need to make sure that NDA is clear, that if we're sharing that data, it's clear what the vendor's going to be using the data for, what are the, er, the rules and restrictions around it …… just so there's a certain protocol followed. So that's very top of mind for everyone on my team and it's very clear that, okay, if this is for working with this entity, you know, here's what we need it to follow." (P24, Company A)

Other descriptions reflected different attitudes and behaviours towards security where employees demonstrated awareness of security risks but were not always compliant with security policy – mainly due to frictions associated with their primary role. Sometimes employees described having to circumvent security processes in order to get their job done, and in some instances develop their own set of processes thereby managing the risks in an ad-hoc way. For example, employees talked about having to send documents to their personal email account so they could get productive work done at home as a workaround because using the company laptop and logging on to a shared service was too onerous.

Consequently, this group of individuals may recognise the security risks but engage in *Hidden* behaviour mainly because it enables them to get the job done more productively. I refer to this area as *Hidden,* because it suggests behaviour that is not sanctioned by the organisation and is therefore not always visible. In addition, this label reflects the original Johari Window categorisation (Luft and Ingham, 1955). This area can be a rich source of information for organisations to consider the efficacy of their policy, and if necessary conduct interventions to improve *security hygiene* in the organisation. If security processes are reducing employee productivity and are therefore inducing workarounds the cases identified within this quadrant may bolster the argument to adapt or change the official security process to ensure *security hygiene* is in place.

One example of the *Hidden* quadrant is where individuals engage in circumvention or workarounds of security policy in order to achieve their primary task. The following exemplar from Company B (P157) shows how an employee created a workaround by using a system not authorised by the organisation to technical restrictions to able to achieve their work goals:

P: "Barriers. Ah, it is incredibly difficult to access any of our services if you are not on our…if you are not within the network. Also, to try and launch new products and services it is quite difficult from a security point of view…Yeah it makes mobility really difficult."
I: "…So how do you tackle that? How do you deal with it?"
P: "I deal with it by not using our systems."
I: "Okay, so…what do you use then?"
P: "I use other systems in place".
I: "Are these provided by the organisation?"
P: "No."

Another key pattern that emerged is that some employees were broadly positive about how organisations sought to manage security, but lacked awareness and knowledge of specific security risks. Some of these employees did not realise they were breaching security policy despite having a generally positive attitude towards complying with organisational policies. An exemplar of this sort of behaviour included employees routinely sharing passwords with team members because they trusted their colleagues and consequently did not perceive password sharing as risky behaviour. Another typical example included employees who did not lock their screen because they considered their colleagues were not a threat to security. This quadrant is referred to as the *Blind* quadrant as employees may adopt a positive attitude towards security policies but in reality, do not recognise the risks arising from their behaviour.

This exemplar is taken from Company A and highlights an individual's tendency to downplay a possible security risk, which has been a pattern identified in the psychological risk literature, where an individual may conflate risk assessment and benefits, downplaying risks for preferred options and vice versa. In this exemplar, the employee describes how they share a password with a colleague as they perceive them to be trustworthy and that they can later change the password. They justified their decision to share the password by downplaying the risk:

"…it's that level of security is, is more tight but the person that I work out in the field with… I have some level of trust with them, it's more if they have enough level of trust with me to be "Okay, here's the thing so you can log in and do it quick. I'll change it as soon as I come back so that we're secure and all that …". (P2, Company A,)

From this example, it is clear that the employee does not see sharing the password as a security risk as they overweight the trust they have in their colleague, which reflects low competence around recognition of security risks or *Negative RU*. They rationalise their decision to share the password by suggesting that the fact that the password will be changed again later will mitigate the risks.

Another example around the *Blind* category is where an individual talks about the security culture in the organisation fairly positively, but at the same time does not see the risks of password sharing for instance:

"*Probably sometimes the rules are... are bent to meet the requirements of the job, in terms of if you want to share a password with someone, that sort of thing... yeah, generally people are pretty careful, I think.*" (P58, Company A)

The other quadrant within the *Johari Window* (Luft and Ingham, 1955) is the *Unknown* area, where the self and others have no awareness of behaviour. The *Unknown* quadrant in the BSG is characterised by the existence of organisational security vulnerabilities for which there is neither a policy for or process to mitigate the risk, nor *awareness* of that risk. It is likely that these issues are only identified after the fact: for instance, a virus which has contaminated internal systems may not have been known to the organisation or employees until a security breach was reported. This area reflects employees who hold negative views about *AS* and low competence in relation to *RU* i.e. *Strong/ Weak Negative AS* and *Strong/Weak Negative RU.* A quotation which exemplifies the *Unknown* quadrant includes:

*"Yeah. Fortunately, I think, we never had any big issues, so we were okay***...** *and nobody probably cared." (P4, Company A).*

Although this quote is similar to the *Hidden* sector, this employee seems to imply colleagues hold a negative attitude towards security, in that they do not care if a security breach occurs. Moreover, there is no mention of risks. It is anticipated that this area will be sparsely populated; whilst many employees may not be aware of some risks they are likely to be reasonably positive towards security. The converse is also true; people may recognise the risks but demonstrate *negative affective* responses towards security.

5.3 Coding themes: affect and security risk

The insights from the coding of the interview transcripts from Company A and B suggest risk may be conceptualised in two ways. Firstly, risk can be considered from the employee's *subjective* point of view on engaging in security tasks, associated training etc. For the employee, the act of compliance *itself* might be framed as a risk, since it will likely require their time and effort, which may interrupt their workflow. The affective and cognitive expenditure is likely to influence attitudes towards security, which in turn may lead to a negative attitude, feeling or negative behavioural preferences towards security, referred to here as *Negative Affective Security*. A negative attitude towards security could directly impact risk perception as research suggests.

Subsequently, these two themes form the basis of a research question, in which I proposed that positive and negative attitudes, feelings and behavioural preferences (in relation to security), referred to here as *Affective Security* (AS), and different levels of knowledge about security risks, referred to as *Risk Understanding* (RU) imply different types of security behaviour.

To offer more granular analysis to these definitions, I decided to delineate the *RU* and *AS* codes into 4 elements: i) *Strong Positive*, ii) *Weak Positive* and iii)*Weak Negative* dimensions and iv) *Strong Negative*. The main reason for doing this was to i) reflect the differing levels of evidence expressed by each participant so that strength of preference or knowledge for instance could be captured via a rating scheme ii) position employees within the context of the BSG. I decided not to use a neutral code as it would not provide additional information in respect of identifying the positive and negative direction of the dimensions. I led a discussion and conferred with the second coder in this process to agree on definitions to ensure we were coding within the same parameters.

5.3.1 Risk Understanding and Affective Security codes

As discussed, risk and affective responses to security, operationalised as *RU* and *AS* emerged as result of the coding process. *Risk Understanding* (*RU*) refers to an individual's level of competence, understanding and recognition of security risks in the workplace. *Affective Security* (*AS*) encapsulates the positive and negative feelings and attitudes as well as positive and negative behavioural preferences the individual espouses/demonstrates in relation to security within their organisation. The definition of *AS* in this thesis extends beyond the narrow definition of affect as a purely emotional response, and incorporates a broader model where affect refers to positive and negative feelings, positive and negative evaluations (e.g. Azjen, 1989) as well as preferences related to security and security behaviour (see *Chapter 3*).

It should be noted that security here refers to the security provision in the organisation and/or the security policy. As discussed, for further granularity, I decided to split the codes into *Strong* and *Weak Positive* and *Strong* and *Weak Negative* for both *RU* and AS, with feedback from coder 2 (Beris et al, 2015, p.74 - 76).

They are defined as follows:

i) *Strong Positive RU* codes indicate in-depth to moderate understanding and recognition of security risks, as well as being able to identify the causal factors that relate to those risks.

ii) *Weak Positive RU* codes indicate those who demonstrated some limited awareness of security risks. They may also demonstrate some limited understanding of the causal factors in relation to the risk.

iii) *Strong Negative RU* codes identify individuals who are not aware of the risks, and therefore the absence of reference to risks in a security context might reflect this level of awareness. Alternatively they may fundamentally lack understanding of a risk '*I don't know what the policy is around data management'* etc.

iv) *Weak Negative RU* codes reflect individuals who are not just unaware of risks, but may also have misconceptions about the security risk. An example of this might be the belief that it is '*permissible to share passwords as long as you trust the team'*.

v) *Strong Positive AS* codes reflect narratives that demonstrate positive attitudes, feelings and/or positive behavioural preferences towards security policy or the security provision within the organisation. It implies a willingness to take personal responsibility for security as demonstrated via narratives about security preferences and behaviours. This code might also include a high level of positive language in relation to security.

vi) *Weak Positive AS* codes are used for individuals who demonstrate reasonably positive attitudes, feelings and/or reasonably positive behavioural preferences towards security but may not always take personal responsibility for security tasks. The strength of language for weak positive codes reflect individuals who are quite positive about security but may not express strongly positive views and behaviours.

vii) *Weak Negative AS* codes reflect individuals who may demonstrate slightly negative attitudes, feelings and/or slightly negative behavioural preferences towards security policy or security tasks in the organisation. The may consider security has a purpose within the organisation, but do not necessarily follow policy themselves. They might make excuses about *why* they are unable to adhere to security procedures, alternatively their language may reveal a slightly negative view on security in general.

viii) *Strong Negative AS* codes reflect individuals who demonstrate strongly critical or negative attitudes, feelings and/or behavioural preferences towards security policy or security tasks in the organisation. This may be reflected in the content of their security narrative or else in the strength of negative language in relation to security. They may actively talk about creating workarounds, conscious that they are circumventing security policy. These individuals may view security tasks and following security policy as something that they are exempt from.

All the transcripts were then re-coded using these delineated *AS* and *RU* dimensions. This more granular approach was second coded by another research colleague to check consistency of approach. As previously referred to, I met with the second coder on an ongoing basis to review the consistency of coding and approach and amend the code list over a period of approximately 10 months (see *Appendix 4* for codebook lists).

5.4. Construction of the Behavioural Security Grid (BSG)

The Behavioural Security Grid (BSG) emerged as a way of representing security behaviour in relation to two key themes which were derived from the initial coding process. 1) The first was that affective responses and preferences to security and security risk competence featured as major themes in the coding analysis and indeed, the two dimensions *AS* and *RU* were developed to test this proposition. 2) The second factor was that the security behaviour of the employees, lensed via the *AS* and *RU* dimensions, could potentially be expressed via an existing psychological paradigm called the *Johari Window* (Luft & Ingham, 1955). I selected the *Johari Window* partly because of the four quadrants *Open*, *Blind*, *Hidden* and *Unknown* which would allow for the categorisation of security behaviour and also because it utilised the idea of two axes as a way to distinguish between quadrants. In the original Johari Window (Luft & Ingham, 1955) the quadrants were separated by what is known and not known about the *self* and *others* and has been used as a development tool to aid interpersonal awareness. The BSG leverages the use of the Johari quadrant names, however, the *Open*, *Blind, Hidden* and *Unknown* simply refer to the mode of the employee's security behaviour. The position of the quadrants has also been revised in the BSG model; in that *Open* and *Blind* quadrants were reversed with *Open* on the right-hand side of the grid instead of on the right-hand side. Further the BSG uses *AS* (or emotion) and *RU* (of security vulnerabilities) to build a revised version of the framework for security behaviour so that the *Johari Window* (Luft & Ingham, 1955) became only a starting point for the framework.

In order to explore the proposition that the BSG represents an effective framework to classify security behaviour, I developed, and confirmed via code review meetings with the second coder, a methodology to test whether the attributions employees provided in the interviews, could be categorised within the framework and in relation to the axes of *RU* and *AS*.

5.5. Methodological Approach: Quantification of the codes

In order to locate each employee on the BSG, and test if the framework was functional (in that it reflected levels of *RU, AS* derived from the security interviews) I had to devise a methodological approach to quantify the codes - in particular, to find a tally for each employee that reflected their level of *AS* and *RU* score combined.

For each of the two dimensions i.e. *AS* and *RU*, in order to reflect the differences between strong and weak aspects of the two dimensions, strongly positive scores would be twice the value of the weakly positive scores. The strongly negative scores would be twice the negative value of the weakly negative score. Therefore, I decided to devise a rough heuristic for measuring the different levels of i.e *Strong* and *Weak Positive* and *Negative* for both *AS and RU*, I conferred with the second coder to agree on the following equation to express the differences in levels between the categories within the *AS* and *RU* dimensions.[4] Hence, the following equation captured the relative values between the positive and negative attributes for each dimension:

AS = 2 (strong positive) + (weak positive) – (weak negative) – 2(strong negative)

RU = 2 (strong positive) + (weak positive) – (weak negative) – 2(strong negative)

The rationale behind this scoring was to weight the 'double strength' of strong positive and negative scores appropriately. Obtaining the code tally for *AS* and *RU* enabled me to locate employees on the BSG. As previously mentioned, the scores are ordinal in that they can be ranked over a dataset but are not meaningful in terms of quantitative value. This methodological approach was used as a basis to categorise employees into one of the four quadrants.

5.6 Case Study 1: Results

Affective Security (AS)	**Company A**	**Company B**
Strong Positive	113	342
Weak Positive	147	181
Weak Negative	121	136
Strong Negative	16	32
Total	397	691

Table 1: Distribution of AS Codes for Company A and B

[4] Dr Adam Beautement, as second coder, provided insightful feedback on the relative values of RU and AC and the development of the equation.

Risk Understanding (RU)	Company A	Company B
Strong Positive	119	249
Weak Positive	100	162
Weak Negative	64	72
Strong Negative	10	10
Total	293	449

Table 2: Distribution of RU Codes for Company A and B

The 2 tables above (Figures 1 and 2) show that Company B was apportioned a higher number of codes overall suggesting that both coders identified more examples of *Weak* and *Strong Positive* and *Negative AS* and *RU* in Company B than Company A. The exception to this was *Strong Negative RU* where the number between Company A and B was equal. (The differences in code numbers will be outlined in the section below, see *Chapter* 5.7: *Discussion*).

In order to compare the *Strong Positive, Weak Positive, Strong Negative* and *Weak Negative RU* and *AS* codes between Company A (n=48) and B (n=45) an independent Mann-Whitney U test was conducted. A non-parametric test was selected because the data was ordinal.

4 significant differences were identified between the two groups:

i) **Strong Positive Affective Security:** there is a significant difference between Company A and B, where Company B demonstrates significantly higher levels of Strong Positive Affective Security than Company A (Company A and B means were 35.53 and 59.77 respectively; U = 516, P < 0.05)

ii) **Strong Positive Risk Understanding**: there is a significant difference between Company A and B, where Company B demonstrates significantly higher levels of Strong Positive Risk Understanding than Company A (Company A and B means were 37.63 and 57.43 respectively; U = 619, P < 0.05).

iii) **Weak Positive Risk Understanding**: there is a significant difference between Company A and B, where Company B demonstrates significantly higher levels of Positive Risk Understanding than Company A(Company A and B means were 41.24 and 53.41 respectively; U = 796, P < 0.05).

iv) **Strong Negative Risk Understanding**: there is a significant difference between Company A and B, where Company B demonstrates higher levels of Strong Negative Risk Understanding than Company A (Company A and B means were 42.06 and 52.50 respectively; U = 836, P < 0.05).

The results showed a significant difference in scores between Company A and B across 4 of the codes. There were no significant differences found for *Weak Positive AS, Weak Negative AS, Strong Negative AS* and *Weak Negative RU*. The results demonstrated that Company B has higher levels of *Strong Positive AS, Strong Positive RU, Weak Positive RU* and also higher levels of *Strong Negative RU* compared to Company A. The significant differences for *Strong Positive AS, Strong Positive RU* and *Weak Positive RU* codes suggest that Company B employees may demonstrate a more positive security posture; since both positive aspects of *RU* and *Strong Positive AS* are significantly higher than Company A. This suggestion is only tentative at this stage since further validation of the framework is required since the data-set is relatively small (see *Chapter 5.7 Discussion* below). Further, the results reflect individual employee scores but do not necessarily reflect the larger organisation.

It should be noted that there was a significant difference found in relation to *Strong Negative RU* which was demonstrated to be more prevalent within Company B than Company A. This suggests that gaps may exist in relation to *RU*. This inconsistency within the *RU* scores i.e. significantly higher than

Company A in relation to the *Positive* aspects of *RU* but not *Strong Negative RU*, indicates that the security profile of each organisational cohort may have particular strengths and weaknesses depending on their particular culture. This would be an area to explore further should an intervention be required to improve this area of cyber risk understanding.

5.7 Discussion: Case-study 1

As previously mentioned, the pattern of results indicate that Company B may demonstrate a more 'positive' security posture since they demonstrated significant differences in *Strong Positive AS* and all the positive categories of *RU*. Many of the security stories that emerged from Company A indicated negative employee attitudes, feelings and behavioural preferences towards security because of onerous security expectations. For instance, the example below details how a Company A (P.23) employee develops their own '*systems*' to manage with the numerous passwords they were required to remember – by keeping them on their personal flash drive. This circumvention of security policy is driven by systems that do not support the employee in complying with security policy:

P: "… but, I mean, there's just tons of, of passwords and everybody I know either has a cheat sheet or something written down, all their passwords, because there's just too much to …"
I: "Okay."
P: "… to maintain."
I: "And how do you, er, manage that? Er, do you have to write them all down?"
P: "I keep them on a flash drive, on a file …"
I: "Okay".
P: "… that's like my personal flash drive."
(P.23, Company A)

Similarly, another employee security story from Company A (P9) described how they shared drives with colleagues that did not have the requisite permissions in order to complete their work:

P: *"Yeah, I, um, yeah, I mean when I first started I didn't have permission to all the right areas. Similarly with, we have some shared, just shared drives, just network drives ..."*
I: *"Mmm hmm".*
P: *"... um, for a while [I] didn't have the right permissions to that. But eventually it sorted itself out..."*
(P9, Company A)

These examples echoes the themes that emerged in Kirlappos et al. (2013) – which utilised the same dataset but adopted a different methodological approach – indicating that Company A employees created workarounds, due to lack of appropriate technical mechanisms or lack of access to required systems, driven by a need to complete their primary task.

The *security stories* associated with Company B, on the other hand, generally conveyed a positive orientation towards security and a more embedded security culture; for instance one employee stated: "*...I think our physical security is actually very good."*(P166, Company B). Another Company B employee demonstrated their security awareness around highlighting the importance of conducting conversations about "*sensitive security matters*" in private (P202). Further, many of the themes that emerged from Company B suggested a culture of *empathy* around security, recognising the challenge security practitioners face in attempting to '*secure*' the organisation.

Hence:

"Equally, what I would say to my guys running delivery programs is that people that work in security type roles have a pretty thankless task, right, in that people like me will always consider them to be a blocker until the day we

get a security breach and then it's their head on the block. So I do have lots of empathy for the role...". (P196, Company B,).

These qualitative examples support the quantitative results which found significant differences between Company A and B, where Company B demonstrated significantly higher levels of: *Strong Positive AS, Strong Positive RU* and *Weak Positive RU.* These three codes indicate that strongly positive affective attitudes towards security as well as a positive weak to strong understanding of cyber risks in the workplace are more prevalent within the Company B cohort than the Company A cohort.

Strong Negative RU represents an anomaly in this pattern of Company B demonstrating a more positive security culture, in that it suggests the contrary in relation to this dimension. Instead, it suggests significant omissions around *RU*, reflected in the *Strong* negative aspect of this dimension regarding employee understanding of security risks and competence in identifying such risks within a small part of the Company B population.

There are various limitations associated with this initial case study. Firstly, the 93 interviews analysed were randomly drawn from a larger data set of 187 transcripts from both Company A and B, and therefore not all of the interviews were included for analysis. As discussed, and consistent with other qualitative researchers (Guest, Bunce, & Johnson, 2006) saturation was reached fairly early on in the coding process with the major themes of risk and affect emerging from a relatively small number of transcripts.

Secondly, the aim of this case study is limited in scope in that it sought to compare *AS* and *RU* scores across Company A and B. The purpose was to identify potential differences and similarities in respect of security behaviour across the two employee populations in respect of these two dimensions. Understanding the *implications* of these differences between Company A and B's organisational security culture in terms of diagnosing and planning an organisational intervention is therefore beyond the scope of Case Study 1. (Notwithstanding, identifying the potential for using the BSG as an employee security diagnostic tool as part of a security culture change process will be discussed in the *Further Research section* (*Chapter 9.6*).

Certainly a difference between the two companies was identified using this methodology, suggesting that the BSG may be a useful framework to compare different cohorts across organisations in relation to the four security quadrants; *Open, Hidden, Blind* and *Unknown*. Further research and validation of the BSG is required to test the efficacy of this framework which Case Studies 2 and 3 within this research attempt to address.

The following two case studies involving i) employees drawn from a government body and ii) senior risk owners/ managers (SIROs) from across a variety of government departments will be used to further test and validate the BSG. I will outline these two case studies in the forthcoming *Chapters 6 and 7*.

CHAPTER 6: CASE-STUDY 2 - SECURITY INTERVIEWS WITHIN ORGANISATION C, A GOVERNMENT DEPARTMENT

This case study involved conducting semi-structured interviewed with 20 employees from Organisation C, a public sector Government department, about staff organisational security behaviour and risk perceptions associated with security. The interview question set was very similar to Case Study 1 (see *Appendix 1*) with the interviews being semi-structured in approach, where prompts and follow-up questions were necessarily individualised for each participant. Nevertheless, both the interview approach and methodological approach (see *Chapter 6.2 Methodology* below) was broadly consistent throughout both Case Studies 1 and 2. The one-to-one interviews were conducted by myself as the researcher at the offices of Organisation C, and lasted approximately 40 - 50 minutes.

This cohort of participants was recruited from all levels of Organisation C by a staff member who had been briefed about the study by a senior security manager, and asked to recruit a representative set of volunteers for the interview. I was not informed of the employees' job roles within the organisation. It was agreed with Organisation C that all the data would be anonymised. As discussed, each interview was conducted on a one-to-one basis over a period of 3 weeks in January and February of 2015.

The purpose of the interviews was to gather data on security behaviour, using the same approach as in Company A and B i.e. using the same question sheet (see *Appendix 1*). The semi-structured nature of the interviews allowed me to probe areas that the participant emphasised, rather than following any rigid line of questioning. The aim of this approach was to elicit the *participant's* view of what the main issues were around security and therefore I encouraged them to express their views candidly. I adopted a person-centred perspective in my interview approach, incorporating an empathic and non-confrontational, collaborative approach (Csillik, 2013). In order to ensure the participant felt at liberty to express their honest views about security, a device was used where they were asked to describe the security behaviour of "*fictional colleagues*" (see *Chapter 6.1.1* '*Ethical guidelines'* below).

Consistent with Case Study 1, the analysis of the interviews focused on examining risk perceptions and affective feelings, attitudes and behavioural preferences towards security. The aims were twofold; firstly to locate the Organisation C cohort within the frame of the Behavioural Security Grid (BSG) using the dimensions of *RU* and *AS*. This was achieved via the use of a quantitative methodology outlined in the methodology section below (see *Chapter 6.2 Methodology* below). The second aim was to use the qualitative techniques of applied thematic analysis (ATA) to explore the thematic relationships underpinning *AS* and *RU* in relation to security behaviour within the specific eco-system of Organisation C.

In terms of the research proposition for this case study, I expected that the Organisation C cohort would demonstrate *Positive RU* because the participants were embedded in a department that included security within their job context and therefore "*fictional colleagues*" were likely to be aware of security risks.

I coded affective responses which incorporated positive and negative attitudes, feelings and behavioural preferences towards security, referred to as *AS,* as well as the participants' perceptions, awareness and recognition of security risks, referred to as *RU*. Both *AS* and *RU* were further delineated into strong and weak positive and negative aspects. (The specific definitions for the *Strong, Weak Positive* and *Negative* aspects of the *AS* and *RU* dimensions are outlined in *Chapter 5.3.1*).

In order to build mutual trust and ensure the principles associated with ethical guidelines were upheld, some key principles were agreed with the partner organisation prior to conducting the interviews. These ethical considerations are outlined in the following section.

6.1. Ethical guidelines and safeguards

In order to effectively manage some of the ethical challenges associated with this project, the partner organisation was reassured that the participants' identities would be anonymised. I also took the decision, after consultation with my supervisor, to specifically avoid collecting personally identifiable information from the participants. For example, I did not formally record the full name, email address, sex or age of the participant. Instead, Organisation C (Case Study 2) provided me with a list of willing participants who were identified by their first names only. As contracted with the partner organisation, I did not record first names on the interview transcripts, but instead assigned each participant with a number.

Participants were invited to read an information sheet outlining the research and sign a consent form prior to proceeding. In order to build a trusted environment at the start of the interview, I also explicitly asked each participant not to share any classified information.

Another safeguard, to encourage openness, involved the practice of asking employees to attribute behavioural observations to non-specific individuals, referred to as "*fictional colleagues*" rather than specific individuals, so that they would not incriminate themselves. There were practical reasons for adopting this approach, namely that participants could then be genuinely reassured that they were free to express their views - whether these views expressed their own personal view or behaviours that they had observed in the organisation - without potentially compromising their own position within the organisation. Organisation C has strict policies including sanctions for non-compliance therefore it was particularly important that the views expressed in the interviews could not be traced back to any individual. Employees were invited to discuss the security behaviour and attitudes towards security and security mechanisms of "*fictional*" colleagues that they had encountered. They were reassured that attribution for their espoused view was not a reflection on their *personal* behaviour, but that the purpose of the interview was to identify patterns prevalent in the organisation. This approach had the advantage of enabling the researcher to collate composites of security behaviour to begin to develop security personas for the research that have face-validity in the real world.

To maintain a confidential environment for participants, I did not record the interviews but typed notes. On a few occasions, I checked back with the employees that they were comfortable that notes were made when certain sensitive issues emerged. During one particular interview, the participant asked me to redact one comment they made when I checked whether they were comfortable disclosing that information.

In addition, it was agreed with the partner organisation that in the expected event the case study is referred to in a report or indeed my final thesis, references to the company will be anonymised and individuals referred to by number only. The data was stored on an encrypted drive.

6.2 Methodology

The methodological approach for Case Study 2 is consistent with Case Study 1 (see *Chapter 4*) where the transcripts were analysed using a qualitative technique called applied thematic analysis (ATA) (Guest & Namey, 2012). This technique includes a hybrid of qualitative techniques where themes are extracted and used to create qualitative codes in order to make sense of and organise the data. I had already compiled a codebook from Case Study 1, which included 18 systems and processes codes and 2 main behavioural codes (see *Chapter 5.1.1*). It is from this initial process, the codes of *AS* and *RU* were developed. An additional step within the ATA system is that codes can be used quantitatively in order to broaden the data analysis approach which was used to score the *AS* and *RU* dimensions.

I lead a discussion and conferred with the second coder to identify a method to derive a quantitative score to the dimensions of *AS* and *RU*. Informed by an earlier study (Case Study 1), *Strong Positive* and *Strong Negative* scores were worth twice as much as the *Weak Positive and Weak Negative* scores for both *AS* and *RU*. The reason for this approach was essentially to position participants within the quadrants of the Behavioural Security Grid (BSG), in order to explore the relationship between *AS, RU* and the implied security modes of behaviour (Beris et al, 2015).

The raw scores are ordinal in nature which means that the quantity of each score has no particular value in and of itself, beyond the capacity for each score to be ranked within the dataset. This was a useful heuristic to assign participants to particular quadrants but there are limitations with this approach in terms of validating individuals scores. This is discussed within the limitations section (see *Chapter 6.6.1* below).

6.3 Results: AS and RU Scores for Organisation C

The AS and RU scores, from a analysis of the data from myself and coder 2 for each of the participants is included within Table 3 below:

Participant	AS (1)	RU (1)	AS (2)	RU (2)
1	POS (22)	POS (22)	POS (35)	POS (17)
2	POS (15)	POS (13)	POS (14)	POS (7)
3	POS (21)	POS (21)	POS (13)	POS (12)
4	NEG (-2)	POS (14)	POS (10)	POS (9)
5	NEG (-1)	POS (24)	POS (7)	POS (11)
6	POS (11)	POS (16)	POS (17)	POS (8)
7	POS (2)	POS (4)	POS (2)	POS (3)
8	POS (0)	POS (20)	POS (15)	POS (13)
9	POS (24)	POS (25)	POS (24)	POS (11)
10	POS (12)	POS (13)	POS (9)	POS (10)
11	NEG (-11)	POS (15)	NEG (-4)	POS (8)
12	POS (16)	POS (12)	POS (13)	POS (15)
13	POS (0)	POS (6)	NEG (-2)	POS (18)
14	POS (1)	POS (3)	POS (14)	POS (13)
15	POS (7)	POS (7)	POS (12)	POS (14)
16	NEG (-5)	POS (9)	POS (3)	POS (8)
17	POS (13)	POS (11)	POS (14)	POS (17)
18	POS (17)	POS (30)	POS (28)	POS (26)
19	NEG (-1)	POS (1)	POS (3)	POS (15)
20	POS (34)	POS (27)	POS (32)	POS (9)

Table 3: Table showing Positive or Negative code categories and raw tallies for Affective Security (AS) and Risk Understanding (RU) mapped across the Behavioural Security Grid (BSG) (Coder 1 & Coder 2)

Key:
POS: denotes Positive category, NEG: denotes Negative category

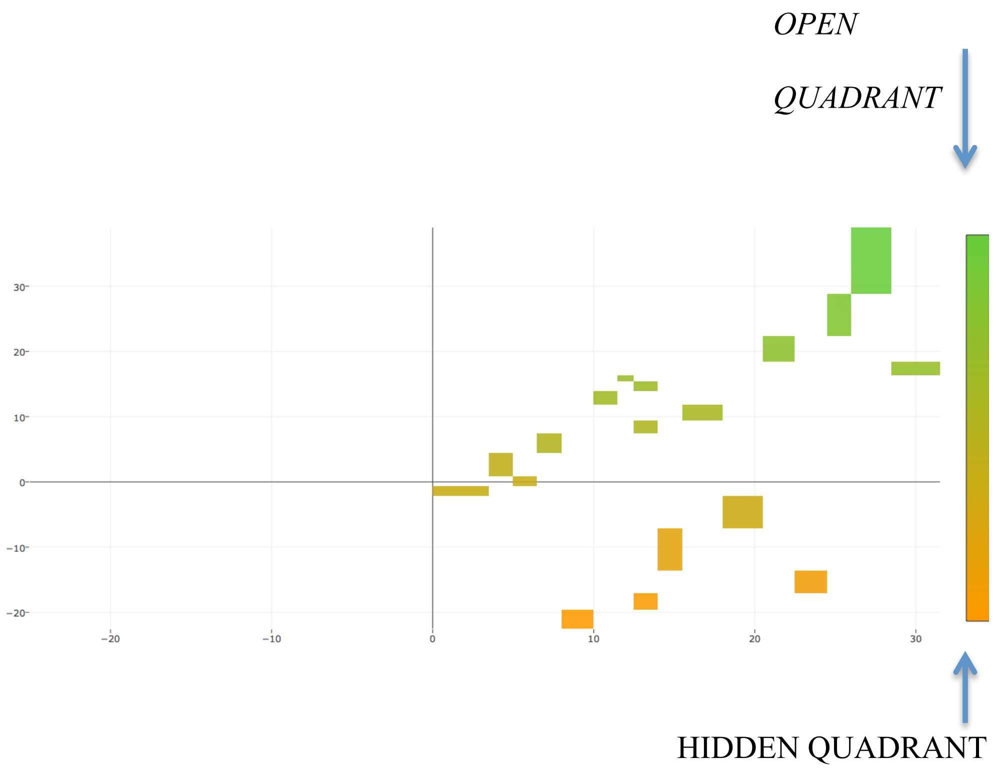

Figure 4: Risk Understanding (RU) and Affective Security (AS) code tallies for Organisation C (Primary Coder data) positioned within the Open and Hidden quadrants

In relation to the BSG framework, the graph (see Figure 4 above) demonstrates that the spread of participants are centred around the *Open* and *Hidden* quadrants, since the *RU* scores are all positive ranging from 1 to 27 (primary coder) which excludes the *Unknown* and *Blind* quadrants which are defined by their *Negative RU* scores. However, the *AS* range of scores from -11 to 34 (primary coder) reflects more variability than the *RU* scores.

6.3.1 Further Validation: Coder 2

To further test the validity of the results from the qualitative coding, a second coder independently coded the transcripts which reflected a similar pattern of results. For instance, coder 2 reported a similar range of *AS* scores (from -4 to 35) which extended into the *Hidden* and *Open* quadrants respectively, and in line with my coding, found the *RU* scores to be all positive (3 to 26). As there was no neutral point in the coding system, scores were either coded *Positive AS/RU* or *Negative AS/RU*. The inter-rater reliability was calculated using Cohen's kappa between two coders for *Positive* and *Negative* categories of *AS* was found to be of fair agreement (kappa = 0.231), in line with Landis and Koch's (1977) guidelines, and almost perfect agreement for *RU* (kappa =1) (both coders rated all the *RU* codes positively).

In terms of percentage agreement, I assigned 75% of the participants to the *Open* quadrant and the remaining 25% categorised within the *Hidden* quadrant, whereas Coder 2 assigned 90% of the participants to the *Open* quadrant with the remaining 10% located within the *Hidden* zone. There was disagreement in relation to the assignment of negative AS scores; I assigned 15% more of the cohort to the *Hidden* quadrant. This will be discussed in the limitations section (see *Chapter 6.6.1 Limitations*). There was however perfect agreement in the direction of RU scores between coders.

As described both coders rated the entire cohort as demonstrating *Positive RU*. These results suggest that this cohort of employees understood the security risks, albeit to varying degrees. This is perhaps unsurprising given that Organisation C's primary *context*, although not always the primary *task,* is security. Their affective attitudes, feelings and behavioural preferences towards security were more variable however.

	Coder 1	**Coder 2**
AS Weak Positive	146	174
AS Strong Positive	91	107
Combined AS +	235	281
AS Weak Negative	92	117
AS Strong Negative	30	6
Combined AS -	122	123

Table 4: Distribution of Affective Security (AS) Codes

	Coder 1	**Coder 2**
RU Weak Positive	180	68
RU Strong Positive	89	145
Combined RU +	268	213
RU Weak Negative	39	31
RU Strong Negative	13	3
Combined RU -	52	34

Table 5: Distribution of Risk Understanding (RU) Codes

Tables 4 and 5 (see above) present the breakdown of the frequency of the code categories across Coders 1 and 2. Figure 3 includes: *AS Weak Positive, AS Strong Positive, AS Weak Negative, AS Strong Negative* as well as the combined *AS Negative* and combined *AS Positive* scores.

6.4. Case-study 3: Qualitative themes

Summaries of qualitative themes for two participants (P9 and P11) are presented below. (For a fuller account of the remaining nine participants in the Organisation C cohort see *Appendix 1)*.

6.4.1. Participant 9

6.4.1.1. Affective Security

This participant's narrative was rated as demonstrating *Positive AS* scores, with both myself and coder 2 scoring the same quantitative score for this interview. This is reflected in the description of the security culture of Organisation C:

> *"…in the environment, security is taken very seriously – work in a secure area lots of classified documents. People are responsible, everything [is] locked away at night – if you don't [put] stuff away, or your leave your cupboard open…[there are] consequences...". (P9)*

6.4.1.2. Risk Understanding

In relation to *RU*, *"fictional colleagues"* are described as recognising the different expectations around security behaviour depending on whether they are dealing with classified documents or not for instance. Therefore if they do not deal with classified information, the employee suggests that "*fictional colleagues*" tend to leave "*stuff over their desk, because stuff on their desk isn't sensitive – probably more relaxed…"*. The employee describes how the "*risk is minimised*" in relation to access to classified material as "*fictional colleagues*" are given specific clearances and also, from a physical security perspective, work on the same floor:

"How much confidential data do colleagues get access [to]? All their work in some jobs is highly classified, the risk is minimised... everyone else has the same level of clearance…to work on that floor…". (P9)

6.4.1.3. Consequences

There is also a sense that "*fictional colleagues*" are aware of the security risks and more specifically the consequences of an ill-judged decision. For instance, the employee suggests that "*fictional colleagues"* are encouraged to recognise that what they send over the internet is akin to leaking information to the press:

"People are aware of the security risks – one of the key phrases 'never send anything over the internet that you wouldn't want to see in The Times'…". (P9)

Similarly, when describing perceptions of the security culture, this participant suggested that there were "*consequences*" if work-related material was not put away or cupboards were left open:

"What sort of consequences? If the police find your cupboard open, they'll put a breach notice[on it], then they'll lock it, then…an interview without coffee…if [one] were to have several breaches…".(P9)

6.4.1.4. Security culture and team work

The employee suggested that security was taken "*very seriously*" and were responsible for locking away documents etc:

"Security is taken very seriously – work in a secure area lots of classified documents, people are responsible everything locked away at night…". (P9)

A key driver in supporting and reinforcing the security culture within Organisation C appeared to be the use of the '*last man out system'* which involved the last team member in the office checking whether cupboards are locked for instance, to avoid potential security breeches:

“no one wants to come in and [find out] they are [the] result of a security breach, or they’ve forgotten to collect anything from the printer. Last man out checks the cupboards, check for colleagues – makes sure nothing is left... looking for each other, when you lock your cupboard you sign a sheet to say where you locked it – last man out signs that too, checks people’s cupboards...you don’t check [the] whole floor, only checking [your own] section…”. (P9)

This theme around non-compliance and team work has implications for risk, where “*fictional colleagues”* are less likely to be reported for security breaches since there is a perception that colleagues are there to protect each other:

“Most people follow the rules, [as regards] non-compliance reporting. Reporting on another colleague is difficult,[we are] there to protect each other – if one of my staff left his notebook out on my desk I wouldn’t go and tell security officer - police each [other], check each other’s cupboards – wouldn’t go and report somebody, wouldn’t go and report a colleague for not locking computer…”. (P9)

There theme within this interview around non-compliance and risk, where “*fictional colleagues*” are framed as individuals who, if circumventing policy, do not do so with malicious intent, instead it is attributed to “*human error*”.

“Always human error – people have had a bad day, left in a hurry forgotten to lock their cupboard...not malicious…”.(P9)

Further, the employee stresses that because security is part of “*fictional colleagues’”* jobs at Organisation C, there is general acceptance and adherence to security culture. P9 suggests that security in the context of Organisation C could be considered part of their primary task because “*security is part of fictional colleagues jobs at Organisation C…*”.(P9)

6.4.1.5. Training

This employee talked extensively about the training provision in Organisation C, indicating that security training courses were available to new joiners for instance, and annually for other staff. Additionally, P9 highlights that there is an emphasis on data management courses in particular.

"…document handling, handling of secure documents – we have a whole security section that do these briefings, when new staff come in and they get a special security briefing – all the different bits of the security world and how all the information needs to be protected. Confidential data briefings…". (P9)

The positive view of the training provision may be linked to the positive attitude expressed towards security within this interview, as the employee suggests security is "*taken seriously*" within Organisation C.

6.5. Participant 11

6.5.1. Affective Security

This participant's *AS* score was ranked the lowest by myself and coder 2. It is the most negative score amongst the employees from Organisation C, which is reflected in some of the negative statements about the usability of technology and the impact on security.

For instance, there is a theme within this transcript that following security rules in the organisation is actually difficult for "*fictional colleagues"*:

"Difficult to observe the rules, literally switching [your] phone on and off, [no]way to be contacted in an emergency… it doesn't work from a security perspective not the way we are living our life…".(P11)

6.5.2. Risk Understanding:

Further, *RU* is explicitly linked to security culture suggesting that although "*culturally, there's a good security culture, this organisation has to steer managed risks*".

P11 also talks about how security behaviour "*relies [on] colleagues understanding the risk*". For instance, they referred to "*fictional colleagues"* emailing documents to themselves to make it easier to work and emphasised whether this is secure or not depends on how colleagues manage the document – e.g. by redacting the sensitive data.

6.5.3. Security culture:

This employee refers to security within Organisation C as something that is "*part of everyone's day, an inherent part of the day*", which is a theme that resonates throughout this interview. P11 highlights that "*fictional colleagues*" are likely to absorb the security policy rules via "*word of mouth*" and that plenty of information is available, albeit that the guidance on the intranet is "*generally aimed at security experts*". Interestingly, whilst the employee acknowledges that there is a focus on personnel security, information security is less thoroughly managed:

> *"Less good at information security ie [the] threat at using wifi – there is a threat briefing, general security… there's an online course…didn't include information security, more big picture i.e. sorts of threats that we face… and how those threats might materialise,[i.e.] the case studies and the weaknesses and how security is compromised…". (P11)*

Nevertheless, P11 suggests that there is a sense of following the security rules which are not always easy to navigate or specific enough to empower the employee to understand what actions they need to take:

"within that – some things that are less good,[they] cover their backs…A culture built around rules, a book of rules, literally a big book of rules, prescriptive, hard to navigate,[especially]when technology changes…smart devices [are] not covered – not specific in the guidance…". (P11)

In addition, there is a perception that the rules are not written for the benefit of employees necessarily, that there may be a legal agenda that primarily serves the organisation:

"Read it several times, wasn't clear on guidance – the people who wrote it didn't really know, [the] guidance was trying to say you can do this if you take these steps, so wasn't very fit for purpose, written in a 'legalistic way' – guidance has been written for a number of purposes…Everyone [tries] to get it right, if something went wrong, but it's really written to protect the department if you do something wrong. This colleague could be feeling paranoid – the guidance could be better, …it was very long…".

P11 goes further, suggesting that "*fictional colleagues*" will actually get reprimanded more for getting the rules wrong, rather than being focused on *why* the security guidance is not easier to understand:

"Security is still rule-based, some effort seems to go beating up the people who get the rules wrong – perception – more scared about breaking the rules…".

Their perception of security is also note-worthy; this employee refers to security as something that "*is much harder to get your head around*". They highlight the differences between security and a health and safety culture, indicating that the latter is perceived as everyone's responsibility whereas people are "*more secretive*" about security:

"On the security side, [we are] more secretive about it – extreme example when an aircraft crashes, forensically rebuild the whole aircraft which went wrong. The investigators come up with [a] conclusion – they will find it – redesign…".

This alludes to the idea that problems with security may be obscured or *hidden* away, unlike health and safety issues where they are more likely to be explored and resolved, if necessary, via redesigning a system or set of processes.

6.5.4. Security cultures and work friction:

P11 attributes "*fictional colleagues*" breaking security policy (in this case in relation to data management) to overwork and friction (because the security policy interferes with work processes):

> *"I know that [fictional colleagues] mustn't leave a secretly marked document on [their] desk overnight, [and] would only do that by severe accident, genuine error, [in] one case: or they were being sloppy in their way of working taking [away] documents, then one day left [them] on a train. Guess the reason they were doing it [is that] they had too much work, the department didn't provide a secure way of working at home…".*

The employee's description of "*fictional colleagues*" narrative here, in terms of explaining the trade-offs between security and usability, suggests that when processes are unusable, risk perception may be downplayed since policy is circumvented.

Another example of the impact of security on productivity can be found in the text where the participant describes circumventing or "*going around*" security in order to get the job done:

> *"...You work in less efficient ways – because you go around security, in ways that are valid, or I suspect, get sloppy with security – [the] only way to get the job done, [is] valid circumventions…".*

They go on to suggest that such circumventions may include sending data over the internet i.e. via email, or taking sensitive data home. Interestingly however, there is a slightly contradictory perception here where the participant suggests they "*haven't broken any [policy] rules*" yet describes the actions as "*valid circumventions*".

6.6. Case study 2 discussion: Why Risk Understanding is not enough

The results show that all of the employees were rated, overall, as demonstrating *Positive RU*, yet *Negative AS* were expressed in approximately 25% of the transcripts (Coder 1). These expressions of negative affective responses were related, in part, to certain security policies or technical provisions that inhibited workflow or caused *friction* with productivity. Another issue that was identified within the interviews was the impact of limited resources, particularly associated with a lack of staff. Subsequently, the task of communicating, managing security messages and training was not fully resourced which likely had a negative impact on security compliance. Potentially linked to this, was the issue of human error in interpreting and understanding what security behaviours were required and compliant with policy, in other words what behaviours constituted security compliance with Organisation C.

Human error or the "*problem of human fallibility*" (Reason, 2000) is delineated in two ways by Reason; i) *a person approach* which blames the individuals for mistakes and mishaps or ii) *a systems approach* where the focus is on developing systems and processes to strengthen the organisation's defences. The incidents thought to be caused, in part, by *human error* were generally not attributed to malicious intent on the part of the employee, but instead linked to the employee either not being clear about what behaviours were required, or due to the limitations associated with cognitive capacities such as memory issues particularly in relation to password management. Employees may not always remember to perform security actions, so forgetting to lock cabinet doors when leaving the building, or leaving a laptop on a train may reflect typical incidents associated with human fallibility. These themes that emerged from the analysis where individuals are struggling to comply with security suggests that Organisation C may benefit from adopting a more systems-oriented approach to security.

From the initial results, one could suggest that *Risk Understanding is not sufficient* alone to ensure positive attitudes, feelings and behavioural preferences towards security, particularly if *security hygiene* is not in place. In these cases, employees may feel they have to circumvent policy to complete their primary tasks in order to save time, meet deadlines or reduce the cognitive load etc. There are many examples within the interviews of insufficient levels of *security hygiene* leading to policy circumvention such as staff emailing work data to their personal account because it is time-consuming to access work repositories remotely for instance, taking confidential hard copy material home in order to work on it remotely, as well as using their own devices because existing systems are not as usable.

As well as having limited technical resources to help employees work productively and securely, another issue that emerged from the analysis of the data was the impact of limited human resources to help improve employee security awareness and behaviour. Indeed, in relation to this case study, one of the emergent themes from thematic analysis of the qualitative data is that security is undermined by inadequate resources (see *Appendix 1*, P4 for details). These include sufficient numbers of security specialists to manage the security provision as well as technical mechanisms and security processes that are usable.

Nevertheless, efforts to improve security awareness such as training courses and targeted security messages for instance to improve *RU* may not be sufficient to improve attitudes, feelings and behaviours towards security. Indeed, if it was, it would reasonable to expect everyone to be in the *Open* quadrant since all employees within the sample demonstrated that "*fictional colleagues*" had understood and recognised security risks in the environment to a reasonable degree. As previously mentioned in this case study, Organisation C data has been shown to straddle both the *Open* and *Hidden* quadrants, suggesting that despite *RU* scoring positively across both independent scorers, the variability in the *AS* scores, ranging from positive to negative scores across this cohort, implied that some employees expressed negative views about security, despite understanding the risks. This combination of *Positive RU* and *Negative AS* scores represents a risk for the organisation, where employees are operating in the *Hidden* quadrant of the BSG, which may in turn, suggest they are i) expressing dissatisfaction with the organisation's security policy ii) may therefore bend or circumvent security policy in order to carry out their primary tasks.

What are the underlying reasons for the variability in *Affective Security* scores and what does that tell us about this cohort? The assumption that *Negative AS* scores reflect "*problem*" employees who i) do not recognise the security risks and ii) are inherently negative about security is challenged by these results. The two qualitative summaries outlined (refer to *Chapter 6.4* and *Appendix 1* for the remaining eighteen summaries) highlights various issues where some of the security processes are failing to meet usability standards leading employees to bend security policy rules on occasion.

If security is not fully supported by the infrastructure in relation to data management processes or compromised by inadequate resources such as up-to-date IT systems for instance, security risk aware individuals may express negative affective responses, coded here as *Negative AS*. It is likely that employees who understand the risks yet feel they have to struggle and in some cases circumvent clunky security policy tasks in order to carry out their primary work, may express *Negative AS* towards security. Further, awareness of needing to break the rules for many employees may lead to stress responses, which might initially be surfaced as negative *affective* statements. In this way, *Negative AS* could potentially act as a flag to encourage organisations to further examine the functionality of the security policy and associated resources.

It is suggested therefore that one of the ways for organisations to utilise the BSG framework is to firstly perceive *RU* as a competence to be measured and achieved. Once this is in place, awareness of employee 'affective' responses in relation to security, measured via *AS* scores, will allow organisations to further investigate *Hidden* security practices which may have arisen as a result of a inadequate resources and/or a faulty security policy.

Using the BSG as a starting point, the population of scores across two of the quadrants – the *Open* and *Hidden* zones - suggest that once competency around *RU* is met, then a further test exploring affective attitudes, feelings and preferences towards security (i.e. *Positive* or *Negative AS* scores) would allow organisational managers to understand more about the security posture and specific security micro-cultures with the organisational eco-system.

6.6.1 Limitations associated with scoring

There were slight differences between my coding and coder 2 in the negative range of *AS* scores. I acted as the primary coder (Coder 1) but also the interviewer, and scored some of the interviews slightly more negatively than coder 2 with an outlier of -11 compared to -4. As reported in the results (see *6.3.1*), the inter-rater reliability demonstrated fair agreement, according to Landis and Koch (1977) (kappa= 0.231). It should be noted that both coders were free to select and code the interview transcripts independently; although we both used the same methodological approach, there were differences in i) the selection of the text within the interviews ii) frequency of negative *AS* codes. As I conducted all of the Case Study 2 interviews – Coder 2 did not conduct any Case Study 2 interviews - I potentially had a more in-depth understanding of the interviews, which may have also impacted on my scoring. The interpretivist paradigm adopted within the qualitative aspect of this study emphasised the subjective aspects of coding; this subjective approach may have resulted in slight differences between coders in the *AS* coding process. (This will be further explored in *Chapter 9.5.1 Limitations*).

Nevertheless, the highest score in the positive range for the *AS* rating across both coders was very close; with the highest scores for *AS* being 34 and 35 for myself and coder 2 respectively, therefore it is argued that the range and pattern of the scoring across both coders is quite consistent. Both coders scored positively for the *RU* set of scores and the overall range of the *AS* scores was similar.

Furthermore, lower inter-rater reliability does not necessarily indicate disagreement between raters (Tinsley and Weiss, 2000), as considering both percentage agreement as well as inter-rater reliability need to be taken into account. A reasonably strong percentage agreement (75%) between coders in relation to the quadrants, coupled with fair inter-rater reliability indicates that there was reasonable agreement between coders. This suggests the methodology offers organisations a valid starting point to begin to categorise employee security behaviour in relation to risk and affective responses. It is important however to ensure the coding process incorporates regular reviews to cross-check consistency amongst coders as conducted within the coding process (see *Chapter 5.1.1*).

The primary function of the scores is that they allow for the categorisation of employees within the BSG paradigm; i.e. whether their *RU* and *AS* scores position fall within the *Open, Hidden, Blind* or *Unknown* quadrants. In this respect, there was agreement across all the *RU* scores i.e. although there were differences in actual scores between coders, both coders scored on the positive spectrum of the dimension for the *RU* variable. Both *AS* and *RU* scores were rated in the same category (negative or positive) in 15 out of 20 participants across the 2 coders. On reflection, I would expect the agreement between coders would be improved by increased experience in qualitative coding particularly in relation to text selection choices (see *Chapter* 9.5.1. *Limitations*).

It should be noted that there are limitations in respect of the *AS* and *RU* scores themselves. Firstly, as previously mentioned, they are ordinal, not interval data - so comparing scores beyond whether they are positive or negative is not meaningful. In addition, when considering the scores in relation to the quadrants, the data is classified as nominal. Therefore, comparing a positive score of 20 with a score of 5 is not meaningful beyond positioning it within the context of the grid which categorises data into quadrants. (see *Chapter 9.4 Limitations*).

CHAPTER 7: CASE-STUDY 3 - SENIOR INFORMATION RISK OWNERS (SIROS) ACROSS GOVERNMENT DEPARTMENTS (ORGANISATION D)

This study comprised a small number of Senior Information Risk Owners (SIROs) and Senior Risk Managers across a variety of government departments. The participants from the different government departments will be referred to collectively as Organisation D rather than reveal the specific department where they worked.

The participants for this study were recruited via a main point of contact within one of the main government departments and participation was voluntary. Eleven participants agreed to be interviewed for the purposes of the research.

In line with Case Study 2, I discussed any potential ethical ramifications associated with the study, such as ensuring anonymity, and subsequently agreed broad principles with the sponsor of the work to ensure the study was in line with the ethics committee's standards. Anonymity was assured in that participants in the study were referred to by number (Participant 1, etc.) and their full name was not written on the interview transcripts. It was also agreed that I would personally interview all the candidates to ensure consistency of approach. Notes would be taken rather than record any of the interviews to ensure security and consistency of approach in line with Case Study 2. Candidates were advised not to reveal any classified data, furthermore, during the interview itself I checked whether employees were comfortable disclosing certain details. I removed or amended comments, approximately three or four times – when a participant asked for it, or when I judged that this was revealing an exploitable vulnerability or could be used to identify the participant.

7.1.Research question & proposition

The focus of this study was twofold; firstly to glean more about the SIROs role and in particular their unique perspective on security behaviour, affective responses towards security policy and recognition of the information security risks in the environment. Secondly, to explore the insights from this unique group in terms of affective responses to security (*AS*) and knowledge and awareness of security risks (*RU)* as well as any other themes that emerge from the analysis. Specifically, in relation to Case Study 3, the research question sought to address whether this SIRO group was likely to demonstrate deeper understanding of the security risks and positive attitudes towards security within Organisation D than the other three populations within Case Study 1 and 2.

Case study 3 proposition : It is expected that the cohort of SIROs demonstrate awareness of security risks (*Positive RU*) and express positive affective responses towards security within the organisation (*Positive AS*), this would imply being categorised within the *Open* quadrant.

7.1.2 Methodological approach

The methodological approach for Case Study 3 was based on the approaches that emerged from Case Study 1 (Company A and B) - although it did not statistically compare two organisations - and also from Case Study 2. The same codebook was used for consistency. As with Case Studies 1 and 2, the qualitative analysis technique *applied thematic analysis* (ATA) was used to code the data (see *Chapter 5.1.1*). As discussed, this qualitative approach allowed the data to be organised in relation to the codes and themes linked to security processes and people, which were already refined in the existing codebook. No additional superordinate codes were developed from this process which suggested that the codebook emerging from the coding of Company A and B was sufficiently comprehensive.

The same code families split into i) *systems and processes* and ii) *emotions and risk* as demonstrated in Case Study 1 (see *Chapter 5.1.1*). The two main dimensions *AS* and *RU* were operationalised for the quantification aspect of this research and included *Positive Strong* and *Weak* and *Negative Strong* and *Weak* aspects. The permutations of these codes were quantified using the simple equation, consistent with the methodology outlined in Case Study 1 (see *Chapter 5.7.1*).

Once the data was coded, quantitative analysis was applied to *Strong, Weak, Positive* and *Negative AS* and *RU* dimensions in order to explore what the security modes espoused by this sample population were i.e. whether they

Open, Hidden, Blind and/or *Unknown* in the context of the BSG. It is noteworthy that the participants in Case Study 2 were employees from the same organisations albeit occupying different positions and departments within Organisation C, whereas the participants in Case Study 3 (Organisation D) were recruited from a variety of government bodies and hold different positions within the organisation. However, as discussed, all the participants in Case Study 3 occupied Senior Risk Owners/Managers as one aspect of their role.

7.2 Results

	Affective Security	**Risk Understanding**	**BSG**
Participant 1	2	15	OPEN
Participant 2	23	23	OPEN
Participant 3	24	29	OPEN
Participant 4	7	32	OPEN
Participant 5	25	16	OPEN
Participant 6	6	32	OPEN
Participant 7	15	22	OPEN
Participant 8	12	14	OPEN
Participant 9	20	19	OPEN
Participant 10	13	18	OPEN
Participant 11	23	27	OPEN

Table 6: *AS* and *RU* results for Case Study 3

All of the participants in this cohort expressed positive levels of *RU* as well as positive levels of *AS*, positioning all of the participants within the *Open* quadrant of the BSG. Thus the participants demonstrated competence in relation to security risks and positive sentiment towards the security provision in the organisation, or security generally. This encompasses the participant's own view related to security and also assessing security behaviour whether it be i) identifying the risks associated with their "*fictional colleagues*" behaviour, or ii) judging the risk assessments made by "*fictional colleagues"*, iii) assessing affective attitudes, feelings and behavioural preferences towards security.

As discussed in the earlier section (*Chapter 7.1.2*) the interviews replicated the format of both Case Studies 1 and 2 in that they were semi-structured in format covering a similar interview question set. However, Organisation D interviews also incorporated material focused on the SIROs role, how they perceive security risk in the organisation and how they manage and communicate that risk. It is therefore a unique cohort in this regard.

7.3. Qualitative Summaries

This section includes summaries of two (P1 & P4) of the participants within the SIRO case study. (See *Appendix 6)* for a more in-depth summary of the remaining nine participants). It should be noted that many of the SIROs interviewed were not engaged as security specialists, and many did not have a 'technical' (IT) background and felt they had not been trained adequately.[5] They performed other roles in the organisation, and part of their challenge was to manage the information security risks or manage others who owned the risk as well as performing their primary duties. An overview of the emergent themes from all eleven participants are outlined in the discussion section.

[5] The technical or non-technical background of the SIRO was not systematically recorded for reasons of anonymity; rather it was an insight that emerged from coding the qualitative themes

7.3.1 Participant 1

7.3.1.1 AS and RU

P1 expressed a positive stance towards security, hence the *Positive AS* scoring – but it was the lowest score out of this cohort. This is reflected by the mixed messages towards security throughout the transcript. For instance, the employee notes *"fictional colleagues"* are aware of the security implications associated with company information, but nevertheless may circumvent security rules when there are "*too many layers of control*" in place and people find "*rat runs*" presumably to speed up the process. Interestingly, P1 highlights that the "*biggest risks are the senior staff*" – a theme I will return to later in this summary (*Chapter 7.3.1.4: Senior Circumvention*).

There seemed to be competence around recognising the security risks within Organisation D across various information security issues, particularly in relation to passwords. For instance, the employee highlights that password sharing is less of a risk, but the entropy of passwords was more of an issue:

> *"Don't see password sharing happening – ...when we did the 'fictional' baseline exercise - didn't see password sharing as a risk. Main risk, digital notes and similarity between passwords, there would be a pattern; [a] high correlation between passwords sequences, same word, different numbers…".*

Another theme around risk management, relates to the participant's observation that it is difficult to track who is the risk owner for certain data within different government departments:

> *"The info asset holder's protocol [is] to manage who is holding the information risk – who owns the risk? One government department straightforward, but another…less well developed".*

This suggests that there are organisational challenges in relation to identifying the risk owner of certain data. Clearly, this ambiguity creates difficulties in risk mitigation around data management.

7.3.1.2 Aesthetic work environment

P1 discusses how fictional colleagues are proud of their work environment, since the building is "*beautiful*" and how this influences security behaviour. Specifically, they refer to the fact that "*fictional colleagues*" adhere to a non-enforced clear desk policy because they want to keep their environment in good order:

"Clear desk policy – how well is it established? Brand new nice building, people feel proud and pleased to have building, environment facilitated high tech building – aesthetics, beautiful – everyone wants to keep it looking nice, not enforced because it's not an issue…".

This quotation indicates that an aesthetic environment is perceived as a positive influence on security culture, in that staff are more likely to improve their security behaviour if they perceive their environment positively.

7.3.1.3 Security messages and training

P1 identified various improvements to help SIROs in their role, which will be outlined here. For instance, P1 suggests that SIRO's understanding of their role would be improved by having more practical case studies to be able to convey security messages more concretely:

"…they'd [the SIROs] like to see more best practice, narratives around a few more case studies - lots of information, dense…no narrative behind it – trying to explain the reasons, no stories, hard to communicate the issues, meaningful conversations – having to find those narratives for those stories…".

This empirical observation aligns with the literature on risk perception, which highlights that transforming abstract risks to concrete narratives potentially improves the efficacy of security messages.

P1 indicates that *"fictional colleagues"* have an awareness of security policy but suggests the challenge for Organisation C relates to maintaining that awareness via security communications and training. For instance, they suggest that individuals taking on a new role may be required to absorb new security information but may not receive sufficient and/or appropriate information and training:

"…not awareness but maintenance of awareness, part of induction process, someone taking a new role, different areas different levels of implementation, maintenance of information [is the] achilles heel; communications, briefings, the continuous training protocols – people could miss 6 months of awareness [training]…".

7.3.1.4 Senior circumvention:

A central theme within this transcript is the perceived ambivalent attitude of "*fictional*" senior members of staff towards security. One example is the observation that senior "*fictional colleagues*" may be "*sociopaths*", because they think security policy rules do not always apply to them:

"Senior leaders are often sociopaths – [security rules] they don't apply to you – world configures around you…".

Similarly, P1 identified that both a "*fictional senior leader and the fictional senior team"* would be inclined to ignore security policy rules at times:

"…a fictional leader may have been worst serial risk – their assumption that rules didn't apply to them –[when using] powerpoint [they] ignore rules around using USBs or sharing drives in a fictional world – biggest risks are

the senior staff. Generally speaking all [are] aware and respect [the rules] – but the senior team…".

P1 proffered a hypothesis to explain the behaviour of "*fictional*" senior staff, suggesting that this senior group do not perceive themselves as subject to the same constraints as others. P1 argues that this extends to "*fictional senior colleagues'"* perception of risks in that - whilst they objectively understand the importance of risk - on a personal level they adjust it, that is they reduce the assessment of the risk, to reflect their senior position:

"Hypothesis: you may find that senior people's disregard for risk [is] at a personal level [they] understand [the] importance but won't hold themselves up for the same level of accountability. Hold staff to expense accounts £25 staff, £100 for senior, acceptance that you reach a certain level, you say all the right things, your staff do it for you;[if you say] "I need this urgently", people will send a file through a personal Dropbox *for senior staff*[6]*…"*

P1 provides various other similar examples of senior staff circumvention such as bypassing protocols, sharing drives and using information ways of sharing information rather than via the approved route:

"Access control – bypassing protocols, sharing files, sharing keys, sharing sticks, emailing from insecure machine, receiving in restricted countries, not using VPNs…informal ways of sharing information – people will bring [data] on a shared drive – share on insecure media...".

P1 also suggests that "*fictional"* senior staff members may be more likely to engage in circumventions when they are under time-pressure, experience cognitive overload and feelings of stress:

"...when people are under stress or overworked they make bad decisions – my experience is they are our highest risk...".

[6] There is no official Dropbox for staff to use, therefore senior staff are expecting junior staff to send the information through via that mechanism

These insights from P1 are characterised, to some extent by their emphasis on the circumvention of "*fictional*" senior colleagues. As a side note, it is useful to note that whilst this individual is not the sole SIRO, s/he is charged with managing these responsibilities on a daily basis which may affect their perspective on this.

7.3.2. Participant 4

One of the challenges for the SIROs is to manage the influx of information they receive. P4 recognises there are many sources of information to support the SIRO in their role; for instance, they refer to a newsletter for SIROs, a 'Government Agency', information from peers and the team. However, P4 also refers to information relating to issues that there are not able to share information on for instance, the issue of being subject to malicious parties' demands, which is something a SIRO is required to deal with:

"How adequate is the info? Nobody wants to talk about this – we are supposed to be honest, but it's a 'dirty little secret' best practice you don't let people [in the industry] know ... you would be targeted [using] denial service attacks ..."[7] *(P4)*

Clearly, P4 identifies a theme around what is not talked about in relation to security, and how there is a sense of secrecy in relation to aspects of risk management.

P4 also discusses the challenges that the SIRO has to manage. They suggest that security has changed, because perimeterisation does not work since one

[7] P4 is referring to external malicious parties involved in activities such as denial of service attacks

"*can't treat everything inside [the] soap bubble as safe anymore*", therefore this new security landscape requires a different approach from the risk owner:

> *"Biggest barriers; long-held notion of perimeter [security], a membrane when everything is safe – inside attack threat [is] absolutely demonstrable, can't treat everything inside soap bubble as safe anymore, able to identify critical services, critical assets, more liberal no…clean boundaries…how do you manage security?". (P4)*

They discuss the notion that the threat is *also* contained within the organisation, which is difficult for the SIRO to police.

7.3.2.2. AS and RU

The *AS* score was positive overall, with the employee appearing keen to implement security improvements within the organisation. One example of this is P4's reference to changing policy around remote working is not made easy for "*fictional colleagues"* within the organisation:

> *"At the moment, remote working [is] quite difficult - most people don't, a third of people do [it] ad-hoc, [they] go to the support desk, book out a clean or dirty laptop (dirty one is for presentations away), [there are] regular home-workers – laptop permanently allocated, take 15 mins pain [to obtain laptop], then [there are] full-time remote workers [who work remotely]…".*

P4 goes on to describe how the policy is in the process of being adapted to reflect the needs of "*fictional colleagues*" flexible working requirements in order to make it more usable:

> *"[I have] just signed off on Monday a huge investment in remote working… massive policy change now, assumption you will not be working at your desk – [we] need to do more hot-desking – even that changes your assumption [about security], huge policy change. [As a] Director you might need more points i.e. 2 laptops, so it is point based system, forces choices between laptop & phone, can't do BYOD at the moment, managing costs…".*

In line with the rest of the cohort, P4's transcript was coded as positive in relation to *RU*. P4 noted that one of the biggest risks may be that employees are not necessarily blind to security risks, but that it is difficult in practice to identify those risks, for instance distinguishing between a genuine email and a phishing email is difficult:

"How does the organisation manage people who are blind to the risk? [The] ability to spoof your email address is trivial – the link takes you to a piece of software, to known unpatched vulnerabilities in your IT. [The] advice is "don't click on links from unfamiliar sources" is not do-able. I could attach something that looked like a word doc and that would attempt to expose a vulnerability that you will not have patched yet – how would you differentiate from an email that's bona fide, do I even believe in the policy?…".

Additionally, there is a theme within the transcript that whilst employees should be educated to recognise the risks, there are some "*nefarious risks*", so it is difficult to manage this dynamic:

"Think people should be educated to see the risk – but don't have a good answer [as to how] to see the risks, the risks are nefarious…fact of the matter is, we [have] got to try and defend the soap bubble."[8]

Nevertheless, P4 acknowledges that there are some "*fictional colleagues*" in the organisation that take unacceptable security risks. P4 attributes this to them not having the necessary level of *RU* suggesting that it may be because they do not have the required security knowledge, so they are '*blind*' to the risk. Alternatively, P4 also states that they may be dismissing the risk because it requires less effort:

"People take unacceptable risks – based on whether they get found out. Access to systems; people doing inappropriate things within that access such as downloading inappropriate material because they have dismissed the risk –

[8] P4's does not specify what "*nefarious risks*" consist of; but later refers to "attacks" aimed at the organisation which could include denial of service attacks and ransomware

without the knowledge, some of them won't know the risk, dismissed the risk, probably a bit lazy. Any of the combination of the above…".

This suggests P4 is aware that some "*fictional colleagues"* do not recognise the security risk, and in that sense, are aware of the human risks associated with security compliance behaviour.

7.3.2.3 Security training, policy and circumvention

P4 reflects their positive attitude towards security, describing how security training is being developed within the organisation.

"Security training? In development but a huge priority – a 10 minute video talking about protecting info – but to a large extent protecting the organisation – a grown up adult-to-adult conversation, more intelligent conversation…".

This suggests that security training within the organisation is not currently established despite being a "*huge priority*".

In terms of how P4 conceptualises "*fictional colleagues"*' attitude towards security compliance, individuals may form perspectives on security based on their consideration of what is appropriate both themselves and the organisation. They also posit that there is a moral aspect to this, where their professional judgement stems from the individual's moral standpoint:

"With some noted exceptions – people look through the lens of 'is it appropriate for me and the organisation?' Extension to how we morally behave, then professionally after that…".

However, P4 suggests that - although people are likely to consider security via an "*information lens*" - they are more likely to take unacceptable risks based on whether they will be found out or not:

"I've got a piece of paper - reading on the train - am I thinking about it through [an] information lens, it's probably more about 'will I get into trouble?'. People take unacceptable risks – based on whether they [are likely to] get found out…".

7.3.2.4 Passwords

One of the areas of security behaviour that appears to be less satisfactory is passwords. P4 infers that this behaviour is not due to malicious intent, but a result of not having a single authentication system. P4 also suggests that - because multiple passwords are required – "*fictional colleagues*" may re-use passwords to increase memorability.

"Passwords [we] do not have a single authentication method, so behaviour is poor. Behaviour is not very good, people using [the] same password for multiple systems…trying to move towards single sign-on…".

This is in line with recommendations from early research which identified that multiple passwords lead to password re-use, and single sign-on is an effective way to manage this (Adams & Sasse 1999). P4 frames the problem of having no single authentication positively, in that there is a stated desire to move to a better security solution for passwords. It is clear that there is an awareness that there is work to be done to improve *security hygiene* i.e. enable staff to be able to comply with security tasks by reducing workload and stress. (As discussed, see *Appendix 5* for the remaining 9 summaries from the Organisation D cohort).

7.4. Case study 3: Discussion of themes for Organisation D

Before looking at the emergent themes across the Organisation D interviews, it is useful to remember however that ‘Organisation D’ is a conglomeration of various departments and agencies under the umbrella of one large government department. Further, in order to preserve anonymity the names of the specific departments were not recorded. It must be taken into account that staff in one part of the organisation may demonstrate different types of security behaviours depending on the security posture of that particular department or organisation. In other words, there are likely to be different cultures within the individual departments. Nevertheless, all the departments from which the SIROs were drawn were guided by the same umbrella security policy, set by Organisation D.

This being said, the participants interviewed within Organisation D for Case Study 3 held SIRO roles, or were directly assisting the SIRO, in addition to their day jobs, and therefore shared some perspective on security. The responsibilities for the SIRO within each of these government departments are similar in that they are charged with managing the organisation’s information risk policy, influencing the board in incorporating information risk issues in their security strategy and policy development. Therefore, their position is significant when interpreting these results because ultimately this cohort are influencing and managing information risk policy within the organisation.

As one would expect, this group of individuals' *primary task* (or at least one of their formal responsibilities) focus is on risk management. Thus, they are more likely to i) score positively on the *RU* dimension and ii) demonstrate positive attitudes and behaviours towards security within the organisation, scoring positive on *AS*. (It is useful to bear in mind that the interview questions were framed in such as a way as to require participants to discuss "*fictional colleagues*" which was a device to capture security themes such as *AS* and *RU* without attribution (see Chapter 9.5 *Limitations*)). Guided by the BSG framework, I would expect that such a cohort would be more likely to be positioned within the *Open* quadrant, reflecting an understanding of the cyber risks as well as a positive attitude towards security.

The results supported this hypothesis in that all 11 SIRO interview transcripts were coded positively for both *AS* and *RU* and that the attitudes and behaviour expressed in the interviews are mostly located within the *Open* quadrant. As the scoring system follows the same parameters as referred to in Case Study 1 (*Chapter 5.5*) , it is useful to remember that the scores are not meaningful in and of themselves; rather that positive scores indicate the positive aspects of the dimension and the negative scores indicate the negative aspects of the dimension. This highlights one of the limitations of the BSG, where the idea of being more or less of a particular quadrant, in this case, more or less *Open* is not meaningfully captured via the scoring system. Indeed, there were variations in the scores that indicated that some employees were 'low' *Open* whereas others were more strongly so. This point will be extended in the limitations section (*Chapter 9.5:Limitations*).

The analysis indicated that the participants demonstrated generally positive affective attitudes, feelings and behavioural preferences towards both security and also reasonable levels of competence in relation to identifying security risks in the workplace. These measures not only encompass the participant's stance towards security and competence around identifying risks but also their appraisal of "*fictional colleagues'*" security stance and risk competence. In line with the Case Study 3 proposition (see *Chapter 1.4.1*) , I would expect this group to demonstrate a positive attitude towards security policy and positive understanding of cyber risks, and that is demonstrated via the finding that this entire cohort are situated in the *Open* quadrant within the BSG.

The finding that this group are located within the *Open* quadrant supports the initial proposition although there are emergent themes from the qualitative analysis that need to be explicated in a more granular way. These themes, or '*security stories'* are useful to unpack the SIRO's perceptions of staff security behaviour in more detail. Summaries of some of the central themes from the qualitative analysis are presented here to provide deeper information in relation to security behaviour within the various Organisation D departments. It is important to recognise that this group are likely to have a vested interest to espouse security values and secure behaviours to safe-guard information assets.

The major themes that emerged include:

i) the importance of senior sponsorship or simply seniority as a SIRO to inculcate security awareness at board level and influence policy

The first theme to explore is the importance of senior sponsorship at board level where P10 highlighted that being a "*heavy hitter*" helped them influence security policy at a senior level. In particular, the employee notes that they have access to a "*fictional Chief Executive*" and are therefore able to inform and guide him/her in relation to security policy; i.e. influencing the key security decision-maker. Similarly, P9 noted that whilst they did not have a 'technical' background - their position on the board assisted them in influencing the executive committee to take security seriously. Clearly SIRO presence at board level is central to changing senior decision-maker's attitudes towards security. A practical recommendation from this, is that security needs to be championed at senior levels such as at board level (P9, P10) or within information management committees (P8) within organisations to influence security culture and policy.

ii) the SIRO's pragmatic approach to the assessment of risks

The reference to a *pragmatic* or balanced approach to decision-making reflects the SIRO's understanding of organisational needs, which incorporates reconciling security needs with the operational focus of the business. This theme of taking pragmatic decisions emerges from the interviews (P3) who acknowledges that - whilst s/he is not a technical expert – s/he integrates the needs of the business into their thinking about security risks. Specifically, P3 identifies there is conflict between operational and security teams, reflecting different perspectives, which is important to consider in relation to gathering relevant risk management intelligence. This gathering of information across business and security functions is key since individuals who are purely technical and work in security departments may not have the oversight to incorporate business decisions into security policy. P3 suggest that there needs to be a trade-off between the usability of technical mechanisms including security tasks that are quick and easy to perform, with the level of security required for the job (see *Chapter 9:Conclusions*).

iii) perceptions around senior circumvention of security policy and the impact on the organisational security posture

Another key issue that emerged was around senior circumvention of security policy. P1 noted that "*senior leaders are often sociopaths*" who think the rules do not apply to them and may therefore feel entitled to breach security policy. The main exemplar of this appears to be the sharing of passwords with personal assistants (PAs) in order to access email accounts – something described by P6 as an "*open secret*". Similarly, another employee (P2) referred to an internal audit which identified that password sharing with PAs as being relatively commonplace i.e. "*…it was only my PA – I needed the thing on my system".* P1 referred to senior "*fictional*" members of staff as "*the biggest risk*" since they were more likely to ignore the rules around removable media such as USBs and also more likely to share drives with other "*fictional colleagues*". P1 also noted that circumvention of security by "*fictional*" senior staff may not just be a symptom of perceiving that the rules do not apply to them, but also due to time-pressure associated with getting primary tasks accomplished, thereby trading off security compliance with job focus. This, of course, is also the case for lower level employees since they are necessarily focused on their primary task and require security tasks to be less burdensome in terms of time and cognitive effort (Kirlappos et al., 2013).

iv) Limited support and training for SIROs

Another theme that emerged was the importance of support and training for SIROs themselves, to enable them to improve in their knowledge and develop a community in practice with other SIROs. Several participants (P8, P9, P5) referred to the benefit of having group events with SIROs to share information about security risks and specifically committees that help the SIRO make security policy more actionable for staff. P9 stated there was a "*lot of assumed knowledge*" associated with role of SIRO and there is a theme around SIROs requiring more information or networking events to perform their roles effectively (i.e. P6) and the role needing to be "*professionalised"* (P2). Indeed, one individual refers to the importance of personal development to help the individual upskill into the SIRO role as well as citing support from colleagues as very important in building capability (P3). Another employee (P1) suggests that there is "*no real community"* when SIROs get together, and argues that SIROs would benefit from more "*narratives*" and security *"stories*" to communicate "*best practice*". P2, in particular, highlights the need for a "*buddying*" mentoring system for SIROs to develop their skills. Participants also suggest that the SIRO would benefit from being perceived as a professional job in itself which would require ongoing skills training and community of practice to ensure standards are met.

The sense that some participants did not feel fully supported or trained to take on the SIRO role was a salient factor. For instance, P7 highlights that "*a peer mentoring structure*" might be of value in supporting the SIRO in their role since they suggested there was no formal peer support in place.

This was not consistent throughout the entire cohort; P10 referred to having a mentor and being well supported in the role, although this theme was not echoed by many of the SIROs interviewed. Of course, not all SIROs actually chose to take on the role since some participants highlighted that the role was imposed upon them; hence one participant's comment around roles being given to individuals when they would rather not do the job and furthermore, not fully skilled to take on the role:

"one of those (SIRO) roles gets given to someone to in the organisation, when people think they'd rather not have that, I came in and got given the role, bit of upskilling being able to identify people who I can trust". (P3)

This contrasted with the tone of P11 who described him/herself as being much more technically focused, and therefore not concerned about requiring more training to take on the mantle of SIRO. On the contrary, their self-perception was as someone who would be able to "*keep their eyes and ears open*" for interceptions that may affect internal and external systems and networks, demonstrating a more technical awareness of the challenges the SIRO faces. Similarly, P4 demonstrated a sophisticated understanding of the security landscape, speaking fluidly about the need for a new understanding of security paradigm such as recognising the limits of security perimeterisation and the awareness of "*inside attack threats*". So the background of the SIRO is likely to influence their approach to their role, where less technical individuals may bring strengths in terms of understanding of the business but may not appreciate some of the technical challenges. Therefore one recommendation for developing SIRO capability, is to ensure appropriate *personalised* training.

v) Variable employee awareness around security policy and circumvention including challenges associated with password management

In relation to awareness of security policy and compliance, many of the participants indicate that most "*fictional colleagues*" want to comply and do their best to do so. P11 considered that "*fictional staff*" are aware of policy but may "*slip into bad habits"* and circumvent policy – for no other reason than a desire to help external customers. S/he cited a particular example where a "*fictional"* member of staff stored a password in the database in plain text so that they would be able to help customers who had forgotten their passwords by reading off their for them. This behaviour created a serious security risk but the motivation for the circumvention was to assist customers. Similarly, P3 describes "*fictional colleagues'*" tendency to leave things on their desks, thereby breaching an unenforced clean desk policy. S/he attributed this non-compliance to "*bad habit*" rather than any malicious intent. P3 suggests that security culture would be improved by being more open about breaches, i.e. "*creating an environment where people can say something has happened*" and frequently distributing security messages throughout the organisation to encourage people to report the "*little incidents*".

Nevertheless, 7 of the 11 participants interviewed suggested that "*fictional staff*" are aware of, or at least have some understanding of security policy. For instance; P1 "*Knowledge of policy well known*", P7 *"everyone is conscious of [security]"* P3 "*most of the time [people] behave in a way that's security conscious*", P10 "*people are familiar with the policies relevant to their role (80%)*", P11 "*most people are reasonably aware of security",* P8 *"most staff are aware…",*P6 "*security policy – yes they are aware".* However, P6 also identifies that "*fictional colleagues*" are aware of security policy but do not always understand it because "*we use too much jargon*".

Three of the participants suggested that "*fictional staff*" were not aware of policy; for example, P2 states that *"most fictional colleagues – don't know about security policy"* and P9 noted that "*most fictional colleagues don't think there is a security policy, probably because there isn't something that brings it all together in a clear way".* Further, P5 stated that security policy was "*not something most fictional colleagues give a great deal of thought to*" and delineates between staff complying with security policy but not necessarily being *explicitly* aware of organisational security policy. P4 highlights that security awareness and compliance may be a more subtle decision, in that *"fictional colleagues"* may think about security in relation to appropriateness for them and the organisation.

P10 states that there are so many new policies that it is difficult to know (and know how to be compliant with) all of them. The other security compliance issue emerging is the idea that staff want to "*do the right thing*" and that they "*really care*" – which highlights the importance of affective responses to security (P3). However, P3 also notes that staff may feel they are inhibited from "*doing the right thing*", because complicated security policies and processes as well as technical mechanisms that are not sufficiently usable act as blockers, and therefore shift individuals scoring positively on *AS* to a *Negative AS* score.

P4 describes *"fictional colleagues"* as demonstrating poor security behaviour in relation to passwords e.g. they re-use passwords for several systems. S/he attributes this primarily to inadequate technical infrastructure, such as lack of a single sign-on systems, which would mean that employees would not have to remember/create multiple passwords. P6 also attributes not having a single sign-on system for remote working specifically – there is single sign-on internally – to poor security behaviour around passwords created by having to remember too many passwords.

Another example of circumvention that occurred in error was provided by P2, who described an incident with a "*fictional*" member of staff relating to confidential data. Essentially, the individual believed they had completed the steps required to secure the data and therefore did not perceive any risk. However there were many steps required to securing the data and since the individual only completed 95% of the security process – thinking they had completed the process and the data was secure when it was not - human error lead to sensitive data being leaked. The security process was so complicated it was not adequately usable.

A similar type of incident, P11, relates to a "*fictional*" member of staff storing passwords in plaintext in order to allow customer service members of staff to assist customers who had forgotten their passwords by telling them what it was. P11 attributed this security lapse to a genuine desire to help others, and reflected *"fictional colleagues'"* lack of security *RU* rather than any malicious intent.

Malicious circumventions were also described in the interviews. P9 did refer to an incident which resulted in a data leak where a "*fictional employee*" was inappropriately downloading data at the weekend and "*alarm bells*" should have rung , i.e. that the breach should have been identified by the organisation at the time. The incident was not due to an honest mistake, since the "*fictional*" individual had come into the organisation at the weekend to download the data. Furthermore, there were consequences associated with this incident, nature since the employee refers to there being pressure put on "*a government department"* due to the sensitive nature of the data, highlighting that not all security transgressions are a result of human error.

vi) Lack of clarity associated with security messages and transparency regarding security communications and security training

The clarity of security messages appears to be a factor in improving perception of security risks. For instance, P6 refers to the fact that *"fictional colleagues"* need more narratives and security stories and less security jargon, to understand policy better. P6 also refers to the need to tailor security messages so that they are more impactful and reach employees with different backgrounds and therefore different levels of *Risk Understanding* in a meaningful way. This ties in with the idea that making policy more accessible to the layperson by not using jargonised language may, in turn, increase cyber risks more tangible. Similarly, P1 refers to the need for more case studies and narrative-based stories to communicate security issues to employees in an engaging way.

Related to this theme of clear security messages, is the act of encouraging a transparent and honest approach regarding security risks. P3 in particular refers to "*fictional senior staff members*" choosing not to attend security meetings as they felt they were being reprimanded by the security team. The employee highlights that taking discussions "*off-line"* in order to understand from senior management what is actually happening in relation to security, helps facilitate better communication and understanding of security incidents and potential risks.

This idea of making security more engaging and relevant is a general theme related to security training offerings, with P11 suggesting they are not effective, and that more effort is required to make it more engaging since it is a "*dry topic*". This theme is not consistent throughout the interviews however, since P10 refers to the positive perception that staff had regarding their data protection training course which was embedded in the security induction training piece.

vii) introduction of policies and technical mechanisms to facilitate employee positive security behaviour.

Technical mechanisms that enable individuals to adhere to security policies also emerges as a theme from the interviews. For instance, one employee (P2) refers to using Boardpad, an application that allows "*fictional*" senior management to access sensitive material without having to print it. The same employee also mentions a classification system called Egress which automatically classifies documents and controls the distribution of sensitive documents i.e. will not allow certain levels of documentation to be emailed.

CHAPTER 8: VALIDATION QUESTIONNAIRE FOR ORGANISATION D

8.1 Aims of validation

In addition to the qualitative interviews conducted across government departments within Organisation D, a follow-up survey was designed to explore how staff perception of security behaviour within Organisation D. The aim of this survey was to derive a snapshot of the security posture by surveying security attitudes and behaviour within Company D. This snapshot reflects the main department within Organisation D although it must be acknowledged that the SIRO cohort was collated across a variety of Government departments. Nevertheless, this main department set the overall security policy the SIROs were required to implement in their departments, linking the relationship between the departments together. (The fact that not all the SIRO departments were surveyed in this validation study will be discussed in *Chapter 9.5.1: Limitations*).

Crucially, the survey results are used as another source of data, in addition to the qualitative interviews, to triangulate the results in relation to the security posture within Organisation D to improve the validity of the research. Indeed, when using case-studies, Yin (2003) advocates the use of data triangulation to strengthen understanding and the validity of inquiry .

In terms of the construction of the survey, the items were selected from the Case Study 3 interview data to reflect the four different quadrants of the BSG, that is *Open*, *Hidden*, *Blind* and *Unknown* zones. Four items were representative of each of the quadrants and the participants were asked to decide whether the statement was *True* or *False* in relation to "*fictional colleagues*" security behaviour (For further information, see *Chapter 8.3 Methodology* below).

8.2. Participant Recruitment

It should be noted that this cohort was different from Case Study 3 participants, in that this group of employees work within the same location within Organisation D, rather than across separate departments as with the SIRO representatives. Furthermore, this cohort was comprised of a random cross-section of employees that were available during the two days of data collection, which is distinct from Case Study 3 which required the parent organisation, a large Government department, to manage and co-ordinate the recruitment of SIRO participants. Participants for the survey were recruited via internal signalling within the organisation via the use of the company intranet. There was also a physical aspect to the participant recruitment where two members of staff informed other members of staff that a security behaviour staff survey was being conducted should they wish to take part.

Participants' names and job titles were not recorded to ensure the anonymity of the participants. Each participant was presented with an information sheets and required to sign a consent form demonstrating their willingness to participate in the survey.

In consultation with my sponsor at Organisation D, the surveys were administered on paper rather than online to minimise data protection issues. For instance, one of the key concerns in terms of assuring anonymity was that employees did not want to link their emails to the survey. Therefore distributing the surveys via paper removed that issue, and although participants were required to sign a consent form, the consent forms were not stored with the completed surveys making it impossible to know who had completed each survey. Moreover, participants were asked not to add their name to the actual survey itself. The survey was brief to encourage participation, only taking about 5 or 6 minutes for the participant to complete.

8.3. Methodology

Two Organisation D employees, who were not participants, were charged with assisting me in the participant recruitment process, selecting the departments where employees were invited to participate in the survey since I was not permitted to administer the survey unaccompanied. They indicated that the participants within the sample population worked across departments and held a positions at varying levels within Organisation D.

As indicated, this study was conducted using paper and pencil. Each participant was presented with a consent and information sheet to read and sign if they give their consent to proceed with the study. Next, a short 16-item survey that included brief statements relating to security behaviour within the organisation was presented to the participant. The participant instructions for the questionnaire emphasised that the views expressed through the item selection did not represent the participant's *personal* security behaviour, but rather referred to "*fictional colleagues*" in the organisation. This was consistent with the approach taken for the interviews with the aim of encouraging participants to answer the questionnaire candidly. They were asked to decide whether each item was '*True*' or '*False*'.

The items were taken from analysis of the Organisation D qualitative interviews on security behaviours which measure positive and negative aspects of *AS* and *RU*. The permutations of the *Positive* and *Negative AS* and *RU* dimensions which reflected each of the quadrants within the BSG were used as the basis for the questionnaire; i.e. *Open (Positive AS, Positive RU), Blind (Positive AS, Negative RU), Unknown (Negative RU, Negative AS)* and *Hidden* zones (*Positive RU, Negative AS*). Consequently, four items were allocated to the *Open* quadrant, four items to the *Hidden* quadrant, four items to the *Blind* quadrant and four items to the *Unknown* quadrant (see *Appendix 6* for the full questionnaire).

Exemplars of the items for each quadrant include;

1. Colleagues generally lock their computer screens, you never know who might be passing by and what they might do with the data. **(OPEN)**
2. The team is completely trustworthy and so occasional password sharing is not a problem. **(BLIND)**
3. The wrong emails sometimes disappear in spam filters, which can be annoying, but people understand the need to screen emails in case they infect their machine. **(HIDDEN)**

4. Colleagues often leave work documents on their desks and do not always lock them away when they leave the office. **(UNKNOWN)**

8.3.1. Scoring

In order to ascertain whether a participant's responses were located within the *Open, Hidden, Blind* or *Unknown* quadrants, or indeed a combination of those quadrants, the participant was required to answer *True* (denoted by T) or *False* (denoted by F) to each question. Each item was assigned to one of the four BSG categories of *Open, Hidden, Blind* and *Unknown.* The number of '*True*' items was added up to reflect each category, where the highest number associated with any one category would suggest an overall pattern of responses within each quadrant. For instance, if a participant scored *True* for all the (4) questions associated within the *Open* mode, and demonstrated a mixed pattern of True or False across the other dimensions, they would be classified as demonstrating a predominantly *Open* style of security behaviour. Participants whose scores were spread equally across more than one quadrant were recorded as demonstrating both those styles of behaviour. Each item was not explicitly associated with each category on the paper survey i.e. the participant was not provided with a definition of the quadrants nor were the labels *Open, Blind, Hidden* and *Unknown* assigned to each item. The participants were simply instructed to consider whether the item reflected the security behaviour of their colleagues or not and were therefore not aware of whether the item reflected an *Open* quadrant or a *Hidden* quadrant for instance.

8.3.2. Results

SECURITY MODE	NO. OF PARTICIPANTS	%
OPEN	46	66%
HIDDEN	3	6%
BLIND	1	1.4%
UNKNOWN	2	2.9%
2 QUADRANTS	9	12.85%
3 + QUADRANTS	9	12.85%

Table 7: Organisation D Survey Results

The results from the survey demonstrated that 46 out of 70 participants responses were predominantly distributed within the *Open* quadrant. This represents approximately 66% of the population sampled, which constitutes over two-thirds of the Organisation D sample. This finding is, to some extent, in line with the findings from Case Study 3, which suggested SIROs description of "*fictional colleagues*"' falls into the *Open* quadrant in relation to their security posture.

In relation to the other quadrants, 3 out of 70 participants were predominately distributed within the *Hidden* quadrant which represents almost 6% of the population sampled, whereas almost 3% (2 participants) were within the *Unknown* quadrant and 1.4% were distributed predominately within the *Blind* quadrant (1 participant). A number of participants' responses were scattered across quadrants reflecting different security modes; i.e. 12.85% (9 participants) across 2 quadrants and 12.85% (9 participants) across 3 or more quadrants.

8.4 Discussion and limitations of validation survey

Approximately two-thirds of the participants (66%) of the 70 participants sampled within this quantitative survey carried out at Organisation D demonstrated a predominantly *Open* mode of security behaviour. In relation to the other quadrants, the percentages were low as expected; with 6% of participants demonstrating a predominantly *Hidden* mode of security, 1.4% of participants demonstrating a *Blind* mode and 2.9% demonstrating an *Unknown* mode. To some extent, this finding corroborates with the qualitative SIRO interviews which scored all of the participants as demonstrating an *Open* mode of security behaviour.

There are dissimilarities between these two cohorts that should be outlined here however. The interview group were senior managers (SIROs) with some responsibility for risk management within the organisation whereas the sample group who randomly participated in the survey were likely to represent different levels, positions and departments across the organisation. I deliberately did not collect any demographic data on this randomly selected cohort, in order to assure participants that there was no personal data collection, therefore it is not possible to identify the employee's grade or position. These differences in background may explain the differences in *AS* and *RU* scores. It should be noted that the sample size was relatively small (70 participants in total) and it would be interesting to identify whether similar patterns of responses would be identified in larger sample sizes.

There are also various limitations associated with the construction of the questionnaire which should be noted. As discussed earlier, (*Chapter 8.3: Methodology*), the individual items in the questionnaire incorporated Positive and Negative aspects of *AS* and *RU* which emerged from the qualitative analysis since, as far as I am aware, there are no existing survey instruments that explicitly reflect the four BSG security modes; *Open, Hidden, Blind, Unknown*. Although the items demonstrated face-validity since they were derived from the interviews on security behaviour, a short-coming of this questionnaire is that it is unvalidated. Although research with the IS literature has used unvalidated questionnaires to explore a topic where no appropriate instruments exist (e.g. Anderson, 2001) clearly, this would be a key area to address in relation to future research.

Another limitation of the questionnaire was the decision to use a dichotomous (*True* or *False*) item response, in particular, the way the questionnaire suggests a predominant security mode is denoted by a higher number of '*True*' items related to that quadrant. This is a simplistic approach in conveying information about a individual's primary security mode, since whilst they may register a higher allocation of *True* responses within a given quadrant, they may also have positive responses, albeit fewer in numbers, across the other quadrants which is not represented via this approach. It is, however, theoretically possible for the participants' security modes to be straddled across 2, 3 or 4 quadrants, providing there are equal numbers of *True* responses across quadrants. Whilst this approach conveys more information about the participants’ observed security modes i.e. inconsistency of security behaviours, it does not force participants to select between security modes.

Despite the limitations highlighted above, the purpose of the questionnaire was primarily to establish another data point to check the observed BSG security modes with Organisation D, and in this regard, it achieved this aim. As discussed, development of this simple survey in relation to establishing validity and reliability would be an area for future research.

CHAPTER 9: CONCLUSIONS

9.1 Summary

Organisations have sought to minimise the risks to assets, associated with security breaches, by implementing risk management policies and processes such as those proscribed by the ISO27001 series. These mitigations have been undermined by human circumvention of security policy (PwC, 2015), therefore greater emphasis has been placed on improving security compliance within organisations. Best practice has suggested that security awareness training will improve security risk awareness and behaviour, but there is concern that this does not work (Caldwell, 2016). Studies have indicated that these interventions do not address the issues surrounding non-compliance where security is not sufficiently usable for their staff to comply even if they want to (Kirlappos et al., 2013). Equally, burdensome security mechanisms which value employees' time and effort at zero (Beautement et al., 2009, Herley, 2009) do little to improve compliance behaviour.

In unpacking this problem, a better understanding of the drivers behind employees' security behaviour, in particular how i) employees *understand* security risks and ii) their *attitudes*, *feelings* and behavioural *preferences* towards security, is necessary. There is a limited research in the IS literature exploring employees' *understanding* of security risk as well as *affective* attitudes and corresponding behaviours towards security compliance. One of the antecedents of my research is Farahmand et al. (2013) who created a twodimensional model consisting of *understanding* and *consequences* to map a cohort of 42 senior executives' security risk perceptions of critical incidents. However, they did not focus on the *affective* aspects of security, which encompass feeling and attitudes and behavioural preferences in relation to security which this research attempts to address. Another antecedent, Massie & Morris (2011) at NASA, drew on existing psychological models such as the Johari Window (Luft & Ingham, 1955) to create a model of risk investigating how differing personalities assess '*unknown unknowns'*. My research builds on Massie & Morris' model in that it also revises the *Johari Window*, but applies this to the domain of information security and investigates the effect of *RU* understanding and *AS* on security behaviour, rather than exploring personality and risk.

This dissertation therefore aimed to explore how *affective* responses to security, which include positive and negative attitudes, feelings as well as behavioural preferences towards security (*AS*), and security *Risk Understanding* (*RU*) can help us better understand organisational security behaviour. In order to examine the relationship between *RU*, *AS* and the implications for different modes of security behaviour, I created a framework, the BSG[9] (Beris et al., 2015) which was a revised version of the Johari Window (Luft & Ingham, 1955) to express four different security modes; *Open, Blind, Hidden* and *Unknown*. I used this BSG framework and the associated methodological approach to categorise participants' security stories about "*fictional colleagues'*" security behaviour into these quadrants across

[9] Dr. Beautement offered valuable insights into the development of the BSG including feedback on delineating the AS & RU codes and acting as a 2nd coder

three case studies. Study 4, a validation study which consisted of a simple survey, was also conducted within Organisation D to triangulate the data. The benefit of this methodological approach was to quantify *AS* and *RU* scores to explore the role of these two dimensions in relation to security behaviours. The other benefit of this approach allowed me to examine the similarities and differences between unique employee samples.

9.2 Research aims/questions revisited

The primary research aim (see *Chapter 1.4.1 Research Questions, Q1*) focused on what can be learned from delineating the dimensions of *AS* and *RU* from employee interviews to better understand employee security behaviour. The findings from the qualitative analysis and the case studies suggest that *AS* emerges as a separate dimension from *RU,* indicating that employees may recognise the security risks, without necessarily demonstrating positive feelings, attitudes and positive behavioural preferences towards security (*Positive AS*). This has not been tested statistically however.

Implications for how the positive and negative aspects of *AS* and *RU* could potentially be used in industry to understand more about employee security behaviour and the BSG framework (*Chapter 1.4.1 Research Questions, Q2 and Q3)* are outlined later in this chapter (*Chapter 9.4.1 Contributions to Practice).*

I analysed two unique cohorts (Organisation C and D participants), which consisted of Government employees and a group of SIROs, in respect of *AS* and *RU*. Using the BSG as a guiding framework, the results have suggested (see *Chapter 6*) that *RU* is not sufficient alone to improve security compliance and that *Positive AS* may potentially improve security behaviour i.e. for behaviour to be more '*Open*'.

In relation to the final research question (see *Chapter 1.4.1 Research Questions, Q4*), the main insight is that organisations and security practitioners could *explore* harnessing *AS* as a potential security '*motivator*'. Notwithstanding, employees who demonstrate understanding of security risks (*Positive RU)* and security mechanisms that are usable (*security hygiene)* are also factors suggested to improve security behaviour. These findings will be discussed in the following section (see *9.3. Substantive contribution & 9.4. Methodological contribution* below).

9.3 Substantive contribution

In summary, one of the primary findings from this research suggests that *positive affective* attitudes, feelings and behavioural preferences towards security *may* play a key role in driving employee security behaviour. As previous research has outlined (see *Chapter 3*), the affect-as-information hypothesis (Clore et al., 2001) suggests that affective responses shape decision-making and therefore behaviour. Further, positive affect has been linked to non-conscious pursuit of goals (behaviour) in that when behavioural states are associated with positive (as opposed to negative) affect, the individual is likely to be more motivated to perform the target behaviour (Custers & Aarts, 2005). If organisations are to improve their security culture and have assured *security hygiene* is in place, where employees recognise the risks and are able to comply with policy, harnessing *AS* is recommended as a fruitful area to explore.

This finding needs to be interpreted with caution however since further research is required to explore the role of *AS* in respect to security behaviour (see *Reflections and limitations 9.5*.).

9.3.1 The role of AS in driving security behaviour

The importance of focusing on *AS* is particularly exemplified by Case Study 2 (Organisation C), which demonstrated that employee competence around recognising and identifying security risks, operationalised as *Positive RU*, is not sufficient by itself to ensure security compliance. The interviews for Case Study 2, conducted at a UK Government department, Organisation C, with a sample of 20 employees who worked across departments and levels within the organisation (see *Chapter 6*) demonstrated *Positive RU*. This cohort worked within a security context, and therefore one would expect that employees performing security tasks within such a context were likely to be more conscious of security risks than most employees working within other contexts. The results supported this proposition since both myself and coder 2 rated all of the sampled cohort as demonstrating *Positive RU.*

It should be noted that the pattern of *AS* scores were mixed, where I categorised 25% of the cohort as demonstrating *Negative AS* scores and coder 2 10%. Nevertheless, despite the differences between *AS* coding scores, the overall pattern of coding was similar, in that there was 75% agreement across both coders in terms of rating employees positively or negatively in respect of *RU* and *AS* and the allocation of quadrant i.e. employees were predominantly grouped within the *Open* quadrant, with a much lower percentage in the *Hidden* quadrant. What is most relevant about the Case Study 2 results, is that it suggests that when *Positive RU* is evident within the employee cohort, it does not necessarily mean that employees will follow security policy.

Negative AS scores, coupled with *Positive RU*, imply employees are operating within the *Hidden* quadrant in the BSG framework, suggesting they may not hold positive attitudes, feelings and behavioural preferences towards security. As a consequence of this expressed dissatisfaction with the security provision within Organisation C, some employees indicated that workarounds were created or security policy circumvented because colleagues were frustrated with the existing security provision. The qualitative summaries echoed this theme, where some employees expressed frustration at various security mechanisms and processes that caused friction alongside their primary role. An example of this is where employees referred to the practice of emailing work to personal accounts because they judged it easier than accessing systems remotely.

These findings resonate with the literature on affect, which link affective states with affective responses/behaviours (e.g. Santos & Boote, 2003) suggesting that negative '*affective behaviour'* may ensue when expectations are not met. In relation to Case Study 2 for instance, this may be one explanation for why employees who express dissatisfaction with security mechanisms/tasks create workarounds. An alternative explanation may be drawn from descriptive theories of decision-making, such as prospect theory for instance (Kahneman & Tversky, 1979) which suggests that in the domain of perceived gains, individuals may adopt a more risk averse strategy, and conversely in the domain of losses may become less risk averse. It is possible that security behaviours within Organisation C that circumvent policy, in other words 'risky' security behaviours, may be more likely to emerge when the recipient perceives security policy negatively (i.e. within the domain of losses). This may be an area for future investigation as it has not been explicitly tested within this research.

9.3.2 Insights gleaned from novel cohorts

The results from Case Study 3, which consisted of a cohort of Senior Risk Owners/Managers (SIROs) across various Government departments, was rated as demonstrating *Positive AS* scores and *Positive RU* scores. This is in line with the proposition for Case Study 3, which one might expect from this cohort since SIROs are effectively stakeholders in safeguarding organisational assets which includes managing or inputting into the organisation's cyber risk strategy. This echoes findings from the IS literature which emphasises the importance of the employee adopting a participatory role as a "*principal agent*" in relation to improving security behaviour (Kirlappos & Sasse, 2014).

As mentioned in the methodological chapter (see *Chapter 4*) participants were not their expressing personal views on security necessarily, but describing patterns of behaviour they had observed from "*fictional colleagues*" within the organisation.

This finding did not imply that participants were *uncritical* of policy, on the contrary they identified many areas for change (see *9.5. Reflections and limitations*). The more critical themes tended to be framed within the context of how policy could be improved however, which was rated as *Positive AS*. Overall, Case Study 3 supported the proposition that Senior Risk Managers/Owners are likely to demonstrate *Positive AS* and *Positive RU*. findings suggest that harnessing affect could play a role in changing organisational feelings, attitudes and behavioural preferences about security policy/security behaviour, although further research is required to experimentally test the role of *Positive AS* on security behaviour. As discussed, it is suggested that *security hygiene* needs to be established and employees are competent in recognising and identifying cyber risks in the work environment.

9.4 Methodological contribution

As far as I am aware, the development of the Behavioural Security Grid (BSG) is a novel approach in presenting types of employee security behaviour in relation to affective responses to security and the employee's understanding and recognition of security risks (Beris et al., 2015). This two by two framework incorporating the dimensions of *Affective Security (AS)* and *Risk Understanding (RU)* represents a unique *methodological* approach to enable security and organisational managers to visualise the types of security behaviour expressed via the sample of employees interviewed. It builds on an existing framework, the *Johari Window* (Luft and Ingham, 1955) which emphasises interpersonal differences and levels of awareness between individuals and others, but revises the model to i) incorporate risk understanding and affective responses as a way of understanding security behaviour ii) uses the *Johari Window* quadrant labels as a way of expressing different modes of security behaviour instead of expressing differences between self and others as in the original model.

Case Study 1 demonstrated that the BSG can be used to distinguish differing organisational populations on the grid; since four of the sub-categories related to *RU* and *AS* between Company A and B were shown to be significantly different. These included a significant difference between *Strong Positive AS, Strong Positive RU, Weak Positive RU* and *Strong Negative RU* between Company A and B. With the exception of *Strong Negative Risk Understanding*, the other 3 categories suggested that Company B had a more positive security culture. Overall, Case Study 1 indicated that the BSG could *potentially* be used to identify different organisational cohorts within its framework in respect of *AS* and *RU*, with the caveat that further validation is required (see *9.5. Reflections and limitations*).

Since the framework required further validation in order to explore whether using the dimensions of *RU* and *AS* would surface differences, or similarities in security behaviour amongst specific organisational cohorts, two further case studies were conducted to explore this. Case study 2 involved conducting in-depth interviews with 20 participants who worked within a Government department, referred to as Organisation C, and Case Study 3 which involved conducting in-depth interviews with 11 participants who acted as SIROs or directly assisted the SIRO, referred to as Organisation D. As indicated, a similar methodological approach was applied to both Case Study 2 and 3 in order to be consistent with Case Study 1. (However, Case Study 2 and 3 did not compare two different organisational profiles as demonstrated in Case Study 1 with the comparison between Company A and B). This included a similar interview question-set, with the caveat that additional questions about the SIRO's role were incorporated into Case Study 3 and the same qualitative coding approach, codebook and BSG framework.

The interviews I conducted for Case Studies 2 and 3 were designed to explore the BSG framework using the same methodological approach to coding and scoring to better understand whether different organisational cohorts are represented within the existing framework. In particular, the multiple case studies were used to test whether the two variables of *RU* and *AS*, in the context of the BSG framework, would demonstrate different patterns of security behaviour in relation to the *Open, Hidden, Blind* and *Unknown* quadrants in the BSG that would suggest specific security cultures.

In relation to Case Study 2, it was anticipated that participants within this environment were likely to demonstrate positive levels of *RU* since they worked in a security context, making security issues more visible. As discussed, whether the cohort was likely to be positive about security, in other words demonstrate *Positive AS* scores, depended on their *experience* of security within Organisation C. From the interviews, the results for Case Study 2 indicated that the Organisation C sample population demonstrated positive scores in relation to *RU* suggesting that the 20 participants demonstrated some competency around awareness and recognition of security risks in the workplace. Despite demonstrating *Positive RU* across all 20 participants however, the scoring showed that some of the participants expressed *Negative AS* scores. In relation to the BSG, this indicates that aspects of Organisation C security behaviour falls within the *Hidden* quadrant, reflecting behaviours that were inconsistent with security policy and characterised by *negative affect*.

As indicated, one of the main findings from the Case Study 2 analysis suggests that negative expressions of *AS* may be key in flagging up potential behavioural issues regarding security compliance. This insight is likely to be of practical use to organisational security managers, where evidence of *Negative AS* can be used as a prompt to investigate whether circumvention of policy is occurring and if so, why. (See *Chapter 9.3:Contributions to practice*). For instance, if security mechanisms are not usable or security training is simply a tick box exercise, indicating *security hygiene* is not in place, these are elements which must be addressed via organisational change interventions.

In terms of using the BSG to understand more about the types of security behaviour within the Organisation C cohort, the results imply that although *most* of the cohort was positioned within the *Open* quadrant, some of the employee scores were located within the *Hidden* quadrant, requiring further investigation. As discussed, one of the substantive contributions of this research is that the BSG may be used as the basis for a *diagnostic tool* to investigate what lies behind the expressions of *Negative AS* such as the practical barriers to security compliance and poor security communication etc. These insights could potentially help organisational development (OD) and security practitioners alike develop appropriate interventions to improve security culture.

In relation to Case Study 3, it was propositioned that this group would demonstrate positive levels of *Risk Understanding* since their role in the capacity of SIROs would suggest higher levels of information security risk competence. This resonates with research findings that suggest expert risk perceptions may be more sensitive in relation to new technologies due to the need for specialised knowledge (Savadori et al., 2004). Whilst the SIROs were asked about the security behaviour of "*fictional colleagues*", the security landscape is lensed through their own perspective on *RU* (see *Chapter 9.5 Limitations* section below). As the SIROs are involved in scoping and influencing security policy it was expected that they were likely to display *Positive Risk Understanding* and *Positive Affective Security* since they are, to some extent, stakeholders in the risk management process and as such their perspective is likely to be positive since there is a clear alignment of incentives. The results supported this. This was in line with research which suggests that employees who play a participatory role in security may engender more positive security behaviours (Kirlappos & Sasse, 2014).

The finding that the SIROs demonstrated *Positive RU,* i.e. competence in understanding security risks, resonated with research relating to stakeholders' perceptions of risk, which suggest that experts tend to be more accurate in their assessments than non-experts (i.e. Knowles et al., 2012). Given their position within the organisation, SIROs are more likely to demonstrate expert knowledge of information security risks than employees without this specialist aspect to their role.

In terms of using the BSG model as a guiding framework, both Case Studies 2 and 3 demonstrated a different pattern of results with the former straddling the *Open* and *Hidden* quadrants and the latter, remaining in the *Open* quadrant. This indicates that the BSG (Beris et al, 2015) *may* be a useful approach to better understand the differences and similarities within employee security cohorts in respect of *AS*, *RU* and the implied modes of security behaviour. The validation study, carried out at Organisation D, supported the findings that the security culture within the organisation was largely positive with approximately two-thirds of the sampled population reporting patterns of security behaviour that suggested security behaviour that might be assigned to the *Open* quadrant. It is important to note however that although this study validates the research data, no further conclusions can be drawn from it.

9.4.1 Contribution to practice: Methodological and substantive

The benefit of the BSG methodology is primarily practical in nature in that it is intended to be used to help security managers and other organisational stakeholders to visualise the said cohort in relation to i) how they *feel* about security and specifically the direction of that affect be it *positive* or *negative* as well as positive and negative attitudes and behavioural preferences towards security ii) their level of understanding, recognition and awareness of security risks in the work environment. These measures are used to position employees within the context of the four quadrants which express different modes of security behaviour implied by the permutations of *AS* and *RU*.

With the caveat that the BSG framework requires further validation (see *9.5 Reflections and Limitations),* it could assist in obtaining a qualitative measure of employee levels' of *AS* and *RU* which may be useful data to shape appropriate security interventions within the organisations. Such interventions may be targeted broadly at employees located within each of the quadrants; *Open, Blind, Hidden* and *Unknown*. For instance, employees situated in the *Blind* section might be suitable candidates for security training and awareness programmes designed to improve their level of awareness and recognition of security risks, whereas candidates in the *Hidden* section might provide security managers with rich data about *why* security policy is being circumvented if indeed it is.

The *substantive* contribution of this research in relation to industry is to harness employees' positive affective attitudes and behavioural preferences towards security i.e. *Positive AS*, as a driver to improve organisational security behaviour. From the many examples of circumventions described in this thesis (i.e. see *Chapter 7*), it is evident that despite demonstrating competency around *RU*, as in Case Study 2, staff are still likely to accidently breach security processes if the requirements are too complicated or time-consuming. Employee frustrations with security processes and mechanisms, may engender *Negative AS* which is manifested in the *Hidden* category of the BSG. Positive security experiences (*Positive AS*), combined with knowledge of the risks (*Positive RU*) may move employees into the *Open* security mode, where security behaviour is aligned with organisational policies.

Thus, the recommendation from these *security stories* is to ensure that security processes and related technical mechanisms are sufficiently user-friendly to encourage security compliance. This is in line with earlier research in the information security domain (see Adams & Sasse, 1999, Kirlappos et.al., 2013). Once *security hygiene* is assured and people understand the risks (*Positive RU*), it is suggested *Positive AS* may improve security behaviour and create healthy security cultures within organisations. Similar to Herzberg's two-factor theory (Herzberg, 1966) *Positive AS* may be perceived as a *motivator*, in improving security behaviour, whereas *RU* and usable security mechanisms could be characterised as *hygiene* factors. As discussed, additional research is required to further explore the impact of *Positive AS* on security behaviour.

The other *substantive* contribution from these research findings is generating new knowledge about unique populations such as the SIROs (Case Study 3) or Government employees (Case Study 2). These different cohorts, as demonstrated by all four studies within this dissertation, present differently in relation to *Positive and Negative AS and RU*. With the recognition of these differences, interventions can be tailored to meet the needs of that particular group within a given organisation security culture. Moreover, the qualitative summaries incorporating '*security stories'* unique to these cohorts, provide insight into their perspectives on security extends knowledge in this area.

9.5 Reflections and limitations

This section will present reflections on the research process, followed by a summary of limitations.

Reflecting on this process, it is clear that as the research aims became more specific, there were inevitably research directions that I did not explore. For instance, the literature review (see *Chapter 2*) referred to descriptive theories of risk including prospect theory and heuristic and biases associated with individual risk perception, which were not directly explored or tested within this thesis. Nevertheless, affect (Slovic et al., 2004), which emerged in the literature in relation to risk perception has been explored within these case studies. In particular, affective responses to security (operationalised as *AS*), emerged as a theme from the coding analysis and has been a key dimension of this research.

I selected the case study as a methodological approach for this research because it allowed me to explore the phenomenon under study, security behaviour, using employees within an organisational context as participants, rather than using students in a lab. From this process, the categories *Affective Security* (*AS*), *Risk Understanding* (*RU*) emerged as key dimensions from the empirical (interview) data with which to better understand security behaviour in the real-world. Teasing apart these dimensions as separate entities from the organisational context, has presented implicit challenges however. As Yin states in relation to case study research, the "*boundaries between phenomenon and context are not clearly evident*" (Yin, 2003, p.13) and therefore extracting *AS* and *RU* from the interview data on security behaviour has been an evolving process.

In order to guide the analysis and reduce bias across case studies, coding protocols were devised including definitions for the main two dimensions (*Strong, Weak, Positive* and *Negative AS and RU*). Notwithstanding, disentangling these dimensions from the environment is inherently difficult, because they are artifacts that have emerged from specific organisational cultures and teams, representing the views of the individual employees interviewed. Indeed, further research is required to test whether *AS* and *RU* are separate dimensions which are orthogonal to each other or whether they are in fact related variables.

Thus, the constraints of the case study approach needs to be taken into account. For instance, the case study can offer insights in terms of the theoretical generalisability of the research findings to theory building within the domain of security behaviour, but it is not using statistical approaches to generalise findings to larger populations (Yin, 2003, p.37) (see *9.5.1. Limitations* below).

A related challenge has emerged in using the case study approach as a primary research strategy to better understand the relationship between *AS*, *RU* and security behaviour. For instance, it is not possible using this research paradigm to statistically determine the *extent* to which *AS* may impact on modes of security behaviour when compared with *RU*. Kaplan & Duchon (1988) note that "*variance theories*" use static variables to determine the antecedents and outcome variables for instance, whereas qualitative approaches develop "*categories and meaning*" using an iterative process of coding and further data collection (i.e. multiple case studies). Consequently, questions relating to the percentage of the variance explained by *AS* as compared to *RU* in relation to security behaviours are not addressed within this research. Moreover, this thesis has not addressed the statistical analysis of *Positive* and *Negative AS* responses to security as antecedents to certain types of security behaviours.

An alternative approach to better understanding *AS, RU* and security behaviour can potentially be derived from considering the theoretical underpinnings associated with each dimension. For instance, *AS* draws from research which positions affect in relation to attitude-behavioural models (Ajzen, 1991) and affect is linked with behaviour, indicating that *positive* affective responses may motivate behaviour (Custers and Aarts, 2005) (see Chapter 1:

Introduction). *RU* has arguably a narrower focus in that it is used within this research as a measure of competence in recognising and responding to organisational security risks. However, the literature review (see *Chapter 2*) highlights that risk perception does not just depend on how knowledgeable about the risk an individual may be, particularly if the area is highly specialised (e.g. Savadori et al. 2004), but the influence of affect on risk perception (Slovic & Peters, 2006). In particular, the '*risk-as-feeling'* hypothesis (Lowenstein et al., 2001) suggests that affective responses to risk may not concur with cognitive evaluations of risk and drive behaviour.

These theoretical insights from the literature taken together with the findings in these case studies suggests that Positive *AS could be* instrumental in motivating types of security behaviours beyond cognitive evaluations of risk. This is a potential area for further study.

Using the BSG (Beris et al. 2015) as a framework to map the relationship between *AS* and *RU* and implied types of security behaviour (i.e *Open, Blind, Hidden* and *Unknown*) has been a visual tool to express differences between employees/teams. However, there are challenges associated with this strategy, namely that the nature of the grid may be overly simplistic. For instance, *Case Study 3* showed that the SIROs demonstrated *Positive AS* and *Positive RU* suggesting that the "*fictional colleagues*'" security behaviour was located in the '*Open*' quadrant. This was unsurprising to some extent, since the SIROs had a vested interest in the safeguarding of organisational assets and risk management.

The qualitative analysis presented richer data (see *Appendix 5*), in that there were themes relating to problems with senior leadership within the organisation for instance which were not captured via the grid. The SIROs '*Open'* security mode did not reflect some of the more problematic issues within the organisation, which the qualitative analysis uncovered. Due to these omissions, the BSG framework requires other data points and modes of analysis such as qualitative data, to elicit some of the contextual organisational factors that could impact on employee levels of *AS* and *RU.* This insight has implications for the construction of the BSG, suggesting that at this stage, the four quadrants can only be used as a guiding heuristic.

A further issue relates to the function of the BSG; although I originally envisaged it as a framework to reflect differences across organisational security cultures, in practice it is evident that it provides a snapshot of the individuals interviewed within an organisation on that given day. Themes associated with each cohort emerged, such as Organisation C employees demonstrating *Positive RU*, but varied responses in relation to *Positive* and *Negative AS*, but these findings can not be generalised across the entire organisation since only a small sample were interviewed. Further, it is possible that there are various security eco-systems within each organisation which may score differently in relation to *RU* and *AS.* This is consistent with research which suggests that organisations may have various "*micro*" security cultures within smaller teams depending on the manager's understanding of security policy (Kirlappos et al., 2014).

Other reflections on the research journey relate to how aspects of the analysis could have been improved. For instance, although code review meetings were conducted and the codebook and protocols were defined, improvements could have been made by recoding some of the data in respect to the *AS* dimension as there was some coder disagreement around this variable. Due to time and resource constraints, this was not possible but would be an aspect to consider for future research using this methodological approach.

Finally, the overall findings from this research *suggest* that *Positive AS* may be a missing element to improving employee security behaviours and organisational security cultures. Whilst promising, these findings do not demonstrate that *Positive AS* influences positive security behavior. Nevertheless, these case study findings could be used to build theory that could be experimentally tested (Eisenhardt, 1989). Using *AS* in an experimental study for instance may be a fruitful line to further investigate the impacts of *Positive* and *Negative AS* on security behaviour.

9.5.1. Limitations

There are a variety of limitations associated with this research which include:

i) There are limitations around the generalisability of this research. As discussed, a mixed methods approach was adopted, using 3 case studies and 1 quantitative survey. The 3 case studies were analysed qualitatively and then quantified to categorise security behaviour within the BSG framework (see *Chapter 4.2:Generalisabilty*). In relation to the qualitative aspects of the analysis, generalising from case studies can be challenging because it does not use statistical significance to establish causality or correlation, that can then be generalised to other populations. However, as Yin (2003) identifies, case studies do not rely on statistical generalisation but "*analytic generalisation*" (Yin, 2003). (The "*analytic generalisation"* from this research indicates that *Positive AS,* as well as *Positive RU,* is likely to be a driver of security compliance). The use of multiple case studies improved the validity of the research, as the same methodological approach including interview question set and scoring system was used to test the propositions across a variety of populations. Further, the scores were quantified which allowed me to categorise behaviour in relation to the BSG framework, which guided the analysis.

ii) The quantitative survey, used as another data to point triangulate the results of Case Study 3, did not fully reflect the same population as the SIRO cohort. The participants were recruited within the main site of Organisation D – but the SIROs were recruited across a *variety* of Government departments which included Organisation D. It was not possible to match the sample with other SIROs due to limitations of access and time and therefore, the participants were randomly sampled at Organisation D. Using matching samples for future research in this area may offer further insights into similarities and differences in *AS* and *RU* scores to compare scores across populations. In addition, the survey was unvalidated and the response format would have been improved by using a likert scale for instance. This would also be an area for development for future research.

iii) There were some differences in coding between myself and the second coder for Case Study 2 in respect of the *AS* dimension (see *Chapter 6.6.1 Limitations* for further discussion). The inter-rater reliability between coders was considered fair according to criteria set out by Landis & Koch (1977), although clearly this level of agreement could be improved. On reflection, this might have been achieved by selecting the same examples of text for both coders to code or as discussed, would potentially have improved with more coding experience.

iv) One of the potential weaknesses of the scoring is that the raw data ordinal is in nature. Further, the *AS* and *RU* code categories are classified as nominal data since they are delineated via *Positive, Negative, Strong* and *Weak* labels in order to distribute employees within the context of the quadrants of the BSG. Thus, it is not possible to meaningfully compare employees within the same quadrant as demonstrating more or less *Hidden* behaviour. This may be an area for potential research, where the two dimensions are quantified more sensitively to offer granular insights into employee security behaviour, beyond offering broad categorisations.

v) Finally, the interview questions were framed in such a way that the participants did not feel compromised about discussing security as the organisations had strict security policies in place. Therefore in order to ensure each participant was not concerned about revealing their views on security, they were informed that their views were based on "*fictional colleagues*", rather than attributable to their own perspective. The implications of this is that when attributing *AS* and *RU* scores to particular groups it should be with the caveat that this may or may not be applied to them personally, but rather reflect a composite of security behaviour within that particular organisational culture and setting.

9.6 Further Research

The findings from this research suggest that the way in which employees emote about security may influence their decision to adhere to or circumvent security policy. Indeed, the "*affect heuristic*" (Slovic et al., 2007) may play a part in terms of how employees evaluate cyber risks by being led by their *affective* rather than their *analytic* mind. Whilst this research has explored the relationships between positive and negative feelings, attitudes and behaviours towards security primarily via the use of case study, it has not explicitly tested the impact of affect on security risk perception itself. Further, as (Garg & Camp, 2012) note, the impact of the cognitive bias of availability on risk assessments and more broadly affective attitudes towards security *(AS)* may be a rich research stream.

In addition, this research did not *experimentally* test any of the behavioural biases outlined in the literature view such as the impact of time, hyperbolic discounting and optimism biases on security behaviour. In particular, the impact of time-pressure on affective responses to security and subsequent behaviour may be an avenue for future study since a theme that emerged from this study was the overhead of time required to complete security tasks which competed with the employee's focus on their primary task.

Related to the theme of *AS*, it would be relevant to understand more about employees' *emotional* discourse around security. This dissertation did not examine the *language* used to describe security risks or security breaches for instance. It would therefore be useful to explore whether there are individual differences, particularly in terms of seniority and gender in the way different groups build mental models about security, in relation to emotion.

As a logical extension of the BSG, *hypothetical* behavioural types emerged as a result of the analysis. For instance, in relation to Case Study 1 which consisted of Company A and B interviews, assigning each of the 93 employees above and below the mean for *AS Strong* and *Weak Positive* and *Negative* and *RU Strong* and *Weak Positive* created sixteen types based on the different permutations of the dimensions. These types are outlined in my co-authored *New Security Paradigms Workshop* paper (Beris et al., 2015). These hypothetical types are beyond the scope of this thesis and would represent a potential stream of research for future work since they require further analysis and validation.

GLOSSARY

Primary task refers to the individual's main focus such as they job role, which is differentiated from secondary tasks

Friction is the 'overhead' created when business and security processes do not align

Triangulation using multiple data points from which to gather evidence to investigate a particular phenomenon

Circumvention of security policy, where employees are acting in ways that do not follow the organisation's security policies or security processes/mechanisms

Affective Security (AS) positive and negative feelings, attitudes and behavioural preferences towards security, delineated as either *Positive* or *Negative and Strong* or *Weak*

Risk Understanding (RU) competency or understanding of information security risks, delineated as either *Positive* or *Negative and Strong* or *Weak*

P - Participant

***Formatting for quotations from interviews:**

… gaps in text

[ ] brackets refer to missing words in quotation. Words within brackets are inserted for the reader's comprehension/ease of understanding

REFERENCES

Abelson, R. P., Kinder, D. R., Peters, M. D., & Fiske, S. T. (1982). Affective and semantic components in political person perception. *Journal of personality and social psychology*, *42*(4), 619.

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS* (Vol. 3). Retrieved from http://www.cpppe.umd.edu/rhsmith3/papers/Final_session6_acquisti.grossklags.pdf

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. *Digital Privacy*, 329.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.

Adams, J. (1995). *Risk (London and New York*. Routledge.

Adams, J. (1999). Cars, cholera, and cows. *Policy Analysis*, (335), 1–49.

Adams, J. (2002). Do we have enough 'injidents'? *The British Journal of General Practice*, *52*(479), 454–458.

Ainslie, G., & Haslam, N. (1992). Self-control. *Choice over Time*, *177*, 209.

Ajzen, I. (1989). Attitude structure and behaviour. In A.R. Pratkanis, S.J.Breckler & A.G. Greenwald (Eds). *Attitude structure and function*, (pp. 241-274). Hillsdale, N.J: Erlbaum.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476–490.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security-Volume 105* (pp. 47–55). Retrieved from http://dl.acm.org/citation.cfm?id=1862275

Alhakami, A. S., & Slovic, P. (1994). A Psychological Study of the Inverse Relationship Between Perceived Risk and Perceived Benefit. *Risk Analysis*, *14*(6), 1085–1096. https://doi.org/10.1111/j.1539-6924.1994.tb00080.x

Anderson, K. J. (2001). Internet use among college students: An exploratory study. *Journal of American College Health*, *50*(1), 21-26.

Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *367*(1898), 2717–2727.

Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental Models of Computer Security Risks. In *WEIS*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.136.5601&rep=rep1&type=pdf

Aven, T. (2012). The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, *99*, 33–44.

Aven, T., & Renn, O. (2009). The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. *Risk Analysis*, *29*(4), 587–600. https://doi.org/10.1111/j.1539-6924.2008.01175.x

Barbour, R. S. (2001). Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *BMJ : British Medical Journal*, *322*(7294), 1115–1117.

Baskarada, S. (2014). Qualitative case study guidelines. *Baškarada, S.(2014). Qualitative Case Studies Guidelines. The Qualitative Report*, *19*(40), 1–25.

Beautement, A., Becker, I., Parkin, S., Krol, K., & Sasse, M. A. (2016, June 22). Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours [Proceedings paper]. Retrieved 30 September 2016, from https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

Beautement, A., & Sasse, A. (2009). The economics of user effort in information security. *Computer Fraud & Security*, *2009*(10), 8–12.

Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New security paradigms* (pp. 47–58). Retrieved from http://dl.acm.org/citation.cfm?id=1595684

Beris, O., Beautement, A., & Sasse, M. A. (2015). Employee Rule Breakers, Excuse Makers and Security Champions:: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (pp. 73–84). New York, NY, USA: ACM. https://doi.org/10.1145/2841113.2841119

Blais, A.-R., & Weber, E. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, *1*(1). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1301089

Blythe, J., Camp, J., & Garg, V. (2011). Targeted risk communication for computer security (p. 295). ACM Press. https://doi.org/10.1145/1943403.1943449

Blythe, J., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Symposium on Usable Privacy and Security (Soups) 2015*. Berkeley: Usenix. Retrieved from https://www.usenix.org/system/files/conference/soups2015/soups15-paper-blythe.pdf

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64–68.

British Intelligence Speaks Out On Cyber Threats | GRT. (2012, August 16). Retrieved 11 October 2013, from http://www.grtcorp.com/content/british-intelligence-speaks-out-cyber-threats

BS ISO/IEC 27002:2013.

Calder, A., & Watkins, S. G. (2010). *Information Security Risk Management for ISO27001/ISO27002*. IT Governance Publishing. Retrieved from http://www.jstor.org/stable/j.ctt5hh7jd

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security*, *2016*(6), 8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

Chamberlain, A., Crabtree, A., Rodden, T., Jones, M., & Rogers, Y. (2012). Research in the wild: understanding'in the wild'approaches to design and development. In *Proceedings of the Designing Interactive Systems Conference* (pp. 795–796). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2317956.2318078

Chandran, S., & Menon, G. (2004). When a Day Means More than a Year: Effects of Temporal Framing on Judgments of Health Risk. *Journal of Consumer Research*, *31*(2), 375–389. https://doi.org/10.1086/422116

Chen, L. S.-L., Lee, Y.-H., & Wang, S.-T. (2012). Impact of intangibility on perceived risk associated with online games. *Behaviour & Information Technology*, *31*(10), 1021–1032. https://doi.org/10.1080/0144929X.2011.624640

Chow, C. C., & Sarin, R. K. (2002). Known, unknown, and unknowable uncertainties. *Theory and Decision*, *52*(2), 127–138.

Clore, G. L., Gasper, K., & Garvin, E. (2001). Affect as information. Retrieved from http://psycnet.apa.org/psycinfo/2000-16445-006

Csillik, A. (2013). Understanding Motivational Interviewing Effectiveness: Contributions From Rogers' Client-Centered Approach: The

Humanistic Psychologist: Vol 41, No 4. Retrieved 18 November 2016, from http://www.tandfonline.com/doi/abs/10.1080/08873267.2013.779906

Custers, R., & Aarts, H. (2005). Positive affect as implicit motivator: on the nonconscious operation of behavioral goals. *Journal of personality and social psychology*, *89*(2), 129.

Ehrlinger, J., Johnson, K., Banner, M., Dunning, D., & Kruger, J. (2008). Why the Unskilled Are Unaware: Further Explorations of (Absent) Self-Insight Among the Incompetent. *Organizational Behavior and Human Decision Processes*, *105*(1), 98–121. https://doi.org/10.1016/j.obhdp.2007.05.002

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

Elahi, S. (2011). Here be dragons… exploring the 'unknown unknowns'. *Futures*, *43*(2), 196–201. https://doi.org/10.1016/j.futures.2010.10.008

Farahmand, F., Atallah, M. J., & Spafford, E. H. (2013). Incentive Alignment and Risk Perception: An Information Security Application. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6197226

Farahmand, F., Atallah, M., & Konsynski, B. R. (2008). Incentives and Perceptions of Information Security Risks. In *ICIS* (p. 25). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.188.5478&rep=rep1&type=pdf

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., & Grimes, J. (2015). Improving SSL Warnings:

Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2893–2902). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2702442

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, *13*(1), 1–17. https://doi.org/10.1002/(SICI)1099-0771(200001/03)13:1<1::AID-BDM333>3.0.CO;2-S

Fischoff, B., Slovic, P., & Lichtenstein, S. (1978). How safe is safe enough? A psychometric study of attitudes towards technological development'. *Policy Sciences*, *9*.

Fishbein, M., & Ajzen, I. (1975). *Beliefs, Attitudes, Intention and Behavior: An Introduction to Theory and Research*. Reading, M.A: Additional Welsey.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245.

Garg, V., & Camp, J. (2012). End User Perception of Online Risk under Uncertainty. In *2012 45th Hawaii International Conference on System Science (HICSS)* (pp. 3278–3287). https://doi.org/10.1109/HICSS.2012.245

Gigerenzer, G. (2004). Dread Risk, September 11, and Fatal Traffic Accidents. *Psychological Science*, *15*(4), 286–287. https://doi.org/10.1111/j.0956-7976.2004.00668.x

Gigerenzer, G. (2014). *Risk savvy: How to make good decisions*. Penguin.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. Los Angeles: SAGE.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133–144). New York, NY, USA: ACM. https://doi.org/10.1145/1719030.1719050

Herzberg, F. I. (1966). Work and the nature of man. Retrieved from http://psycnet.apa.org/psycinfo/1966-35012-000

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221–232.

ISO/IEC 27001 (2005).

Jackson, J., Allum, N., Gaskell, G., & Trust, C. (2006). *Perceptions of risk in cyber space*. Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.2577&rep=rep1&type=pdf

Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, *45*(1), 20.

Johnson-Laird, P. N., Legrenzi, P., & Legrenzi, M. S. (1972). Reasoning and a Sense of Reality. *British Journal of Psychology*, *63*(3), 395–400. https://doi.org/10.1111/j.2044-8295.1972.tb01287.x

Ka Ping, Y. (2004). Aligning Security and Usability. Retrieved 26 January 2017, from https://www.computer.org/csdl/mags/sp/2004/05/j5048-abs.html

Kahneman, D. (2012). *Thinking Fast and Slow*. Penguin Books.

Kahneman, D., & Tversky, A. (1972). Subjective probability: A judgment of representativeness. *Cognitive Psychology*, *3*(3), 430–454. https://doi.org/10.1016/0010-0285(72)90016-3

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–291.

Kaplan, B., & Duchon D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS quarterly*, 571-586.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J., & Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk Analysis*, *8*(2), 177–187.

Kirlappos, I., Beautement, A., & Sasse, M. A. (2013). 'Comply or Die' Is Dead: Long Live Security-Aware Principal Agents. In A. A. Adams, M. Brenner, & M. Smith (Eds.), *Financial Cryptography and Data Security* (pp. 70–82). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-41320-9_5

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from 'Shadow Security:' Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. Internet Society. https://doi.org/10.14722/usec.2014.23007

Kirlappos, I., & Sasse, M. A. (2014). What Usable Security Really Means: Trusting and Engaging Users. In T. Tryfonas & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 69–78). Springer International Publishing. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-07620-1_7

Knowles, W., Prince, D., & Hutchison, D. (2012). Perceptual Influences on Risk Assessments and the Challenges for Information Security and Network Management. Retrieved from http://www.cms.livjm.ac.uk/pgnet2012/Proceedings/Papers/1569607803.pdf

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

Landis, R.J., & Koch, G. G. (Mar. 1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159-174.

Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology*, *32*(2), 311–328.

Lincoln, Y. S., & Guba, E. G. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New Directions for Program Evaluation*, *1986*(30), 73–84. https://doi.org/10.1002/ev.1427

Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, *127*(2), 267.

Luft, J., & Ingham, H. (1955). The Johari Window: A graphic model for interpersonal relation. *Los Angeles*.

Luhmann, N. (1990). Technology, environment and social risk: a systems perspective. *Organization & Environment*, *4*(3), 223–231. https://doi.org/10.1177/108602669000400305

Massie, M. J., & Morris, A. T. (2011). Risk Acceptance Personality Paradigm: How We View What We Don’t Know We Don’t Know. Retrieved from http://arc.aiaa.org/doi/pdf/10.2514/6.2011-1455

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, *31*(5), 622–660.

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. *Journal of Vocational Behavior*, *61*(1), 20–52.

Nickerson, R. S. (1998). Confirmation bias: a ubiquitous phenomenon in many guises. *Review of General Psychology*, *2*(2), 175.

Nyshadham, E. A., & Minton, R. F. (2013). Affect and Risk in IS Research. https://doi.org/10.2139/ssrn.2225446

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673–680.

Pallas, F. (2009). *Information Security Inside Organizations - A Positive Model and Some Normative Arguments Based on New Institutional Economics* (SSRN Scholarly Paper No. ID 1471801). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=1471801

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, *11*(4). https://doi.org/10.1515/jhsem-2014-0035

PwC. (2015). 2015 Information security breaches survey. Retrieved 16 July 2015, from http://www.pwc.co.uk/audit-assurance/publications/2015-information-security-breaches-survey.jhtml

Reason, J. (2000). Human error: models and management. *Western Journal of Medicine*, *172*(6), 393.

Renn, O., & Benighaus, C. (2013). Perception of technological risk: Insights from research and lessons for risk communication and management. *Journal of Risk Research*, *16*(3–4), 293.

Rhee, H.-S., Ryu, Y., & Kim, C.-T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. Retrieved from http://aisel.aisnet.org/icis2005/32/

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221–232. https://doi.org/10.1016/j.cose.2011.12.001

Rottenstreich, Y., & Hsee, C. K. (2001). Money, kisses, and electric shocks: On the affective psychology of risk. *Psychological Science*, *12*(3), 185–190.

Rundmo, T., & Moen, B. (2006). Risk Perception and Demand for Risk Mitigation in Transport: A Comparison of Lay People, Politicians and Experts. *Journal of Risk Research*, *9*(6), 623–640. https://doi.org/10.1080/13669870600813811

Santos, J., & Boote, J. (2003). A theoretical exploration and model of consumer expectations, post‐purchase affective states and affective behaviour. *Journal of Consumer Behaviour*, *3*(2), 142-156.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? Retrieved from http://discovery.ucl.ac.uk/20345/

Savadori, L., Savio, S., Nicotra, E., Rumiati, R., Finucane, M., & Slovic, P. (2004). Expert and Public Perception of Risk from Biotechnology. *Risk Analysis*, *24*(5), 1289–1299. https://doi.org/10.1111/j.0272-4332.2004.00526.x

Schneier, B. (2004). *Secrets and Lies: Digital Security in a Networked World* (1st ed.). Wiley.

Schneier, B. (2008). The Psychology of Security. In S. Vaudenay (Ed.), *Progress in Cryptology – AFRICACRYPT 2008* (pp. 50–79). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-68164-9_5

Schroeder, N. J. (2005). *Using prospect theory to investigate decision-making bias within an information security context*. DTIC Document. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA445399

Seo, M.-G., Goldfarb, B., & Barrett, L. F. (2010). Affect and the framing effect within individuals over time: Risk taking in a dynamic investment simulation. *Academy of Management Journal*, *53*(2), 411–431.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). Retrieved from http://dl.acm.org/citation.cfm?id=1753383

Shepherd, L. A., Archibald, J., & Ferguson, R. I. (2013). Perception of Risky Security Behaviour by Users: Survey of Current Approaches. In L. Marinos & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 176–185). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39345-7_19

Sjoberg, L. (2000). Consequences matter,‘risk’is marginal. *Journal of Risk Research*, *3*(3), 287–295.

Sjöberg, L. (2002). The allegedly simple structure of experts’ risk perception: An urban legend in risk research. *Science, Technology & Human Values*, *27*(4), 443–459.

Sjöberg, L., & Engelberg, E. (2010). Risk perception and movies: a study of availability as a factor in risk perception. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *30*(1), 95–106. https://doi.org/10.1111/j.1539-6924.2009.01335.x

Slovic, P. (2004). What’s Fear Got to Do with It - It’s Affect We Need to Worry About. *Missouri Law Review*, *69*, 971.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis*, *24*(2), 311–322.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333–1352.

Slovic, P., Finucane, M., Peters, E., & MacGregor, D. G. (2002). Rational actors or rational fools: implications of the affect heuristic for behavioral economics. *The Journal of Socio-Economics*, *31*(4), 329–342. https://doi.org/10.1016/S1053-5357(02)00174-9

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why Study Risk Perception? *Risk Analysis*, *2*(2), 83–93. https://doi.org/10.1111/j.1539-6924.1982.tb01369.x

Slovic, P., & Peters, E. (2006). Risk Perception and Affect. *Current Directions in Psychological Science*, *15*(6), 322–325. https://doi.org/10.1111/j.1467-8721.2006.00461.x

Slovic, P., Peters, E., Finucane, M. L., & MacGregor, D. G. (2005). Affect, risk, and decision making. *Health Psychology*, *24*(4, Suppl), S35–S40. https://doi.org/10.1037/0278-6133.24.4.S35

Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & Security*, *29*(6), 659–679. https://doi.org/10.1016/j.cose.2010.02.002

Song, H., & Schwarz, N. (2009). If It's Difficult to Pronounce, It Must Be Risky Fluency, Familiarity, and Risk Perception. *Psychological*

Science, *20*(2), 135–138. https://doi.org/10.1111/j.1467-9280.2009.02267.x

Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, *23*(5), 645–665.

Takemura, T. (2011). Empirical Analysis of Behavior on Information Security (pp. 358–363). IEEE. https://doi.org/10.1109/iThings/CPSCom.2011.8

Takemura, T., & Komatsu, A. (2013). An Empirical Study on Information Security Behaviors and Awareness. In *The Economics of Information Security and Privacy* (pp. 95–114). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39498-0_5

Taleb, N. N. (2007). *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets* (Re-issue). Penguin.

Taleb, N. N. (2010). *The black swan: The impact of the highly improbable*. Random House Trade Paperbacks.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244. https://doi.org/10.1080/01449290903121386

Tinsley, H. E., & Weiss, D. J. (Eds.). (2000). Interrater reliability and agreement. *Handbook of applied multivariate statistics and mathematical modeling*, 95-124 Academic Press.

Trope, Y., & Liberman, N. (2003). Temporal construal. *Psychological Review*, *110*(3), 403.

Trope, Y., & Liberman, N. (2010). Construal-Level Theory of Psychological Distance. *Psychological Review April 2010*, *117*(2), 440–463.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, *5*(2), 207–232.

Tversky, A., & Kahneman, D. (1981). The framing of decisions. *Science*, *211*, 453–458.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297–323.

Van der Pligt, J., Zeelenberg, M., van Dijk, W. W., de Vries, N. K., & Richard, R.. (1998). Affect, attitudes and decisions: Let's be more specific. *European review of social psychology*, *8*(1), 33-66.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging The Qualitative-Quantitative Divide:Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly*, *37*(1).

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, *10*(1), 69–80.

Wang, P. A., & Nyshadham, E. (2011). Knowledge of online security risks and consumer decision making: an experimental study. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1–10). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5718703

Wason, P. C., & Shapiro, D. (1971). Natural and contrived experience in a reasoning problem. *Quarterly Journal of Experimental Psychology*, *23*(1), 63–71. https://doi.org/10.1080/00335557143000068

Weinstein, N. D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of Behavioral Medicine*, *10*(5), 481–500. https://doi.org/10.1007/BF00846146

Weinstein, N. D. (1989). Optimistic Biases about Personal Risks. *Science*, *246*(4935), 1232–1233. https://doi.org/10.2307/1704599

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137–143). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=508195

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40.

Yin, R. (2003). *Case Study Research: Design and Methods, 3rd Edition (Applied Social Research Methods, Vol. 5)*. SAGE Publications, Inc. Retrieved from http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&path=ASIN/0761925538

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332.

APPENDIX 1: CASE STUDY 2 (ORGANISATION C) QUALITATIVE SUMMARY OF THEMES

The following section summarises the key themes from each of the participants interviewed, highlighting some of the contextual factors influencing affective and cognitive responses to security as well as understanding of security risks.

1. Participant 1 - OPEN

AS & RU

The employee suggested that fictional colleagues are generally positive in their attitude towards security; hence the *AS* Score of 20. For instance, they emphasise that "*fictional colleagues"* recognise the *purpose* of security:

" Overall people understand security is not just there to get in the way"

The participant notes that "*fictional colleagues"* link security with protection stating that they are aware of the impact of the disclosure of information on their colleagues. They also refer to feeling 'proud' that they helped others through their security prudence:

"Lot of people feel 'I've done my bit today', helping lads…It's there to protect, colleagues have empathy for those they protect, pride in assisting…"

This employee suggests that "*fictional colleagues"* demonstrate positive risk awareness and understanding within Organisation C, stating that "*everyone is aware of the risks*". They indicate that "*fictional colleagues"* recognise the technological safeguards that reduce risk, for instance they state that staff felt "*pretty secure*" in relation to devices such as laptops for instance, which are encrypted with two-factor authentication.

Passwords

Some of the key themes that emerged from this interview included reference to problems with memorising passwords. In response to how people manage passwords, the participant suggested: "*you're not supposed to write them down, but you have to*", highlighting that in this instance, security policy is not realistically aligned with individual capability; echoing the "*can't comply*" theme in the literature. However, not sharing passwords emerged as an ingrained part of the culture where the employee suggested: "*People know: never share passwords and you're not meant to have shared mailboxes*".

Data Management: Changing Climate

Another theme that emerged was how people dealt with sensitive information within the organisation. The participant noted that "*in the past colleagues have managed it badly" citing* examples of:

> *"poor record keeping, poor management of that information, not filing them properly, printing off copies leaving them in cupboards, the worst one is printing off classified information and not registering with everyone, meant to log everything you produce…"*

This mode of behaviour, where employees are not diligent in management of data, reflects individuals with low levels of *RU* regarding management of sensitive data. However, the employee referred to gradual improvements since the policy is now being enforced: "*you have to book things in now, people* *aren't printing things off, feeling that some people didn't take it seriously in the past*".

Culture of positive security habits

Certainly, from the perspective of this individual, there appeared to be a culture of compliance at Organisation C, where ingrained *habits* influenced security behaviour and inculcated a *Positive AS* attitude:

"People follow the rules everyday you have to log into your machine…Lock the computer pretty much everybody does that on a regular basis. Everybody locks screen – 10 years, maturity, it's ingrained. Quite security conscious overall".

Context – Government and Security

Additionally, the employee referred to the cultural "*pride in assisting"* that their colleagues had in relation to their main job role in the context of a government department. Awareness of the importance of security compliance in this context The employee suggested *fictional* colleagues were "*aware of the impact of information being released [had on] national security*", suggesting that employees understood the security risks by referring to the connection between adhering to security policy and the consequences of data loss.

Senior Management

Whilst this could indicate the perception of a '*culture of compliance'*, this employee saw senior management as a driver for non-compliance. For instance, the employee suggested that although fictional colleagues would be disciplined if they did not follow the rules and regulations, this did not apply across of levels of the organisations: "*ultimate consequences, you will be disciplined there are rules and regulations…*".

The employee suggested s/he had the impression from colleagues that there was a theme of "*'do as I say, not as I do' from the top*" and that there was "*not a top-down example*" which was the main issue. This quotation suggests that there is a relationship between positive security habits and the impact the example of senior staff may have on employee security behaviour:

"…if top-down is serious and conscientious about it people will improve– if people at top are lax and lazy you're not going to be [security conscious] – it doesn't help reinforce positive security habits…".

Physical Security – Security Culture

This appeared to be an area of security strength, where the employee identified that security was "*crucial in the way we operate*" and linked physical security to emphasising the security culture. P1 also noted that visitors to the organisation were subject to various checks and restrictions:

"…[People] can't just walk in, need a pin [to] get in, even a guest needs to be approved…areas of the building [people] are not allowed in…".

2. Participant 2 - Open

AS & RU

The *AS* score for both coders is in the positive zone, generally representing fictional colleagues as being security-oriented. For instance, P2 refers to Organisation C as being "*security conscious*" and "*tight on security*" with security behaviours that are indicative of this:

"…if people leave their desks, lock our screens… shut down terminal clear desk even for lunch, lock cabinets, cabinets lock during the day as well…".

Similarly, they refer to "*fictional colleagues*" being aware of security rules and following them:

"Most people follow the policy rules – if a document goes through, from the outset they are totally engaged with the contact, people are aware…".

Some of the comments, whilst demonstrating a positive stance towards security, expressed more negative emotions too. For example, the employee referred to there being "*complacency*" in "*fictional colleagues*"' attitude towards security. This did not indicate that fictional colleagues were negative in their stance towards security but that the employee might be downplaying familiar risks, and vigilance might be needed.

This employee's score for *RU* was in the positive aspect of the dimension. The participant reported that in general, there was a high level of risk awareness demonstrated by fictional colleagues within Organisation C, stating: "*People are aware of the risks, visibly seen a marked improvement.."* indicating that not only do "*fictional colleagues"* understand the security risks but also have improved in relation to their awareness of risks, suggesting a shift in the security posture within the organization.

Physical Security: Complacency (rather than habit)

As previously mentioned, P2 suggested that the attitude from "*fictional colleagues"* towards security within Organisation C reflected complacency, and they explicitly linked this to physical security. For instance, the participant suggested that although security is a "*visible community at the door*" and there is "*security personnel as you come in the building*" nevertheless, "*there is a* *complacency*". They highlighted that scanners had not been used for a long time, and that large numbers of people were coming in to the building.

Security Culture and Policy

The employee referred to Organisation C culture as "*security conscious*", stating that there was an acceptance that security was "*ingrained in the culture*". Examples of good security practice include "*shut down terminals… clear desks even for lunch, lock cabinets cabinets, lock during the day as well*".

Linked to the culture is understanding of the policy and this participant suggests that there is a high knowledge of security policy. This exemplar relates to how *fictional colleagues* manage data:

"Security policy – high knowledge of security, then handling and your relation to it, if you're not the originator of the document from A to B to C…".

Password Sharing

The participant suggested that password sharing was a "*closed shop thing*" in that it was not an ordinary occurrence but something that happened within the organisation in extreme circumstances when it was necessary to access an account:

"…if you had to access a principal's account, being given permission to do that, depends on the situation, rare… something that is so extreme, something is locked in there, something has happened need to try and get something. This is a crisis what do we do [in] extremis…".

Nevertheless, the participant emphasises that "*fictional*" staff are aware of standard security procedures for passwords including the non-sharing of passwords, indicating that are mindful of potential risks.

"When it comes to passwords, security procedures in place for that – standard…Everyone is aware…People don't share passwords – they are aware. They should know them…".

Security Training

This seems to be an area for development for Organisation C, with employee suggesting that the security training provision is a "*bit of a gap*". They highlight that whilst security training is available to "*fictional colleagues"* it can be difficult to access since the internal course is not available online. In addition, the course doesn't have a central point of contact, so it is incumbent upon the member of staff to find out who is running the courses.

"There is a security course out there but it's a course that's internal, not online even though the policy is there to do basic security training – doesn't give you a point of contact, [you] must find out who is running the courses…".

The employee notes that, - confusingly for staff at Organisation C - there is a link for online security training - which does not lead anywhere.

3. Participant 3 - OPEN

AS & RU

P3 demonstrated *Positive AS*. P3 highlights that:

"…everything is security conscious. Nobody goes out their way to have a security breach, [there is a] culture of security…".

P3 suggests that as well as there being a culture of security most "*fictional colleagues"* are "*risk aware*" and this theme is resonant throughout the interview. Specifically, P3 suggests, in relation to their "*fictional colleagues"* that: "*Most have a very good level of Risk Understanding – if not sure, most people will ask – can I do this, can I do that?*" Further, they provide an example of how "*fictional employees*" make instinctive assessments when they are classifying documents:

> *"Most people are risk aware - you used to do a risk analysis, when you produce a document you put a classification on it – gut feel on what is the classification…"*

The other key theme within this interview, is the implicit link between risk and consequences. For instance, the participant noted that "*fictional colleagues"* were aware that leaking information had consequences and therefore tended to adhere to security guidelines:

> *"You won't pass information – people will share information [on a] need to know principle, [it is] people's lives. In the main this is adhered to…consequences, individual based consequence management…".*

Security Culture and Policy

The employee indicates that colleagues are likely to be security-conscious as "*everything is security conscious,*" due to the processes within the organisation. For instance, P3 suggest that "*nobody goes out of their way to have a security breach*" and that there exists a "*culture of security*" within the organisation. They also note that "*fictional colleagues"* are likely to be compliant 99% of the time and that the risk of failing to comply is a "*career limitation*".

Adherence to policy and consequences of non-compliance are referred to within this transcript. For instance, the employee notes that people are familiar with the security policy and also recognize the consequences if the policy is not followed:

"Security policy – people are familiar, familiar with the principles of the document [they] use it day in and day out…Consequences if policy is not followed – you can end up with people…exploited, embarrassment of [senior fictional colleagues], leave a cabinet unlocked you get a ticket it has a personal consequence on you…".

Teams

The participant also noted that there was a culture of security within the organisation in relation to team working and reciprocity in relation to security actions. For instance, they referred to how people check each others' drawers within the team to ensure they are locked:

"…you lock your drawer and you lock your cabinet, you check others' drawer within the team, he will check mine…".

Training

The participant referred to "*fictional colleagues"* engaging in various training courses such as cyber awareness courses, police talks on personal security and social media advice. They also refer to an information protecting information course which is computer based and designed to be completed annually. However, P3 states that some fictional colleagues perceive the security training course as "*noddy*" and "*time consuming*".

Laptops

The employee notes that "*fictional colleagues"* are aware of the security risks associated with the laptop encryption devices; i.e. they realise that they shouldn't carry the encryption device with the key. They also suggested that laptops occasionally are stolen, but that "*fictional colleagues"* report the loss. Further, that in relation to blackberries they need to make sure it is secure and remember not to leave it.

Passwords

This appeared to be an area of *friction* for Organisation C. The employee describes how fictional colleagues have to go through a '*tortuous*' process to reset their password, wasting productive work-time:

> *"...Reset – process tortuous to reset. Length of time, you can't get in to your system you have to go through a single point of contact, use that password to access the system, a very secure system…2 hours – can't access the system it can impact on your work...".*

The *negative* affect expressed in relation to this process may contribute to a sense that security is not always usable, which may lead to circumventions particularly if the individual is under time pressure at work.

In terms of security awareness around storing passwords however, P3 notes that fictional staff do write them down but "*store them securely*", suggesting they are aware of potential security risks. They also note that colleagues are aware that if they left passwords out on their desks in notebooks for instance, security would be likely to "*flag it up*" and enforce policy.

4. Participant 4 - Hidden

AS & RU

This participant's *AS* score is in the negative numbers, suggesting that they perceived that "*fictional colleagues"* were not wholly positive about the security provision or processes within the organisation. Coder 2 however, scored the *Affective Security* dimension within the positive zone for this interview which may be attributed, in part, to me coding the transcript much more densely (I used 44 codes in total for the transcript compared to Coder 2's 30. (For further discussion of code differences between coders, see *Chapter 9.5.1 Limitations*).

"Yes there is a clear desk policy. On the whole, people will put away their work, and lock it away in their cupboards, you wouldn't have books, protectively marked documents could be left under or in…".

The general level of perceived *RU* for "*fictional colleagues"* was reasonably high with the employee suggesting that most people had a "*pretty good idea"* in relation to security risks surrounding emails and hardcopy processes. However, they did suggest that there were some discrepancies in relation to when it was permissible to have their mobile phone switched on within Organisation C.

Security Culture

The participant referred to security as being something that is on "*fictional colleagues'"* minds in the work environment and to illustrate, gave an example of how there are "*codes for cupboards*" so irrespective of whether people are aware of it, security is present in their day-to-day physical environment.

Nevertheless, in relation to compliance however, the employee suggests that "*fictional colleagues"* engage in workarounds more frequently of late:

"annual security awareness training may [or] not may not be happening, people more blasé lately, if there are processes people will use those workarounds…".

Of interest here, is the fact the employee links security training with the increase in "*blasé*" attitude towards security.

Resource shortages: Culture and security policy

A key theme that emerged from this interview was the impact a shortage of resources has had on security awareness and emotional responses to security. The participant talked about a culture change in relation to data management processes within the organisation, which highlighted the move from hard copy to digital copy and also coincided with a reduction in staff numbers. The implication of this was that there was not enough support staff to support the changing processes, which made work "*difficult*". The participant also mentions that it was also more difficult to track who had completed security training.

"Gradually [it] happened – change in culture over last 10 years. Increasingly… we've reduced number of support staff – 4/5years. Support staff very few not normally centered in the business, don't get involved in the business with day to day work. The implication of that – nothing really to fill the void – don't think individual member of staff [were] as savvy…A bit difficult… not sure how often people do security training".

Further, the participant notes that although "*fictional colleagues"* were required to attend an annual security briefing for instance, they were unsure whether there was a central record to manage this.

This theme of limited resources also extends to the impact on the awareness and understanding of employee policy. The employee suggests that "*fictional colleagues"* may struggle absorbing the policy document since it is long and previously were used to relying on others who would be more familiar with the document. With the reduction in staff focused on communicating security information to employees, there is a potential negative impact on employee security behaviour:

“Security policy – it’s such a long document, how am I supposed to understand it? In days gone by who would be familiar with the security document, but with reduction in staff, more on intranet, more impetus, fictional colleagues less inclined. A few bronze security officers – fewer staff than previously…”.

There are further exemplars of the theme of limited resources and the impact on security compliance. The employee highlights in this instance that the main reason for non-compliance is not that people are unaware of the policy, but that they do not have the necessary technical tools to work both remotely and security.

“There is a broad understanding of what the policy is…[if you] send something to yourself at home, [you] take off the classification, not because of ignorance of policy - not having the necessary tools, readily available to meet the business need [such as] working on documents at home….”.

In this example, compliance becomes a trade-off between the primary task and security, demonstrating understanding of security risks is not enough in and of itself to ensure compliance.

Physical security

In relation to the physical environment and security, the employee refers to open plan working and indicating that it is not wholly secure:

“Open plan working – you hear a lot more about what’s going on, it probably it isn’t always the best idea – fosters a culture of openness and everyone knowing everything…”.

It might be suggested that in a way the organisation is engaging in a kind of security ‘*double-think*’ where employees are expected to accept two mutually inconsistent positions as correct; that the organisation thinks security is important, yet not important enough to design the environment and processes to align with that goal. Employees are expected to comply with security policy since the organisation deems it to be important, yet the organisation does not provide an environment that facilitates that outcome. In other words, security hygiene which involves aligning enabling tasks with the job holders primary function (Pfleeger et al., 2014) is not in place.

Security compliance

The employee suggested that most "*fictional colleagues*" tend to follow security policy and that the malicious insider was not a common entity within Organisation C:

"On the whole, fictional colleagues follow [security policy] very often & for the majority of cases [i.e. circumvention] it's in order to get the job done… Malicious intent is not common…".

5. Participant 5 – Hidden

AS & RU

The *AS* result for P 5 was scored negatively by myself (-1) which differed from Coder 2, who scored this transcript a low positive (7). In terms of qualitative analysis however there were numerous examples of negative affect in relation to security since there was an overall theme of security as a '*blocker*' or a '*hindrance*'. For instance, P5 noted:

"*Security seen as a hindrance, frustrated, the log-ons, the passwords, other than that a begrudging tolerance of it unless they feel they need to ignore it to* *achieve their aims…".* Similarly, later in the interview, they describe the perception of security within Organisation C as something that inhibits operational business rather than enables it:

"…security is seen as a blocker, circumventer. Can be seen as getting in the way of progress. Recently security seen as a set of rules as a set of red tap – not enabling. Restriction & requirement…".

Consequently, the overall final *AS* score is negative since there are many examples within the text that illustrate how technical processes in the business are not aligned with security policy.

Overall, the score for *RU* is positive, across both coders. The level of *RU* varies within this interview transcript however. On the one hand, P5 indicates that there is a lack of risk awareness amongst "*fictional colleagues"* and also this is mirrored, to some extent, by the lack of organisational tracking of security risks:

" Fictional colleagues aren't aware of the risks – what the department does not do, departmental security officer doesn't have a risk register, although building one. Until that happens within security – [we can't] understand how people are grading their risks…".

On the other hand, there are many examples of *Positive RU* within the interview transcript. For instance, the employee talks about how "*fictional colleagues"* are aware of the security risks associated with storing authentication materials together.

"You shouldn't store the password & the security token & dongle separate. Colleagues are aware & adhere to that…".

Interestingly, the employee notes that "*fictional colleagues"* do understand the security risks but because the risks are virtual and not concrete, they may not always follow policy:

"Most people are aware of the risks but able to ignore it because it's easier to ignore – the threat on information security nebulous…"

This is relevant because the employee is describing how the information security risks are not concrete and therefore difficult to conceptualise.

Resources

Explaining, in part, the negative perception of security within Organisation C is the theme around limited resources. P5 notes that security is under-resourced which they suggest has a negative impact on how security is integrated into functional tasks:

"…security is dragging it back, preventing progress. The reasons for that the security sphere isn't as well resourced as it should be…".

This also extends to technical resources where "*fictional colleagues"* may be circumventing security because they are not always provided with appropriate devices, such as company blackberries for example:

"Circumventing – emailing stuff to themselves they can't get a blackberry using their smartphone…".

Security Culture

The employee describes the way fictional colleagues perceive security within Organisation C as something that is "*subliminal*" and "*just happens*" where people "*don't notice it*". The flipside of this is that they refer to the fact that "*fictional colleagues"* can ignore security, hence: "*Implications – a creepy* *complacency – with regard to security matters, almost an inconvenient truth people do tend to ignore it…*".

Training

A key theme that emerges here is that "*fictional colleagues"* are not provided with sufficient security training, the employee notes that although training is provided around "*safeguarding information*" they are not provided with much guidance in relation to other security matters. An Information Security CBT every 3 years is referred to but there is a suggestion that less than the majority of fictional colleagues may have completed this training.

Authentication - Secondary Tasks

One of the issues that the employee raises is how the system is "*antiquated*" and takes "*fictional colleagues"* at least 2 minutes to log on. They also suggest that security is "*perceived as a blocker*" and that fictional colleagues may therefore expedite security processes in order to get the job done:

"*Fictional colleagues – being able to use their own device, circumvent the security regulation – a matter of expediency. Someone desperate to get a paper written, email it to themselves this to the personal email…Expediency. No maliciousness in it – just trying to get their job done…".*

Compliance/Non-Compliance

The employee suggests that most fictional colleagues are aware of security policy and "*general dos and don'ts*". In terms of awareness of some of the detail, the employee indicated that "*fictional colleagues"* may less informed and may for instance need to check with their supervisor on issues such as the safety issues associated with holidaying in certain countries etc.

However, the employee that "*fictional colleagues"* are likely to engage in circumvention where security interferes with their primary task. In this particular example, "*fictional colleagues"* are described using their own devices where they are not provided by the organisation: *"Circumventing – emailing stuff to themselves they can't get a blackberry [so they are] using their smartphone"*.

Clear Desk Policy

Although the employee mentioned that "*fictional colleagues"* are reminded of the importance of the Clear Desk Policy, this was not an enforced policy and adherence was "*patchy*". Specifically, they state that cabinets which should be locked are left open by mistake, an additional risk since cleaners "*come to the floorplate*". Nevertheless, awareness of this risk emphasises the strengths around the *RU* dimension.

6. Participant 6 – Open

AS & RU

The overall score for *Affective Security* is positive. P6 indicated that whilst security can elicit frustration amongst "*fictional colleagues"* in general it was not perceived negatively: "*Had a couple of instances, you have that frustration – [security] a necessary evil but not a negative perception, [people] consciously think about security…*".

In a similar vein, the employee noted that the majority of staff accepted the need for security and were prepared to take responsibility for adhering to security policy for instance checking other members of staff were in possession of the appropriate clearance level:

"Most people's perception – security is accepted, always check have the certain clearances, taking that responsibility…"

This employee perceived "*fictional colleagues"* as being aware of the risks, linking the awareness to security awareness training which they believed occurred more than once a year, possibly six-monthly or quarterly. In addition, they consider that "*fictional colleagues"* understand security policy and people "*question things*" about security, suggesting it is 'front of mind' for most employees in Organisation C. Further, the employee also states that "*fictional colleagues"* are "*more conscious [of security] than they've ever been, need to know*" and also that "*most people's perception* [is] *that security is accepted and that they "always check they have the certain clearances, taking that responsibility*". On the other hand, P6 suggests that security is not often discussed within the organisation.

Clear desk policy and security practices

However, the employee highlighted an issue around Clear Desk Policy where people don't always follow the rules and sometimes "nest" at their desks, rather than maintaining a relatively clear desk:

"Clear Desk Policy – there should be, but people nest, fictional colleagues – it's not good, don't think it's enforced, so stuck - an area of improvement…"

Conversely, the employee noted that "*fictional colleagues"* were aware *"there is a risk leaving documents on the desk"* despite the fact that adherence to this policy could be improved. Similarly, they highlight that not everyone locks their screens - which was also a potential area of improvement. It appears, according to this participant, that there is enforcement of security policy with a *"3 breaches and you're out"* rule where the inquiry is escalated to the CIO. Presumably this is likely to be something that "*fictional colleagues"* are aware of.

Team work

However, P6 describes a culture of team work around security practices; for instance, fictional colleagues check each other's desks and make sure documents that are left on desks etc. are not classified. There is a practice where they are required to sign the sheet out for the last person, which involves checking cupboards are locked for example.

Passwords

This is also an area where fictional colleagues are likely to follow the rules since P6 identifies that "*fictional colleagues not likely to share passwords – a culture around not sharing passwords, not taking responsibility if there was a breach, etc. …*". Colleagues are however likely to write down their passwords but store them in a locked cabinet, although some will memorise them. Moreover, P6 indicates that there is a perception there are too many passwords, at least 6 to 7.

Laptops and IT System

The employee suggested it was "*bureaucratic*" in relation to the process surrounding obtaining a laptop. They suggested that moving between checking email and getting into the system caused friction with productivity:

"Reading an email – within a minute or minute and a half – then…10 minutes to get back into the system, it's not conducive…restricts your working"

In addition, they noted that laptops were heavy and whilst there were "*no real incidents with laptops*" there was a risk in leaving them on the tube.

7. Participant – Open

AS & RU

P7 scored positively across both coders, indicating a generally positive attitude towards security. The incumbent suggested that *"fictional colleagues"* perceive security as something that is top of mind with Organisation C:

"*Day to day it's part of the furniture it's not foremost in everyone's mind, whether you are working at official increasing levels of awareness…".*

Interestingly, the employee delineates between "*fictional colleagues'"* awareness of security in general, since it is embedded in compliance process and their awareness of the security risk itself, hence: [their] "*awareness embedded in those processes [ie] compliance"* however *"people's mental awareness of the risk [is] less embedded*". They also referred to the risk appetite within Organisation C which "*drops to zero*" if there is a leak in the press regarding breaches in security for instance, which suggests an awareness of the impact of organisational reputation.

Another theme related to *RU* that emerged was the idea that perception of security risk is linked to age; so for instance if an individual is used to being open with their personal details on social media, i.e. less concerned with privacy issues, this may be translated in terms of security behavior, which in turn may impact on risk appetite change:

"Generational thing – older people greater awareness of understanding of security non-compliance, a generation [that remembers the] IRA, cold war still in living memory, start from a more risk.[This]generation – put your whole life on facebook – so you think it follows through in terms of security behavior…Risk appetite changes, technical control means you can do things – acceptance…".

Data Management & Risk Understanding

The employee suggested "*fictional colleagues"* understood the implications of storing data on a personal computer for instance, however, they may not realise the risk in sending work information to a personal email: "*Fictional colleagues sending information to personal emails, sending official or official sensitive, some people will not realise, the risk verse the business benefit…*" Therefore there seemed to be some variation in terms of understanding of security risks.

Training

There is mandatory security training for fictional colleagues every 2 years, administered on the Organisation C intranet. It was noted that security messages were delivered to raise security awareness at the "*point of consumption*" as timely reminders.

Security Culture

The employee described "*fictional colleagues"* awareness of security of being "*part of the furniture*" on a day-to-day basis, in other words suggested that security was not "*foremost in everyone's mind*". There also seems to be a perception that the organisation's technical security controls are "*fit for* *purpose*" to meet the business need, which belies a positive attitude towards the security provision in the organisation. In addition, the participant notes that most fictional colleagues are compliant with security policy stating: "*Most people follow the policy rules…most people report non-compliance…*".

Clear Desks

According to this participant, this was an area of compliance. "*Fictional colleagues"* were described as following the policy and it was suggested that material of a "*sensitive nature*" tended to get locked away.

> *"Clear Desk Policy – most people follow [policy]– most stuff is locked away, lock up their cabinets, secure environment – depending on the physical security, not mandatory. In an open plan work environment such as this, most people will follow…".*

Passwords

Similar to Clear Desk Policy, "*fictional colleagues"* are not inclined to share passwords, however, it was suggested that higher status "*fictional colleagues"* may share passwords with their executive assistant due to their workload:

> *"Passwords sharing – not usually, on occasion higher echelons – more because they won't have the time or space, or administer an individual, executive assistant might have the access, security not compliant – wouldn't be unlikely…".*

In relation to *RU*, one emergent theme is that perceived risks maybe "*traded-off"* according to seniority as well as pragmatism. Regarding the storage of passwords, "*fictional colleagues"* are described as being likely to write down passwords, "*putting [them] in a secret place*". The interview also highlights that many "*fictional colleagues"* have at least 10 passwords which is perceived by some to be "*annoying*". The participant notes that identity access management may make day-to-day working simpler but not necessarily less secure and that there was an "*aspiration*" to simplify working practices.

8. Participant 8 - Open

AS & RU

Overall, this participant's *Affective Security* score is positive. The positive comments included reference to an idea of security being an *intuitive* thing, embedded in the culture:

"…security is the main thing, it becomes intuitive. Organisation C [is] security minded to begin with …"

There are other comments which echo this sentiment, for instance, the employee suggests that security is a "*cultural thing*" and most people follow security policy rules most of the time:

"Most people [follow policy] most of the time otherwise we'd be breach every half hour, breaches are rare…".

There are mixed sentiments within the transcript however, despite the *Affective Security* score being broadly positive, with the employee expressing some frustration about the security controls within Organisation C. One exemplar of this is where the participant suggested that there could be improvements such as being able to access search engines such as 'google' for work purposes, as they had to visit the library to access external websites.

In terms of *Risk Understanding*, P8 highlights that *"fictional colleagues"* in general are aware of the 'need to know' nature of confidential material; "…*if you don't know you can't tell, dealing with sensitive material no need to* *know*". As mentioned in the section below (Security Culture vs Security Policy) the employee argues that "*fictional colleagues"* understand the security risk in relation to their environment, i.e. work and social contexts, consequently levels of risk perception are presented here as context-dependent:

"People are aware of security risks – you know what the implications of talking…outside the office, you only tend to go to places you know everyone around you, the only trouble time is the Christmas period & leaving drinks – don't drink in certain pubs, advised not to go into…".

Data Management

P8 highlighted that one of the potential areas to "*slip up*" on, in relation to risk management, is management of sensitive information. An exemplar of this is where "*fictional colleagues"* may be using an unclassified system for appropriate material but since there is often a "*fine line*" between unclassified and classified material, this can lead to security transgressions. This employee suggested it was a "*judgement call*" in classifying sensitive data between restricted classified and unclassified material, indicating awareness of potential security flaws, or risks.

Security culture vs security policy

This employee talked about fictional colleagues perceiving security as something that is "*instinctive*" or that becomes second nature:

"Security is the main thing, it becomes intuitive...physical security, information security – it becomes instinctive after a while…"

This security awareness is carried into the social domain which requires Organisation C employees to be aware of the risks of talking about organisational issues in a public, social environment. The employee suggests "*fictional colleagues*" are mindful of this in social contexts, indicating a reasonable level of *RU*: "*anyone outside the circle…Implications – if fictional characters are out, leaving drinks and talk shop – get them to stop doing it in a social environment*".

On the other hand, the employee identifies "*fictional colleagues*" 'talking shop' in the lift within the organization, suggesting low risk awareness:

"When people talk in a lift, they are talking to someone in a lift and they assume everyone is in the know. [It] occurs - more frequently than you'd like to believe – you only talk about work amongst work colleagues, especially in a lift…".

Another key theme that was raised by this particular employee was that whilst "*fictional colleagues*" are described as aware of security risks, they are not necessarily familiar with the *content* of the policy. This is interesting as it suggests that employees' risk perception is not necessarily dependent on knowledge of the policy but absorbed via the organisational culture at Organisation C:

"Security Policy – people know very little about the content, you know your job, you wouldn't expect them to talk to you about it as well, don't think you need to read study & digest. It's a cultural thing [being security conscious]".

Friction

The employee identified the IT system as source of friction to productivity for fictional colleagues, for as exemplified here:

"Laptops – they are totally unreliable. It's the IT, rubbish IT, synchronise between your work, take them outside and do some work at home and they crash, a running joke...They [fictional colleagues] come back into the office & moan…loss of time…".

Similarly, the employee noted that the organisational IT systems were:

"too slow, it crashes, frustratingly slow, you have 5000 terminals all try to get into a 3 inch pipe, still using copper".

Whilst these issues were not directly related to security, out-of-date systems can influence "*fictional colleagues"*" behaviour in circumventing policy to complete their primary task, which may open up security vulnerabilities".

Passwords

Another source of friction for "*fictional colleagues"* appeared to be the challenge of having to memorise passwords. This participant thought that writing down passwords, even if locked away in a cupboard, was not compliant with policy stating "*you [fictional colleagues] are supposed to remember them*". However, it seemed that people were reasonably aware of the security risks surrounding writing down passwords since they worked within a work area where only colleagues could access the passwords. Nevertheless, the employee outlined how the policy of memorising passwords was problematic for "*fictional colleagues"* since the employee noted that they may to change 10 of their passwords within a year, making them difficult to remember:

"That's why they write them down, you might have changed 10 passwords after a year. Wrong passwords in wrong system – 3 systems some have numerous systems, different layers – and all require passwords. If people said they could remember all passwords they were not being honest…".

Desk Policy

The employee commented that although there is a clear desk policy "*certain people do not adhere to it at all*" suggested there is a mixed response to compliance. Conversely, they also say that the security guards go through anything left out on the desk and fictional colleagues may lose their clearance if they "*get more than 1* [breach]". The employee points out that "*fictional colleagues*" do check before they leave that they have not left out any documents etc, indicating a reasonable level of *RU* around this topic:

"Double-check – people are aware of the risk, it's quite easy to leave a disc/document out – when you're in a rush, half-way through and the phone rings answer the call – human error you get distracted. Locking up – don't want routine interrupted – concentrate on what you're doing, one task at a time ... ".

9. Participant 10 – Open

AS & RU

This employee reports a positive *Affective Security* score across both coders suggesting that overall their view of "*fictional colleagues*" attitudes towards security within Organisation C is reasonably favourable. In terms of the qualitative themes, whilst the participant is broadly positive about security there are expressions of negative sentiment also. One example of this is the employee's comment that they were "*not sure if security fits into people's day*".

The employee suggests that "*fictional colleagues'*" perception of risk is partly shaped by their understanding of the security risk. For instance, they outline how fictional colleagues are unsure how to gauge the appropriate level of security risk and may "*push back*" if they are not given a reason for an aspect of security policy:

"People's perception – unsure whether risk is minimal or not – but people think we're over-egging, people haven't seen otherwise…problem is not given the background, people will push back if they can't see the reason for it" .

They also suggest that "*people are quite prudent*" in recognising the organisational security risks; one example of this is that fictional colleagues who home-work understand they need to separate the plug-in toggle to minimise risks.

Security Culture

There is a perception that security is "*done pretty well*" within Organisation C which is reflected in the lack of security breaches within organisation. Further, there is a sense that security is absorbed into the culture via "*osmosis*" which is unsurprising perhaps given the primary focus of the organisation is security: "*Most of day to day security knowledge on the job, from the manager/colleagues, by osmosis…*".

On the other hand, the employee notes that "*fictional colleagues"* may be unlikely to challenge individuals who do not have a pass or in the event the individual has a pass, may not check to see whether it is valid for that floor:

"Most fictional colleagues wouldn't challenge if you didn't have your pass, bit more wary [in] more secure areas. If you've got a pass round your neck, you won't be challenged…".

This employee also suggested that "*policy needs to be more pragmatic*" and indicated that, in their view, "*fictional colleagues"* require the flexibility to interpret the policy as their work requirements dictate:

"Improved – policy needs to be more pragmatic, guidance of saying be aware of limitations be pragmatic about trying to live to the word of the policy, interpret it yourself. You are as secure as the policy demands…".

Security Culture and Non-Compliance

However, "*fictional colleagues"* are described as transgressing policy by keeping their mobile phones on when mobile phones are not allowed on the floorplate.

"Mobile phone use on floorplate is prohibited, having in your pocket is prohibited, it must be off…most people don't take any notice, putting them on where they shouldn't…On a daily basis hear a phone going off…it is actually a line manager's responsibility, you can point out to people they shouldn't have their phone on, but there is a certain amount of hitting your head against a brick way, & reiterating what the policy [is] policy isn't consistent across the Department…".

This employee talked about "*fictional colleagues"* becoming "*blasé*" in relation to following security policy:

"When there a few docs leaked to the press, some of the docs were quite classified docs – when the police turn up at your desk it's real, locking down cabinets, you get blasé... without having that real experience – may be a bit blasé at times in some quarters…".

10. Participant 12 – Open

AS & RU

The *Affective Security* score for this interview was in the positive category for both coders. The employee also suggests that "*fictional colleagues"* are positive in their attitude towards security, taking the need for security and the associated risks within Organisation C seriously:

"Fine with security – sufficiently aware of threats, sufficiently aware of cyber threat and just how severe that is, that they take is seriously – doesn't have any adverse impact on them, work for government, ...appreciate [the] need to be secure…."

The employee acknowledges that whilst most "*fictional colleagues"* have a "*good level*" of security awareness, security may not be at the forefront of their mind, hence their comment:

"Doesn't think it enters their consciousness too much, aware of personal security, aware of security of others, security of documents and getting people out – good level of awareness…".

The *RU* score attributed to P12 is in the positive category. The employee gives various examples of "*fictional colleagues'" Risk Understanding*; for instance, the employee suggests that they have a "*reasonable risk awareness of social media*" which arose through "*clear instruction from [the] director*". This exemplar suggests that there is likely to be a clear link between specific security and understanding of security risks.

Security culture – Awareness and policy

P 12 talks about "*fictional colleagues"* having a good level of security awareness being "*aware of security, aware of [the] security of others, security of documents*…". They also noted that "*fictional colleagues"* are generally security aware but not necessarily conversant with the policy:

"Most of the time security policy isn't well known though, but most people are security aware anyway – carry most risk with recent grads, but they do the induction, formal organisation induction, mitigates that risk, waiting time on to the course etc…".

Indeed, P12 describes security policy as being something that isn't advertised well within the organisation. Moreover, P12 indicates that the organisational systems such as the induction process for new joiners and security awareness training which could support the dissemination of effective security messages are not effectively doing so. For instance, the induction process is described as "*immature*" in that they "*don't have one*" or if they do "*you have to wait a little time to get through it*". In addition, the employee notes that "*it's up to line manager to check staff have been through mandated courses [which is the] biggest area of risk".* Further, although the interview acknowledged that "*fictional colleagues"* do have access to an information security awareness course they "*are not aware anyone has done it*". Clearly the perceived lack of visibility of security policy and security awareness training from the employee's point of view may potentially have an impact on i) how "*fictional colleagues*" understand and recognise security risks and ii) how their affective attitude towards security.

On the other hand, describes how "*fictional colleagues"* deal with their passwords which suggests they do have some security awareness; for instance they are aware they should store passwords in a secure environment should they write them down:

> *"...Passwords…probably write down – can't remember, but pretty sure you shouldn't write it down or if you do keep it in a secure environment I think. Tend to write in a notebook, maybe put it onto their electronic device – but wouldn't be visible...".*

However, the lack of clarity around the specific behaviours that are compliant with policy indicates that there is a potential gap in translating policy into employee understanding of security actions within Organisation C.

11. Participant 13 – Open

In terms of the BSG, this participant falls slightly into the *Open* quadrant since their *AS* score is neutral but their *RU* rating is positive. (However, coder 2 rated the transcript as negative in relation to *Affective Security*, although also rated it positive for *RU* which would imply the *Hidden* quadrant).

Encapsulating the tension between positive risk awareness and neutral/negative affect towards security which are attributes of *Hidden* quadrant, the employee noted:

"Most people are aware of security risks in their work [they have] awareness but adhering to the regulations is another [matter]…".

This tension is reflected in the discourse around security with the themes which will be discussed below.

AS & RU

For this employee, the *Affective Security* score straddled the neutral and negative for myself and coder 2 respectively. This suggests that "*fictional colleagues"* are described, by this participant, as holding negative or neutral emotional attitudes towards security within Organisation C.

Both coders rated this participant's responses as positive in the *Risk Understanding* category. Coder 2 identified higher levels of *RU* that the first, however, as discussed, they were both above neutral levels of *RU* in the positive zone.

Security Culture

Participant 13 discusses how it is difficult to get "*fictional colleagues"* to engage with security processes, whether it be because it is hard to remember what to do or alternatively that they become "*blasé*" and less mindful of the risks:

"...individuals can be quite lax sometimes...quite difficult sometimes to get across to people how important it is, even locking up cabinets...become blasé...day to day routine, sometimes you forget..."

Security Training

This employee suggested that some "*fictional colleagues"* may see security training "*as a bind*" but also inferred that the course hadn't changed much over time and consequently perception of the course was that it was not imparting new information:

" *[the course is the] same thing, it's the same chap who ran the course, people tend to think 'I've done it'. IT security-wise [things] do change but the course is the same, but these systems don't change much...*"

In relation to improving the culture, P13 does advocate more security training:

"Perhaps there could be more security training – people wouldn't appreciate it. There is a culture of 'I do know, you don't need to tell me', more of a bind to have to do it. Perhaps it has to be done..."

P13 argues that "*fictional colleagues"* are aware of the policy but it maybe that distraction i.e. their primary task at hand (their job) or security protocol being commonplace may result in individuals becoming less vigilant:

"People do seem to know about the content (security policy) – either through distraction not bothering too – people just get a bit blasé [and] don't need to pay too much attention...".

In terms of embedding security training messages, P13 highlights that are posters and an intranet which focuses on IT security. Interestingly, the employee suggests that posters in particular are effective in dissemination security messages as they are "*put in front of people's faces*".

Security, Trust and Non-Compliance

P13 does refer to instances of non-compliance however; one exemplar of this is where they suggest that "*no one locks the screen, maybe 1 or 2* [people]". On the other hand, the employee mentions that the screen defaults to a locked status after 15 minutes and that the doors are not accessible. Interestingly, the employee notes that "*fictional colleagues"* may feel "untouchable" in respect of trusting others to the extent where they do not feel the need to lock their screens:

"Fictional colleagues feel they may be "untouchable". Everyone trusts each other – security wise amongst ourselves we trust each other enough to not lock the machines down, but we're taught to…".

This is interesting because trust, in this example, acts to reduce levels of security compliance because the associated security risk is considered to be non-threatening.

Primary task and work friction

P13 also refers to "*fictional colleagues"* engaging in short-cuts such as emailing work to personal email accounts so that they may work at home. They describe how this is consistent with security policy as long as the work is at official level and the motivation is derived from a desire to complete work, rather than circumvent process. In addition, it suggests that the existing systems are time-consuming if "*fictional colleagues"* find it quicker to email work to their personal email:

"May be likely to send work home to personal email – not got time to do it in the office, something I need to send home, believe it is consistent with security policy at official level – perception is it's fine – but could speak to [someone] to check this is ok – just for speed, & not wanting to find out you can't do it. Trying to get the job done…".

12. Participant 14 – Hidden/Open

AS & RU

There are differences between myself andcoder 2 around the direction of affective attitudes towards security where I rated *AS* as slightly negative and coder 2 found a *positive* direction of attachment. However, this does not necessarily imply that "*fictional colleagues*" hold a dismissive attitude towards security, rather the employee describes how fictional colleagues are circumventing policy in order to get their job done.

Examples of *Strong Negative Affective Security* include exemplars where :

"People will have a document held for years and refer to once a week [they have] circumvented [policy], so it is locked up so not booked out. Registered whether you have printed it, whether you actually register it in the logbook. To book all that out, [fictional colleagues] circumvent occasionally…".

In respect of *RU*, both coders reported positive levels of RU. As the employee suggested in relation to data management for example; "*people are aware of the risks of leaving documents*".

Security Policy

The employee notes that most people will adhere to security policy and "*circumvent them at their peril*". Furthermore, they note that "*fictional colleagues"* tend to comply with security policy and "*don't have to be* *reminded of the rules*".

Nevertheless, there is some inconsistency in this statement since P14 refers to "*fictional colleagues*" circumventing security policy if "*the rules encourage circumvention*" and when under time pressure for instance. The following specific example suggests that when "*fictional colleagues*" experience security tasks as too much "*hassle*" or difficult to comply with they are increasingly inclined to circumvent:

> *"Time-pressure…people didn't have the time to printed out, you need to have time 30 minutes – but then [the] rules [stipulate], in the right kind of bag, people just don't want to go through that hassle – rules which encourage circumvention – more people will send information on…".*

Interestingly, P14 suggests people more aware of consequences of leaving something on a train than "*sending on*" or emailing documents or information that they are supposed to print out for instance.

13. Participant 15 – Open

AS & RU

Both Affective Security scores are rated positively, suggesting that P15's perception of "*fictional colleagues*'" attitude towards security in Organisation C is largely positive. For instance, the employee draws attention to how "*fictional colleagues*" working at Organisation C think security is "*good*" but also that they feel "*a bit special*" because they are working within a governmental department.

That said, the employee did refer to "*fictional colleagues*" struggling with some security mechanisms leading to frustration:

"Sometimes security is frustrating though; change of government departments email addresses – some email gets rejected…security firewalls not helpful, not helpful. For a while on a different classification system couldn't send emails working at a higher level of classification…".

Risk Understanding scores across both coders are in the positive half of the *Risk Understanding* axis. There are examples throughout this interview where P15 refers to "*fictional colleagues'*" awareness of risk. For instance P15 highlights how sensitive briefings, security messages, notification when breaches occur and in particular, consequences of breaches in the media raise risk awareness:

"…[fictional colleague are] aware of security risks, warning and notices and suppose when there are breaches, you get stories in the media, leads to action taken understanding…".

Security Culture

P15 notes that Organisation C is "*highly security orientated*" citing examples of how security is explicitly present as you initially enter the building: "…*to just get in the building, [you] go through the airlocks, [have to] remember your pin number, secondary set of security – extra security – right from the beginning*" .

The employee also describes how "*fictional colleagues*" are required to go through various security processes to begin work such as unlocking cupboards, accessing the IT system which requires security authentications etc. This initial security setting may, arguably have an impact on the levels of security *Risk Understanding,* since P15 highlights the visible presence of security in the environment.

There is a reference to enforcement of policy in the form of punishment in relation to breaches; for instance, P15 discusses how breaches are used against a person's record and "*fictional colleagues'*" are also aware that senior people monitor breaches:

"People forgetting to lock a cupboard, leaving a document on the printer, there are unit security officers in each area, any kind of breaches, last man out sign out sheets, they have to go and look around. The guards come round to check round – the guards will issue a breach, it is monitored, [they] will use it against the person's record. Senior people are aware of who receive the breaches…".

However, P15 also acknowledges that "*fictional colleagues*" may be distracted by their primary task which causes the break. In these instances, they suggest there is "a bit of a nudge" but the individual is not formally disciplined:

"It is quite common for people to forget to lock a cupboard, caught by last man out – you did realise, bit of a nudge, no disciplinary. Rushing to get out...".

Security Policy - dissemination

P15 refers to "*fictional colleagues"* building awareness of security policy primarily via "*interaction with colleagues*" but also suggests that most of the key aspects of the policy are available via the intranet and via security briefings. The employee does refer to security policy training being available for "*fictional colleagues"* although the employee was unsure of specific details such as timings etc.

Nevertheless, P15 highlights that security is not always prioritised since there is a perception that people '*just know'* what the correct actions are in relation to security policy:

"Security isn't always a priority not talked about with their staff – assumed people are going to know…".

Passwords

There appears to be a lack however, in relation to whether writing down passwords is in line with security policy. P15 notes that passwords change 3 times a year, are randomly generated and therefore "*fictional colleagues"* record on a piece of paper and store the passwords in locked cupboards.

"How do people remember their passwords? – randomly generated, write down on an unidentifiable piece of paper & lock in their cupboards…Not sure if they [fictional colleagues] are aware of whether it's consistent with policy or not…".

14. Participant 16 – Hidden

AS & RU

The *AS* scores across both coders straddle the positive and negative zones with scores of -5 and 3 from myself and secondary coder respectively. The slight variation in scores may reflect different interpretations by the coders in classifying the emotive content in the summaries, however the 2nd score is a low positive. Taking the 2 scores together, there is a slight bias towards the negative part of the *Affective Security* dimension. This suggests that the individual would be likely to take a *slightly* negative view of security within Organisation C.

The scores are both in the positive part of the *Risk Understanding* dimension indicating that the employee perceives "*fictional colleagues'"* risk awareness to be competent. However, P16 raises the issues that a key challenge for Organisation C is the failure to educate "*fictional colleagues"* about security policy and "*understanding the threat*".

Security Culture

Overall, there is a theme that most people want to comply and follow the rules, but occasional breaches can be "*problematic*" in terms of impact. This highlights that P16 is generally positive about "*fictional colleagues'*" security behaviour but is also aware that occasional breaches can be costly to the organisation:

"Most people follow the rules most of the time. The problem is, the percentage of the people who don't at the wrong moment is very problematic…"

One of the themes that emerged from this employee is that there is a fundamental misalignment of security with the business (see section below) which impacts on how fictional colleagues perceive security at Organisation C:

"Stuck in world war 2. Security never seen as a business enabler... doesn't allow people to have confidence to deliver…".

These attitudes can negative impact on "*fictional colleagues'*" acceptance of security within Organisation C. P16 highlights that security is perceived to '*get in the way*' of "*fictional colleagues'*" primary tasks to some extent, in that security "*probably doesn't*" fit into people's day:

"*It doesn't fit in – a lot of the time the security people in the dark ages, processes and our policies aren't fit for the community…*".

Similarly, they also specifically state that security rules are not workable for the business which is likely to encourage circumvention of the policy despite having understanding of the security risks:

> *"You lay a new lawn – builders put a path across the side – but smart people see the trail across the lawn – we should be better at doing that for security, a lot of the time we put in security rules aren't workable for the business unit…".*

Data Management

From this observation, it is clear P16's perception is that security mechanisms and policy are not aligned with job roles. In many ways, these are the conditions for the *Hidden* quadrant to be populated, where employees understand the risk but may highlight frustration with unusable or effortful security mechanisms. One exemplar of this is the document booking out system, which is a key instance that emerged from other "*fictional colleagues"*, where the security process is considered onerous and effortful:

> *"Booking in of documents; every time you create one you have to book it in, sign it in and sign it out – so of course what happens – no one has done the document register form properly, [the] system [is] based on resources that we had, no staff to do it now. It just takes people too long, some people don't even know the system is there…underinvested to the point where we can't resource…".*

The specific themes that were highlighted in relation to problematic security/technical mechanisms include a lack of resources and underinvestment to implement and manage the process i.e. staff to register documents. In addition, P16 suggested "*fictional colleagues"* perceive the process as too effortful. This lack of *security hygiene,* where staff may feel they may bend/circumvent policy to get their job done, is likely to encourage "*fictional colleagues'"* security non-compliance despite knowledge of the security risks.

Passwords and the 'Delusional Compliance' Effect

P16 refers to the fact that some "*fictional colleagues*" carry their passwords written down on paper for their laptop and dongle together, which is not consistent with security policy. This exemplar however is used by the employee to illustrate how "*fictional colleagues*" delude themselves that "they aren't *not* complying" with policy:

"People carry round a bit of paper, people carry the passwords with the laptop, most of the time people carry dongle & password with the laptop. People delude themselves that they aren't not complying...Most people want to conform – department... quite conservative, like to conform[?], but then there's the business need. Human nature [needs] to convince self [it is] doing the right thing...".

The underlying reason for this appears to be difficult in remembering passwords, since the employee refers to the "*fictional colleagues*" preferring to "*conform*" or comply:

"...Each system has a different password, then within that you need another password to get on to the internet... It's not possible to remember them. Write them down, store them all over the place, hide in diary, regularly go round the building do covert search... Most people will lock them up in the cabinet, but some people won't...".

P16 also refers to instances where "*fictional colleagues*" may share passwords if they are time-pressured to get into the system in order to perform their primary task:

"People will share passwords, if their log in doesn't work, that's because they need to get in quickly – this isn't common, it does happen..."

Interestingly, P16 notes that Organisation C needs to improve hardware and authentication mechanisms: "*My computer fails or slows down one every couple of weeks – so get what you pay for. Need to get better at identity and access control...*" .

Evidently security non-compliance, despite *RU* being in the positive end of the dimension, will emerge if the context does not support efficient security mechanisms/processes that factor in the user's time and needs.

15. Participant 17 – Open

AS & RU

Both coders reported similar levels of *Positive AS*, indicating that the employee describes the organisation and "*fictional colleagues'*" attitudes towards security as broadly positive. This is linked to the security culture (see below) where the employee suggested that security it "*ingrained into behavior*" within Organisation C and that it is "*way we do things*". Consistent with the other employees in this cohort, the *RU* rating is located within the positive spectrum of the dimension.

Security Culture

There is a sense, from this employee, that security is embedded in Organisation C's culture. This is highlighted, not only by the *Positive RU* and *Affective Security* scores, but also, by the references to security being presented as something "in the culture": "*It's like [security] a vibration on a ship, in the culture…*". Similarly, the employee highlighted that management discussed security to their staff, generating a security culture amongst staff: "*Managers talk to staff about security. IT security awareness – it's mandated. It's so ingrained in the culture in the military community…*".

In terms of work-related behaviours that impact on security, P17 acknowledged that "*fictional colleagues*" do send work emails to their personal accounts but "*you can as long as it is official",* demonstrating awareness of the risks associated with different security classification levels.

Passwords

This seemed an area of challenge for "*fictional colleagues*"; P17 notes that there are various passwords for different systems which effectively mean fictional colleagues need to write passwords down:

"Fictional colleagues, put it [passwords] in an envelope, write passwords down put it in the safe…".

Although the employee noted that passwords are occasionally shared, they noted that it would only happen if someone was away, demonstrated awareness of the security risk around password sharing:

"Share passwords, don't want it [system] compromised, the only time you might do it if someone is away, then it will be here it is. Reset immediately, very unusual…".

Security Compliance

P17 suggests that non-compliance is unusual in Organisation C, noting that "*fictional colleagues"* will not break security rules to get a job done quicker: "*Compliance – follow the policy rules – conscious decision to set outside standard, people won't step outside procedures to get a job done quicker…*".

They also indicate that Organisation C is checked by security for breaches and therefore it is likely that if "*fictional colleagues"* transgress policy it will be detected, thereby acting as a deterrence:

"Security sweeps through the building – if non-compliance is leaving your safe (cabinet) open, to transgress not in open view – it will be detected subsequently in audit, if people haven't taken care of equipment…".

16. Participant 18 – Open

AS & RU

Both the coders rated P18's description of "*fictional colleagues'"* attitudes towards security as positive. Both the scores were positive, demonstrating a *Positive* level of security *Risk Understanding* and awareness.

Security Culture

P18 describes "*fictional colleagues"* as being aware of the security policy, although not necessarily following all security diktat to the letter:

"Familiar with the policy? People may not know where it is – they are congruent with the policy, understand why but not necessarily doing it by rote. Live the spirit and most of the letter…".

Generally "*fictional colleagues"* are considered to demonstrate security behaviours that are congruent with policy and specificially, P18 highlights that most senior colleagues have never been in breach throughout their career:

"*Most people are compliant with the policy – most senior colleagues has not been [in] breach [of policy] in [their] entire career, maybe only to have been breached once very early on – should they get breached – treated with the upmost serious[ness]…".*

Further, "*fictional colleagues*" are presented as adhering to clear-desk policy suggesting “*there is little material on people’s desks*”.

The overall tone of the employee’s description of “*fictional colleagues’”* attitude towards security suggests that security is embedded in the culture because it is central to the organisational purpose:

“Although because we talk about security so much it is deeply ingrained; civil procedure rules, how you can behave in providing the material how you can protect it and duties that you owe, transparent in terms of process – security impacts…”.

Security Mechanisms and Resources

They also note there is a burn bag for the disposal of hard copy material for employees, with different levels of shredders depending on the classification of the documentation. This suggests that Organisation C has made adequate provision for “*fictional colleagues*” disposal of documentation. On the other hand, reference is made to how “*fictional colleagues*” do not like working on Organisation C secure laptops remotely as connectivity is considered “*pretty patchy*” and some are not connected to the system. This may lead to circumvention with “*fictional colleagues”* defaulting to personal devices if the Organisation C resources are not sufficiently usable.

Passwords

In relation to passwords, the employee notes that “*fictional colleagues”* may write passwords down, but will do so in a way that is mandated by Organisation C:

“Fictional colleagues – tend to write down passwords in the course of this job, taken security, writing down in an envelope, store it appropriately in a locked cabinet…”

Conversely, the same employee also notes that "*fictional colleagues may write passwords in desk diaries…"* which may be considered to be a security risk depending on the security of desk diaries.

17. Participant 19 – Hidden

AS & RU

The *AS* scores are clustered around the neutral point, (-1 and 3). This suggests that P19 depicts "*fictional colleagues*" attitude towards security as demonstrating *Weak Negative* or *Weak Positive AS*. An example of *Weak AS* is reflected here:

"Rely quite heavily on email – people send different bits of information in own work accounts, when working on personal computer, you don't have access to the source material that enables you to do your job…"

The *RU* scores were rated as positive by both coders. However, coder 2 rated the *Risk Understanding* scores more highly (a score of 15 compared to 1). An exemplar of *RU* is as follows:

"The person developing the document knows what the classification is – one of the 1st things you learn is the understanding [of classification] if you're developing a piece of work – mindful if it's released to a 3rd party – what is the potential damage to the UK government?…".

Security culture

The employee suggests that security is something that is "*always there*" as a "*background issue*" for "*fictional colleagues"*, and they are aware of security in their day-to-day work. Nevertheless, they also point out that security policy is often perceived as yet something else they must know about which is cognitively effortful and inhibiting to business rather than a business enabler:

"Security policy, pretty sketchy – earlier point, security often seen, wrongly so, as another thing you need to know and…that gets in the way of you getting on with your day job…".

Security and flexible working

One of the key themes from this interview is the tension between security assurance and "*fictional colleagues*" desire to work more flexibly i.e. from home. The employee highlighted that increasingly more people were working from home but noted the security risks and that resources were an issue in facilitating this change:

"Remote working, increasingly starting to happen but it is rare. [Fictional colleagues are] concerned about information getting into the wrong hands, leaving things on trains – associated costs around secure laptops and things like that. Issue around recognising its importance, the barriers on day to day work…".

Restrictions around working from home, due to limited resources may potentially lead to circumvention of security policy. Resources is not the only issue in limiting flexible work - the employee referred to "*fictional colleagues*" being able to use home machines for work as long as it was for 'official' level material.

"Can't use a laptop at home, think you are allowed to use [a] home machine for official work, no concerns about leaking, but it's difficult to narrow down things that aren't sensitive but you might need additional information that might be more classified and sensitive…".

However, the challenge seemed to be that "*fictional colleagues*" are required to make a judgment about the sensitivity of the material they are working on and may potentially email additional material to their personal accounts to facilitate home working, which may introduce security risks:

"Rely quite heavily on email – people send different bits of information in own work accounts, when working on personal computer, you don't have access to the source material that enables you to do your job…".

Clearly some of the practical issues for "*fictional colleagues*" in remote working is that they may be constrained by IT systems in terms of what they are able to email to their accounts. With the requirement to finish tasks and preferring to work at home, may be inclined to use their personal email when the firewall blocks the document:

"…some fictional colleagues may send to personal email because of pressure of work, you can get on with stuff when you get home, means you're not slaving at your desk to not late on in the evening…".

Further, P19 notes that if "*fictional colleagues*" need to get home and finish their work, and may be constrained by IT systems blocking document, they may print out documentation to work on at home:

"Fictional colleagues would have a requirement to get home, concern about getting far behind...you couldn't send a higher classification because IT systems that you have prevent you to send it, couldn't send secret to Hotmail account there's a block on that. Print it out – may be a temptation, fictional colleagues may do that…".

This is relevant here because it demonstrates how "*fictional colleagues*" - who recognise the security risks but are under pressure to get the job done - may start to circumvent security protocols due to work pressures. The expedience or circumventions with policy appear to be motivated from a desire to 'be good workers' rather than rule-breakers. Being aware of the risks then may not act as a brake to modifying security behavioural choices; in this example it suggests that the need to fulfill the primary task in a timely fashion is the principal driver.

Security culture and non-compliance

P19 highlights mobile phone usage on certain floors as an example of security non-compliance driven by business need rather than rule-breaking tendencies or maliciousness. P19 explains that the use of mobiles is clearly in breach of security policy, but due to a business need where a "*fictional colleagues*" might have to obtain information via their smartphone or share information with a colleague, it is easier to use their own device:

"One of the frustrations – access to information – give you an example; work quite closely with a think tank…[where] websites are blocked, so the only way to get to it is using a smartphone. Often it's just conversation with team members, friends or family but sometimes a business requirement to find out information…".

Furthermore, P19 notes that these circumventions, when carried out to enable business and primary tasks, are not only tolerated but become absorbed into the culture:

"…part of this building where you can't have a mobile – clearly signposted [fictional colleagues have] got their phones on their desk. None of these people are breaking the rules because they have it in for [Organisation C] – might be work related, phoning back to explain what's going on, people share mobile phone numbers with team members often colleagues in the same organisation – unless it's stamped on early on, senior people do it – it becomes more widespread; the culture is don't worry about – becomes a norm of behavior…".

Passwords

The employee notes that "*fictional colleagues*" may have up to 3 passwords but do not tend to write them down in full sight, for instance on a post-it note, but dock away which the suggest is consistent with policy:

"Often by writing them down in a notebook, in a notebook that is carried that is generally locked away as part of clear desk policy. Don't write down you

passwords on a post-it note – big no-no – quickly gets enforced. Consistent with policy…”.

18. Participant 20 – Open

AS & RU

Both coders scored P20’s perception of “*fictional colleagues*” attitude towards security as largely positive.

In relation to *Risk Understanding*, both coders scored “*fictional colleagues’*” understanding of security risks as positive. P20 notes that risk awareness and understanding is a feature of the culture at Organisation C, which is turn is likely to influence understanding and recognition of security risks:

“Everyone has a responsibility to understand their security and understanding it – made aware…”.

Security Culture

P20 suggests that security is “*always*” on “*fictional colleagues*” minds because of the infrastructure of the organisation:

“…heavy presence of security by the time you walk in the building, to putting stuff away in the evening, clearing desk before you leave. Always on your mind, how you act and what you do from the moment you step into those booths. When you work for a place like this you can’t leave your desk as you left it. As soon as you walk through those doors,[it is a] different environment…”.

It also appears to be inherent in the culture according to this employee. For instance, P20 highlights that most “*fictional colleagues”* prefer to follow the rules and oftentimes when they do not, it is because they are not aware of it:

“Most people follow the rules. Everyone has a responsibility to train up new members, they just tell them they are not doing it right, if something is not right – you have to tell them – most people will say ‘oh I didn’t know that’…”.

Security Culture and Consequences of Breaches

One of the themes that emerged from this interview was the idea that breaching security rules could potentially have a strong penalty attached to it, such as prosecution:

"…you can be prosecuted – if you've done something wrong, for instance, a few years ago [a fictional colleague] left a document on a train, don't know why you would take that risk. I can only think you can't cope with your job and …haven't got time…".

The attributions the employee provided for why a "*fictional colleagues"* might break the rules include inability to cope with job and time-pressures, rather than a maliciously motivated desire to break the rules.

Physical Security

P20 notes that physical security is prevalent in the building. For instance, they refer to how (*fictional*) external visitors are booked in, collected at the door, even escorted to the toilets, highlighting the importance of security in managing visitors. In addition, P20 notes that "*you would be challenged on your pass*" if you were not wearing it, indicating that there is a culture of security where passes are checked for instance.

Physical Security and Confidential Data

P20 describes how physical security and confidential data are linked within Organisation C since certain areas were accessible had limited accessibility to "*fictional colleagues"*:

“Confidential data – depends what floor depends what area you work in…highly sensitive areas, no reason to see anything, nothing for you to have access to…”

In addition, the idea of “*fictional colleagues”* demonstrating *Risk Understanding* in relation to confidential data is also referred to by the employee:

“If you’re in those areas – you are aware of the risks associated with confidential data – made aware of how sensitive the information you’re dealing with is, you have to act accordingly, all of [the fictional] colleagues are very aware of what you [have to] deal with…”.

APPENDIX 2: INTERVIEW QUESTIONS (CASE STUDIES 1 & 2)

*This question set was used by my colleagues within the Productive Security at UCL for Company A and B security interviews. As previously described, I did not personally conduct the interviews nor design the question set for Case Study 1. In order to maintain consistency for the interviews I conducted for Case Studies 2, the same interview question set was used as the basis of the semi-structured interview format.

Interview Questions - Staff

Intro:

Thank you for reading and signing the information sheet and consent form.

Basically your data is anonymous – I won't be writing down your full name – and although the general pattern of the results will be used to inform this research project you won't be identified from the data.

I would like to spend the next 40 minutes or so asking you about the sorts of attitudes and behaviours you have observed towards security within your organisation. I won't be asking you to personally identify any one specific person or talk about your own security behaviours – instead I'm just looking to get an understanding of the sorts of behaviour and attitudes you may come across in your organisation. (Think of it as talking about "fictional colleagues").

Security Awareness

1. How do you think security fits in to most people's (your colleagues) day?
2. What security implications, if any, are associated with their work?
3. How much confidential or sensitive data do you think your "fictional colleagues" experience in their day-to-day role?
4. What risks do the people around you show awareness of in their work?

Sensitive Information

1. Do colleagues have to deal with personal student or staff information?
2. Do you think they have access to other sensitive information?
3. Have you ever known of anyone refusing to pass some information to someone in the organisation?
4. (If yes) What was the situation?
5. How often do you think colleagues send company information to their personal email for reading at home?

Policies, Reporting and Training

1. Is there a security policy within the organisation?
2. What do people seem to know about the content?
3. What security training, if any, have you and your colleagues received to date?
4. Have you ever received any security communication?
5. How effective do you think people think it is?
6. What do you think most people see as the pros and cons of following security policies?

Clear Desk Policy

1. As far as you are aware, how do most people interpret the policy in relation to what you should do with your desk when leaving in the evening?
2. Do colleagues have a secure drawer or storage area you can use?
3. How much of your work do people do on paper (if at all)?

4. How do you think colleagues perceive the risk regarding leaving documents on your desk?

Password Behaviour

1. How many different passwords do your colleagues need?
2. How often do they need to be changed?
3. How often do they need to reset their password?
4. How easy is it? How is the verification done?
5. How risky do you think most people think sharing passwords is with other people?

Laptops, Remote working and Removable Media

1. Do people ever use a laptop in the course of your work?
2. How do they share information with their colleagues?
3. What removable storage devices, such as USB sticks, do people use?
4. How often do most people work from home?
5. When working from home what systems or technologies are used?
6. If a laptop was stolen, how secure do you think most people would think the data would be on it?

Leadership and Management Roles

1. How much, if at all, do supervisors discuss security issues with their staff?
2. What is your perception of how prevalent this is across work groups?

Data Classification – Access control

1. Does the organisation have any data classification scheme?
2. How is the classification done? Who assigns those?
3. What is the difference between classification levels?
4. How likely are your colleagues to check eligibility before sharing information?
5. Do you think staff need to access some information that they're not allowed to access?

Compliance

1. How often do you think people generally follow the policy rules?
2. How likely are most people likely to report non-compliance?
3. How does the culture compare to health and safety and physical security?
4. What do you think most people see as the risk for failing to comply with security policy poses to the org?

General Information Security

1. What is the perception of how effective the current implementation is in keeping the organisation secure?
2. What do you think could be improved?
3. How exposed do you think the organisation is to unauthorised people entering the building?

Optional Topics

1. Personal/mobile devices
2. Locking screens
3. Compliance and security culture perception
4. Security Helpdesk
5. Physical security

Additional probes

- What do you think most people think are the pros and/or cons are of taking that approach?

- How does that approach fit with employees' work activities?

- How do you think others feel about that?

APPENDIX 3: INTERVIEW QUESTIONS (CASE STUDY 3)

*Interview questions for Case-Study 3, adapted from Case-Study 1 interview questions

Interview Questions - Staff

Intro:

Thank you for reading and signing the information sheet and consent form.

Basically your data is anonymous – I won't be writing down your full name – and although the general pattern of the results will be used to inform this research project you won't be identified from the data.

The interview is scheduled to last about 45 minutes and is in 2 parts. In the first part, I would like to ask you broad questions about the SIROs role and in the second part, the sorts of attitudes and behaviours you have observed towards security within your organisation. I won't be asking you to personally identify any one specific person or talk about your own security behaviours – instead I'm just looking to get an understanding of the sorts of behaviour and attitudes you may come across in your organisation. (Think of it as talking about "fictional colleagues").

SIRO Questions

1. What does the SIRO role involve on a daily basis?
2. How do SIROs obtain relevant information to form a risk judgement?
3. What sources of information are key to informing a risk judgement?
4. How adequate is the information SIROs receive in allowing them to make a risk judgement?
5. What would SIROs like to see more of/less of?
6. What do *fictional colleagues* perceive to be the main risks in their role?
7. What is their approach is to managing those perceived risks?
8. How do SIROs communicate information security risks to their team and the wider organisation?
9. What do they perceive as the biggest barriers to safeguarding organisational information security assets?
10. What would help SIROs to optimise performance in their roles?

Security Awareness

5. How do you think security fits in to most people's (your fictional colleagues) day?
6. What security implications, if any, are associated with their work?
7. How much confidential or sensitive data do you think your "fictional colleagues" experience in their day-to-day role?
8. What risks do the people around you show awareness of in their work?

Sensitive Information

6. Do fictional colleagues have to deal with personal student or staff information?
7. Do you think they have access to other sensitive information?
8. Have you ever known of anyone refusing to pass some information to someone in the organisation?
9. (If yes) What was the situation?

10. How often do you think fictional colleagues send company information to their personal email for reading at home?

Policies, Reporting and Training

7. Is there a security policy within the organisation?
8. What do people seem to know about the content?
9. What security training, if any, have you and your colleagues received to date?
10. Have you ever received any security communication?
11. How effective do you think people think it is?
12. What do you think most people see as the pros and cons of following security policies?

Clear Desk Policy

5. As far as you are aware, how do most people interpret the policy in relation to what you should do with your desk when leaving in the evening?
6. Do colleagues have a secure drawer or storage area you can use?
7. How much of your work do people do on paper (if at all)?
8. How do you think fictional colleagues perceive the risk regarding leaving documents on your desk?

Password Behaviour

6. How many different passwords do your fictional colleagues need?
7. How often do they need to be changed?
8. How often do they need to reset their password?
9. How easy is it? How is the verification done?
10. How risky do you think most people think sharing passwords is with other people?

Laptops, Remote working and Removable Media

7. Do people ever use a laptop in the course of your work?
8. How do they share information with their colleagues?
9. What removable storage devices, such as USB sticks, do people use?
10. How often do most people work from home?
11. When working from home what systems or technologies are used?
12. If a laptop was stolen, how secure do you think most people would think the data would be on it?

Leadership and Management Roles

How much, if at all, do supervisors discuss security issues with their staff?
What is your perception of how prevalent this is across work groups?

Data Classifcation

Does the organisation have any data classification scheme?
How is the classification done? Who assigns those?
What is the difference between classification levels?
How likely are your colleagues to check eligibility before sharing information?
Do you think staff need to access some information that they're not allowed to access?

Compliance

How often do you think people generally follow the policy rules?
How likely are most people likely to report non-compliance?
How does the culture compare to health and safety and physical security?
What do you think most people see as the risk for failing to comply with security policy poses to the org?

General Information Security

What is the perception of how effective the current implementation is in keeping the organisation secure?
What do you think could be improved?

How exposed do you think the organisation is to unauthorised people entering the building?

Optional Topics

Personal/mobile devices
Locking screens
Compliance and security culture perception
Security Helpdesk
Physical security

Additional probes

- What do you think most people think are the pros and/or cons are of taking that approach?

- How does that approach fit with employees' work activities?

- How do you think others feel about that?

APPENDIX 4: CODE LIST FOR COMPANY A & B (CASE STUDY 1)

Company A & B: June 2014

Access Control
access control - controlled by information owner
access control - leaver's access revoking problematic
access control - need business case
access control - problems accessing files on Sharepoint in the past
access control - same from any location
access control - sharepoint - anyone with access can grant access
access control - sharepoint easier than shared drive
access control - sharepoint harder than shared drives
access control - takes long to setup
Access Control:Admin Rights
Access Control:Administrative Process
Access Control:Administrative Rights
Access Control:Anonymised data
Access Control:Authorisation
Access Control:Blocked
Access Control:Clearance Process
Access Control:Data Streaming
Access Control:Departmental Shared Drive
Access Control:Does not have Admin Rights
Access Control:Downloading Software
Access Control:Fixed Screen Lock Timings
Access Control:Internet
Access Control:Job Specific
Access Control:Lesser Rights
Access Control:Local Admin Rights
Access Control:No Admin Rights
Access Control:Permission by invite
Access Control:Permissions
Access Control:Personal Data
Access Control:Problems
Access Control:Program Manager
Access Control:Project Managers
Access Control:Removal of Administrative Rights
Access Control:ResearchTtools
Access Control:Restrictions
Access Control:Restricts updates
Access Control:Review
Access Control:Revoked
Access Control:Rights
Access Control:Sensitive Data
Access Control:Sharepoint
Access Control:Technology
Access Control:Unauthorised access
Access Control:Validate
Access Control:Warning
Access Control:Website Blocked
Access Data:Stored Locally
Access Information:Software
Access to Data:Customer/Contractor
Access: Documentation
Access:Administration
Access:Automaticity
Access:Communcation

Access:Contractor
Access:Credentials
Access:Customer
Access:Customer Data App
Access:Data
Access:Defined by Protocol
Access:Does not require logging on
Access:Effort
Access:Files
Access:Helpdesk
Access:Information
Access:No Customers
Access:Permissions
Access:Personal Laptop
Access:Problems
Access:Reliable
Access:Responsibility
Access:Restricted
Access:Restriction
Access:Restrictions
Access:Service Desk
Access:Share Desktop
Access:Shared Drive
Access:Slow
Access:Systems
Access:VPN
Access:Website
Acquisition:Company
Affective Security:Low
Affective Security:Negative
Affective Security:Neutral
Affective Security:Positive
Affective Securtiy:Negative
Assigned Desk:Leeds
Assistance:Supervisors
Audit:Access Retrictions
Auditor:Consequences
Authenticate Phone:PIN
Authenticate:Time
Authentication
Authentication 2 Factor
Authentication Phone:PIN
Authentication:
Authentication:2 Factor
Authentication:Access Token
Authentication:Browser Preference
Authentication:Central Service
Authentication:Cognitive Effort
Authentication:Customers
Authentication:Employee Numbers
Authentication:Hassle
Authentication:ID
Authentication:Individual Log ins
Authentication:Locked Out
Authentication:Log in
Authentication:Log in IDs
Authentication:Log in passwords
Authentication:Log ins
Authentication:Log on
Authentication:Manager Approval

Authentication:Network card
Authentication:Not Shared
Authentication:Password
Authentication:Passwords
Authentication:Perceived Effort
Authentication:Pin
Authentication:Q & As
Authentication:Remember me
Authentication:RSA Key
Authentication:Security Questions
Authentication:Shared Systems
Authentication:Single Sign-on
Authentication:Token System
Authentication:Token, Password & User ID
Authentication:User Name & Password Not Required
Authentication:User Names
Authentication:Username & pin
Authentication:Username, Password & token
Authentication:Usernames & passwords
Authoriations:Mgr Sign Off
Authorisation
Authorisation:Access Calls
Authorisation:Approval
Authorisation:Attachments
Authorisation:Electrician, Contractor & Owner
Authorisation:Line Manager
Authorisation:Manager Sign Off
Authorisation:Process
Authorisation:Quick
Authorisation:Request
Authorisation:Restricted Access
Authorisation:System
Authorisation:System Not Functional
Authorisation:Team of People
Authorisation:Various People
awareness - breach consequences
awareness - confidentiality agreements for information protection
awareness - importance of information to the organisation
awareness - news about security breaches do not affect behaviour too much
awareness - no concerns about security
awareness - not sure about breach consequences
Awareness:Low
Background:Computing
Benefits:Low Financial Reward
Budgets
burden - relaxing security could boost productivity
burden - slowdown
Business:Less Technical
Business:Security
Business:Shared Drives
Call Retrieval:Application
Calls:Encrypted
Calls:Software
Can't Comply
Can't Comply:Converting file formats
Can't Comply:No locked drawer
CBT
CBT:2 years
CBT:Common Sense
CBT:Customer data

CBT:Customer data & Control of Documents
CBT:Fraud & Security
CBT:General Content
CBT:In-depth
CBT:Information
CBT:Information Retrieval
CBT:Infrequent
CBT:Multiple-Choice
CBT:Security Markings
CBT:Test
CBTs:Different Versions
Change:Not dictatorial
Changes:Business
Circumvention
circumvention - confidential documents sent home on email
circumvention - overshare in access control setup
circumvention - people are very clever trying to circumvent security
circumvention driver - connectivity problems
circumvention driver - impossible to remember all passwords
circumvention driver - lack of awareness
circumvention driver - misconception
circumvention driver - need for wide access
circumvention driver - problematic mechanisms
circumvention driver - productivity
circumvention driver - slowdown
circumvention driver - slowdown on getting access
circumvention driver - trust
Circumvention:Admin Rights
Circumvention:Change file
Circumvention:Email confidential documents home
Circumvention:Reduced
Classification:Confidentiality
Clean Desk Policy
Clean Desk Policy:Lack of awareness
clear desk - aware about the need for it
clear desk - downplays risk
clear desk - knows and follows clear desk
clear desk - no confidential information around
clear desk - no lockable space
clear desk - not aware
clear desk - not aware - still does it
clear desk - not followed
clear desk - people have a locker, nothing on desk
clear desk - violation - computers lying around
clear desk - violation - confidential information around
clear desk - would like to have lockable space
Clear Desk Policy
Clear Desk Policy:Enforced
Clear Desk Policy:No documentation
Clear Desk Policy:Screen and Keyboard
Clear Desk:No Sensitive Data
Clear Desk:Paperless
Clearance:Background checks
Clearance:Business Need
Clearance:Data Access
Code:Application
Code:Can't Install
Cognitive Effort:Password
Cognitive Effort:Password Rules
Cognitive Effort:Passwords

Cognitive Effort:Process
Cognitive Effort:System
Collaboration:Guidelines
Collaboration:Minimal Effort
Collaboration:Moderate
Collaboration:Other departments
Colleagues:Tenure
Colllaboration:Moderate
Communication
communication - adequate
communication - constantly receiving information about various subjects including security
communication - inconsistent
communication - infonet only communication of policy changes
communication - more information should be put out there
communication - needs to be role-based
communication - not done
communication - not everyone reads emails or the Infonet
communication - on par with safety
communication - policy communication through emails
communication - security lower than other factors
communication - team talks - no need to discuss about security
communication - team talks, manager discussions
Communication:Content
Communication:Information Security Policy
Communication:Security
Communication:Systems
Communication:Work related
Communications:Memorable
Company Network:Devices
Company System:Policies
Company Webset:Infonet
Company:Location
Company:Trust
Competitor:Information
Competitors:Turnover
Compliance
Compliance:Access Control
Compliance:Accountability
Compliance:Can't Comply
Compliance:CBTs
Compliance:Collusion
Compliance:Costs
Compliance:CostTooHigh
Compliance:Customer Data
Compliance:Documentation
Compliance:Does not share log-in ID
Compliance:Enforced
Compliance:Negative impact on productivity
Compliance:No power to enforce
Compliance:Passwords
Compliance:Policy Change
Compliance:Primary Task
Compliance:Reputation
Compliance:Unquestioning
Compliance:Without Security
computer - shared - Open built
Conference calls:Passwords
Confidenital Data:Support team access
Confidential data
Confidential Data

Confidential Data:Can't Verify Removal
Confidential Data:Compliance
Confidential Data:Customer
Confidential Data:DOB
Confidential Data:Email
Confidential Data:Encrypted
Confidential data:HR records
Confidential Data:Laptop
Confidential Data:Mother's Maiden Name
Confidential Data:NDA
Confidential Data:No access
Confidential Data:No access to Customer Data
Confidential data:Passwords
Confidential Data:Printer
Confidential Data:Protected
Confidential Data:Recorded Calls
Confidential data:Reports
Confidential Data:Risk Mitigated
Confidential data:Security
Confidential Data:Security Questions
Confidential Data:Sensitivity
Confidential Data:SharePoint
Confidential Data:Shredded
Confidential data:Stored securely
Confidential Discussion:Private
Confidential Documentation
Confidential Documentation:Removal
Confidential Information
Confidential Information:Customer
Confidential:Competitor
Confidentiality
Confidentiality Agreement
Confidentiality:Classifications
Confidentiality:NDA
Confidentiality:Non-disclosure
Confidentiality:Outsourcing
Confidentiality:Responsibility
Confidentiality:Sanctions
Confidentiality:Sensitive Data
Connectivity Problems:Sharepoint
Connectivity:Wi-Fi Network
Conscious Collusion
Consulting:Security Mindset
Contact:Coordinate
Contact:Questions
Contractor:Lack of knowledge
contractors - lower awareness
contractors - more likely to misbehave
contractors - no vetting
contractors - same access as others
contractors - vetting
Contractors:Construction
Contractors:Knowledge Seeking
Contractors:Lack of knowledge
Contractors:Phone contact
Contracts:Break
Contracts:External Companies
Contracts:Regimented breaks
Contracts:Services
Contracts:Union

Contractual Agreement:Logging in to same service
Coping Strategy:Reset Passsword
Corporate Communications:Emails
Cost Too High
Course: Content
Crime:Reporting System
Critical Infrastructure
Critical Infrastructure:Safety
Culture
culture - current approach leads to oversharing
culture - currently static
culture - improving
culture - is a mixture of secure and insecure behaviours
culture - low security consideration
culture - most people know role-specific stuff
culture - mostly compliant
culture - people care more about personal than company information
culture - people want to comply
culture - productivity driven
culture - sanction rather than education
culture - varies across locations
Culture Change:Sharepoint
Culture:Email
Culture:Low financial reward
Culture:Low Financial Reward
Culture:No laptops
Culture:Safety
Culture:Stability
Culture:Turnover
Customer Data:Commercially Sensitive
Customer Data:Record phone calls
Customers:Internal
Data
Data Analysis:Music Streaming
Data Management
Data Management:Leavers
Data Sharing
data sharing - confidential information shared via emails
data sharing - confidential information shared via internal systems
data sharing - documents send by post (on CD/paper)
data sharing - external systems
data sharing - missent information
data sharing - no confidential data on email
data sharing - password protection on important documents
data sharing - USB - mostly used for file transfers
Data Sharing:Email Confidential Data
Data Sharing:Email or Phone
Data Sharing:NDA
Data Sharing:Password
Data Sharing:Sensitive Information
Data Sharing:Sharepoint
Data Storage
data storage - confidential documents taken home on USBs
data storage - locally
data storage - network drive
data storage - no protection on individual files
data storage - no way to recover data if laptop lost/stolen
data storage - sensitive stored under restricted access
Data Storage:Copy
Data Storage:Insecure

Data Storage:Restricted Access
Data Storage:Secured Shared Space
Data Storage:Security Compliant
Data Storage:Shared Drive
Data Storage:Sharepoint
Data Streaming:Burden
Data:Accidental leak
Data:Business Case
Data:Competitors
Data:Confidential
Data:Customer
Data:Design items
Data:Disposal
Data:Documentation
Data:Encrypted Local Drive
Data:Insider
Data:Loss
Data:Not shredded
Data:Operational
Data:Password
Data:Patient Information
Data:Printing
Data:Project Information
Data:Risk
Data:Secure
Data:Secure Area
Data:Secure Sharing
Data:Sensitive Personal
Data:Shared
Data:Shredding
Data:Storage
Data:Viewed offshore
Decision-making:Effectiveness
Decision-making:Time
Decision-making:Top-down
Defence:Physical Security
Delivering:Fraud & Security
Department:Construction
Department:Customer Order Fulfillment
Department:Distribution Planning
Department:Engineering
Department:ENI Asset Policy
Department:Fraud & Security
Department:Integrity Engineering & System Integrity
Department:IT
Department:Mergers and Acquisitions
Department:Operations
Department:Procurements
Department:Project Management
Department:Sensitive Data
Department:Service Management
Department:Strategic Market Intelligence Group
Department:Trans
Department:Transmission Planning
department:transmission planning
Design Document:Project Plans
Design Project:Paperless
Design Projects:No Customer Data
Different roles:Different CBT requirements
Different System:Expiry

Different Systems:30
Different Systems:Different Passwords
Different SyStems:Passwords & Single Sign-on
Different Systems:Passwords & Single Sign-on
Digital
Discuss Security Issues
Diversity:International Staff
document handling - not-secure disposal
document handling - prints confidential information
document handling - secure disposal
Document:Data Classification
Documentation
Documentation Sharing:Electronically
Documentation:Binned
Documentation:Circulated
Documentation:Design
Documentation:Faxed
Documentation:Interested Parties
Documentation:Not confidential
Documentation:Paper-based
Documentation:Paperless
Documentation:Printing
Documentation:Project Design
Documentation:Read on-screen
Documentation:Relevance
Documentation:SharePoint
Documentation:Sharing
Documentation:Shredded
Documents:Advantages
Documents:Backed up on network
Documents:Confidential Waste
Documents:Format
Documents:Print
Documents:Printing
Documents:Share Drive
Documents:Store
Dongles
Drawers:No confidential data
Drive:Encrypted
Dynamic Licensing:User restriction
Education:Work
Email
email filtering - inconsistent
email filtering - protection for the organisation
Email Filtering:Blocked
Email:Customer Data
Email:Error
Email:Filtering
Email:Outlook
Emailing Documents
Emails
Emails:Accidental Recipient
Emails:Error
Emails:Smartphone
Emails:Spam
Emotional Consequences:Anger
Emotional Consequences:Animosity
Emotional Consequences:Apathy
Emotional Consequences:Difficult
Emotional Consequences:Frustrated & upset

Emotional Consequences:Frustrating
Emotional Consequences:Frustration
Emotional Consequences:Irritation
Emotional Consequences:Positivity
Emotional Consequences:Safety
Emotional Consequences:System 1
Emotional Reasoning
Emotional Reasoning:Laughs
Emotional:Health
Emotional:Upset
Employment:Temporary Jobs
Encrypted Calls:Restricted Access
Encrypted USBs
Encryption
Encryption:Bit Locker
Encryption:McAfee
Energy industry:Changes
Environmental
Error:Accidental
Error:Accidental Email
Evaluate Agent Performance:Access Calls
experience of security problems - but no checks were in place at that time
experience of security problems - had a number of high-profile thefts - led to requirement for encrypted USB adoption
experience of security problems - loss of shared access area at critical time
experience of security problems - oversharing can cause problems with pricing
Experience:2 years
Experience:BT
Experience:Computing
Experience:Different company
Experience:IT
Experience:IT Depart.
Experience:Retail
Experience:Staff
Experience:Telephony
Experience:Training
Expertise:Business Knowledge
Expertise:Knowledge
Expertise:Risk
Expertise:Technology
Expertise:Training
External facing:Communication
External Storage:Encrypted USBs
External Storage:USBs
File Sharing
File:Password Protected
File:Storage
Filing Systems:Access
Flexible Working:Home and Office Based
Flexible Working:More Effective
Flexible Working:Techology
Folders:Access
Fraud & Security
Fraud & Security:Best Practice
Fraud & Security:Consult
Fraud & Security:Customers
Fraud & Security:Review Policies
Fraud:Risk
Friction:Primary Task
Front Desk:Contractors

Geographic Area:New England North
Group
Group:12 people
Group:Customer Service
Group:Distribution
Group:Instrumentation & regulation
Group:Services
Group:Tranmission
Group:Transmission
Habituation
Health & Safety:Policies
Health Issues:Access
Health Issues:Benefits
Health Issues:Blood pressure
Health:No offshore data
Help:Request
helpdesk - concerned with their access
helpdesk - unresponsive
HIDDEN:Under the radar
Hierarchy:Security
Home-working
Home-working:Can't Comply
Home-working:Friction Outsourcing
Home-working:Positive
Home Security:Can't Comply
Home Security:Compliance
Home Working:Remote Access
hot desk - no hot desking
HR induction:20 people
HR induction:paperwork
HR induction:questions
HR:On-boarding
Identification
Identification: Name
Identification:Challenges
Identification:Covering Colleagues' Work
Identification:Work Access
Implementation:Planning
Incidents:Verbal & Physical Assault
Individual Responsibility
Induction:Online training
Induction:Safety Culture
Information Security:Prevalence
Information:Archive
Information:Department
Information:Faxes
Information:Phone
Infrastructure
Infrastructure:Drive Encryption Software
Infrastructure:Encrypted Hard Drives
Infrastructure:Problematic Mechanism
Infrastructure:Problematic Technology
Infrastructure:Problems
Infrastructure:Property Services
Infrastructure:Separation
Infrastructure:Technology
Inhouse:Business Analysts
Insider:Incident
Insider:Malicious
Insiders:Malicious

Installation:Software Request
Integrity:Data
Internet:Abuse
Internet:Access
Internet:Blocked
Internet:Lunchbreak
Internet:Not Blocked
Internet:Personal Browsing
Internet:Restrictions
Intranet:Security Information
Intranet:Work Group
IT
IT Funding:Upgrade
IT Helpdesk:Locked Out
IT Outsourcing:Decreased Productivity
IT People:Reward
IT Platforms:Design and Architectural Work
IT problem:Decreased productivity
IT Process:Burden
IT Support
IT Support:Access Rights
IT Support:Authentication
IT Support:Competence
IT Support:Effectiveness
IT Support:Helpdesk
IT Support:Installation of Software
IT Support:Outsourcing
IT Support:People
IT Support:Positive Experience
IT Support:Preference In-house
IT Support:Reduced Effectiveness
IT Support:Same Day
IT Support:Short waiting time
IT Support:Ticket Request
IT Support:Time Factor
IT System:Fraud and Security Policies
IT Systems:Architecture Standards
IT:Change
IT:Consequences
IT:Fix
IT:Helpdesk
IT:Inhouse
IT:Migration to Laptops
IT:No formal training
IT:No major problems
IT:Personal
IT:Problems
IT:Remote Assistance
IT:Timely
IT:Trust
Job Role:Analyst
Job Role:Category Manager
Job Role:Contractor
Job Role:Financial Analyst
Job Role:Project Manager
Job Role:Senior Analyst
Job Status:Employee
Job:Analyst Policy Group
Job:Designer
Job:Electrician

Job:Verification
Jobs
Jobs:Equal benefits
Jobs:Outsourcing
Jobs:Reapplying
Jobs:Transit
Knowledge of Policy:Low
Knowledge Sharing
Knowledge Sharing:Communication
Knowledge Sharing:Documentation
Knowledge Sharing:Interdepartmental
Knowledge Sharing:Presentation
Knowledge Sharing:Technology
Knowledge:Lack of Staff
Knowledge:Organisational Citizenship Behaviour
Knowledge:Policies
Knowledge:Security
Knowledge:Specialised
Knowledge:System
Knowledge:Technology
lack of awareness - need to physically protect laptop
Laptop
laptop - aware about need to protect it
laptop - closed built
laptop - has two
laptop - is password protected
laptop - need to give a justification for Open-built laptops
laptop - Open built
Laptop:Back up
Laptop:Backup
Laptop:Boot
Laptop:Company Encrypted
Laptop:Confidential Data
Laptop:Docking Station
Laptop:Does not leave on desk
Laptop:Encrypted
Laptop:Home working
Laptop:Locked cabinet
Laptop:Log in
Laptop:Network Drive
Laptop:No Secured Storage
Laptop:On desk
Laptop:Ordering System
Laptop:Password Protected
Laptop:Secure
Laptop:Storage
Laptop:Theft
Laptop:Transit
Laptops:Encryption
Laptops:Transit
Learning
Legacy:HR Systems
Legacy:Servers and Applications
Legacy:Third Party
length of service
Line Manager:Customer Data
Local Storage:Back up
Location:Leeds
Location:Leeds and Slough
Location:Office

Lock Out:Password Reset
Lock Screen
Lock Screens
Lock Screens:Automatic
Lock Screens:Enforced Policy
Locked Screen
Locked Screen:Quick Setting
Locked Screen:Reminder
Locked Screens
Locked Screens:Norm
Locked Screens:Reminder
Log-in:Drop Connection
Malicious Insider
Manage:Customer Systems
Management:4 people
Manager:Security Awareness
Managerial
Managers:Responsibilities
Merger:2 Companies
misconception - blocked facebook protects personal information
misconception - confidential data deleted from laptop and recycle bin (TECHNICAL ROLE - SHOULD HAVE KNOWN DELETION IS NOT SECURE)
misconception - desktop not C drive
misconception - everyone told about security at some point so awareness must be good
misconception - filtering provide protection for data (???)
misconception - misunderstanding security purpose
misconception - no data on laptop is confidential so would not be a problem
misconception - nothing security-related specific to their role
misconception - password protection perceived as encryption
misconception - PDF prevents people changing, copying and pasting things
misconception - sending documents through emails is secure
Mitigation:Guard
Modes of Working
Naive?
Network Drive
Network:Broadband
Network:Connection
New Starter:Intranet
New Starter:No Laptop
No Evidence:Inappropriate Access
Non-compliance
Non-Compliance:Attributed to accidental error
Non-compliance:Can'tComply
Non-Compliance:Challenge
Non-Compliance:Circumvention
Non-compliance:Cost too high
Non-Compliance:Credit Card System
Non-Compliance:Culture
Non-Compliance:Documents
Non-compliance:IT Helpdesk
Non-Compliance:Lack of Security
Non-compliance:Memory Sticks
Non-compliance:No incentive
Non-Compliance:Non-malicious
Non-compliance:Organisational Consequences
Non-compliance:Password
Non-compliance:Personal Consequences
Non-Compliance:Personal Risk
Non-Compliance:Reprimanded
Non-Compliance:Security Breach

Non-Compliance:Sharing Passwords
Non-Compliance:Software
Non-compliance:System
Non-Compliance:Time
Non-Compliance:Won't Comply
Non-compliant:Breached Security Protocol
Non-compliant:Old Assets
Office Based
Office Based:Assigned desk
Office Based:Frequency
Office Based:Sometimes
Office:Friction Outsourcing
On-boarding:Basic information
Online Training:Accounting
Online:websites
OPEN
Organisational Change:Open environment
Organisational Change:Outsourcing IT
Organisational Change:Security
Organisational Change:Security Culture
Organisational Change:Security Policies
Organisational Change:Security Priority
Organisational Consequences:Decreased Productivity
Organisational Consequences:Efficient
Organisational Consequences:Locked out
Organisational Consequences:Low Security Culture
Organisational Consequences:Outsourcing IT
Organisational Consequences:Turnover
Organisational Risk:No Encryption
Organisational Support:Clearance Process
Organisational:Hierarchy
Outsourced Jobs:Equal benefits
Outsourcing
outsourcing - decline in service quality
Outsourcing IT
Outsourcing IT:Decreased productivity
Outsourcing IT:Difficult to understand
Outsourcing IT:Function
Outsourcing IT:Increased waiting time
Outsourcing IT:Low cost country
Outsourcing IT:Not personalised
Outsourcing IT:Perception
Outsourcing IT:Possibility
Outsourcing Projects:China
Outsourcing:Consequences
Outsourcing:Decreased Productivity
Outsourcing:Employees
Outsourcing:Frustration
Outsourcing:Function
Outsourcing:Guarantee jobs
Outsourcing:IT
Outsourcing:Low Quality
Outsourcing:Not happy
Outsourcing:Productivity Decrease
Outsourcing:Unhelpful
Outsourcing:Unsuitable for Organisation
Paper:Shredding
Paperless:Hot-desking
Password
password - advised to change default

password - advised to keep changes simple!!!
password - advised to not make it easy to remember
password - advised to set it to username
password - change - rules are quite different across different systems
password - change - rules cause problems
password - change time varies - some haven't been changed for years
password - has quite a few
password - keep all the same
password - keep changes simple
password - need to reset those often
password - only has two passwords - other systems are Open access
password - reset easy
password - reset slow
password - reset verification not secure
password - set it to username
password - shared area passwords can be guessed
password - sharing done
password - sharing done - changed password
password - sharing done - not changed password
password - sharing not happens
password - simple word
password - uses month
password - writes on locked piece of paper
password - writes those in document
Password Changes:All Passwords
Password Changes:Different Time Periods
Password Changes:Every month
Password Construction:Pattern
Password Cracker
Password Generation:No System
Password Management
Password Management:Cognitive Effort
Password Management:Doesn't Save
Password Management:External to Work
Password Management:Length
Password Management:Locked out
Password Management:Password Reuse
Password Management:Recycling
Password Management:Software
Password Management:System
Password Management:Unmemorable
Password Reset:1 System
Password Reset:System
Password Sharing:Doesn't Share
Password Sharing:No Evidence
Password Storage:Note on Phone
Password Storage:Write down
Password Strategy:Memorable
Password:Changes
Password:Changes Automated
Password:Cognitive Effort
Password:Does not share
Password:Forgot
Password:Frequency Memorable
Password:Locked out
Password:Management:Locked out
Password:No Paper Storage
Password:Numerous
Password:Remember me
Password:Reminder

Password:Reset
Password:Rules
Password:Same
Password:Strategy
Password:Synched
Password:System
Password:Systems
Password:Timeframe
Password:Work and Personal
Password:Write down
Passwords
Passwords Management
Passwords Reset:Can't at home
Passwords Reset:LAN reset
Passwords:Breach
Passwords:Changes
Passwords:Cognitive Effort
Passwords:Cogntive Effort
Passwords:Complexity Rules
Passwords:Construction
Passwords:Different Rules
Passwords:Don't Share
Passwords:Dozen
Passwords:Effort
Passwords:Electronic Storage
Passwords:Expiry
Passwords:Forgotten
Passwords:ID
Passwords:Incorrect
Passwords:Log
Passwords:Low Cognitive Effort
Passwords:Mechanism
Passwords:Memorable
Passwords:Memory
Passwords:No Paper Storage
Passwords:Not Sharing
Passwords:Numerous
Passwords:Pattern
Passwords:Policy
Passwords:Protected Document
Passwords:Random
Passwords:Reduce Cognitive Effort
Passwords:Remember Me
Passwords:Reset
Passwords:Reset Online
Passwords:Reset with same password
Passwords:Same
Passwords:Same one
Passwords:Secure
Passwords:Self-generated
Passwords:Separate
Passwords:Sharing
Passwords:Single Sign-On
Passwords:Storage
Passwords:Strategy
Passwords:Synchronise Change
Passwords:System
Passwords:Time-Limited
Passwords:Training
Passwords:Write down

PCIDSS Compliance:Protocols
PCIDSS Compliance:Secure Credit Card Information
People:Information-Seeking
People:Technical
Perception
Perception of Expertise:Informed User
Perception of IT:Efficient
Perception of Risk:Fear of Virus
Perception of Risk:Locked Screens
Perception of Risk:Websites
Perception of Safety
Perception of Security
Perception of Security Culture:Medium
Perception of Security Risk:Customer Credentials
Perception of Security:Easy to Tailgait
Perception of Security:High Level
Perception of Security:Safety Culture
Perception that screen lock timings can't be changed
Perception:Low financial reward
Perception:Safety
Performance Objectives:Circumvention reduced
Performance Security
Performance:Recorded Calls
Permissions
Permissions:PA
Permissions:Sharepoint
Personal contacts:IT
Personal Devices:Company Wifi
Personal Devices:Music
Personal Devices:None used
Personal Devices:Not Connected to Network
Personal Devices:Phone
Personal Email:Hacked
Personal Security
Physical Security
physical security - assume people in the building have right to be there
physical security - aware about need to challenge, don't do it though
physical security - challenge people in the building without ID
physical security - easy for someone to gain unauthorised access
physical security - people would not challenge someone tailgating
physical security - someone without a pass would be picked by someone
physical security - strong ability to not let unauthorised individuals enter premises
physical security - takes some caution with host desking people - make sure they are not strangers
Physical Security:Access
Physical Security:Access Building
Physical Security:Badge
Physical Security:Barriers
Physical Security:Breaches
Physical Security:Building Access
Physical Security:Cameras
Physical Security:Car park
Physical Security:Card
Physical Security:Cards
Physical Security:CCTV
Physical Security:Challenge
Physical Security:Documentation
Physical Security:Functional
Physical Security:Guards
Physical Security:Hot Desking

Physical Security:Incident Reporting
Physical Security:Intruders
Physical Security:Laptop
Physical Security:Lockable Cabinet
Physical Security:Lockable drawers
Physical Security:Locked cabinet
Physical Security:Manned Gates
Physical Security:Meeting Booking
Physical Security:Negative Experience
Physical Security:No Access
Physical Security:Not functional
Physical Security:Risk
Physical Security:Secure
Physical Security:Secure Rooms
Physical Security:Security Incident
Physical Security:Tailgaiting
Physical Security:Tailgating
Physical Security:Unbadged Personnel
Physical Security:Unchallenged
Physical Security:Unenforced
Physical Security:Unmanned Technology
Physical Server:Software
Physical Server:Softww
Policy
policy - a lot of governance procedures
policy - actively try to stay up to date
policy - aware about policy regarding their role
policy - common sense
policy - compliance depends on individual
policy - does not check policy website
policy - electricity and gas procedures do not include security
policy - impossible to know everything
policy - incident driven
policy - information on Info Net
policy - knows little about policies
policy - no idea about policies
policy - no idea where policies are
policy - no sanctions
policy - people know quite a lot about the policies
policy - violations on someone's discretion
Policy:Legislation
Policy:Locked Screen Timings
Policy:Paperless
Policy:Recycling
Policy:Refuse
Policy:Transmission
Positive affect:Language
Previous Employment:Consulting
Previous Employment:Start-up Company
Primary Task:Friction
Printing
Problem-Solving:Escalate upwards
Problem:Legacy components
Process
Process:Access
Process:Administration
Process:Audit
Process:Authentication
Process:Burden
Process:Bureacratic

Process:Clearance
Process:Conference Calls
Process:Delayed
Process:Departments
Process:Difficult
Process:Documentation
Process:Documentation Sharing
Process:Frustration
Process:Health Issues
Process:Ineffective
Process:Interdepartmental differences
Process:Interface
Process:IT
Process:Lack of Consequences
Process:Lack of knowledge
Process:Legal Compliance
Process:Non-disclosure
Process:Not user-friendly
Process:Numerous
Process:Passwords
Process:Photographic ID
Process:Project delay
Process:Redaction
Process:Time delay
Process:Tracking
Process:Verification
Procurement:Low Security Emphasis
Procurement:Software
Productivity:Decreased
Productivity:Increased
Program Mgt Role:10 years
Program Support Person:Sharepoint
Program:Log on
Project
Project blocks:Shared Experience
Project Delivery:Responsibility
Project Delivery:Security Guidelines
Project Launch:NDA
Project Launch:Sensitive Information
Project Plan:Build in Security
Project Responsibility
Project Solving:Escalate
Project:Budget
Project:BYOD
Project:Compliance
Project:Design Documentation
Project:Design Documents
Project:Documentation
Project:Functionality
Project:Health
Project:Importance
Project:Interdepencies
Project:NDA
Project:Priorities
Project:Requirements
Project:Scope
Project:Security Policy Compliant
Project:Strategy
Project:Technology Requirements
Project:Time delay

Projects
Projects:Competitors
Projects:IT
Projects:NDA
Projects:Security
Protocols:15
quote - "can use unencrypted" - security manager
quote - "close down everything before outsourcing control centre takes over"
quote - "company would prefer the job done"
quote - "documents syncronised somewhere"
quote - "passwords for shared files all the same"
quote - asks security policies regarding what?
quote - aware but not know any policies
quote - loss of access to a shared area resulted to problems for company
quote - ordered secure USB after major leak
quote - ordered to change rucksack
quote - password and screen lock should be their only concern
quote - password sharing
quote - people moan so a good thing
quote - people went through disciplinary procedures for sending inappropriate emails
quote - policy content by policy designer
quote - security manager's perception
quote - should not trust people as much
quote - social engineering - "would target someone else"
quote - social engineering "very common"?
quote - takes weeks to get something up
quote - too many sharepoint sites so someone must have a reason to look for a specific one
quote - understands that trusting employees is not easy in the current 'cyberterrorism environment'
quote - usb can use unencrypted ones for non-critical data
Refuse:Health and Safety
Relocation:Biased towards other company
Relocation:Burden
Reloccation:Expertise decrease
Remote Access
Remote Access:Ease of use
Remote Access:Email
Remote Access:Extranet
Remote Access:Infrequently use
Remote Access:Laptop at Home
Remote Access:Outlook
Remote Access:RSA keys
Remote Access:Time
Remote Access:VPN
Remote Access:Working hours
Remote Working
Removable Drives
Removable Drives:Usage
Removable Drives:USBs
Removeable Devices:Memory Sticks
reporting - afraid to report
reporting - motivation - charity
Research:Commodity Markets
Research:Internet Based
Research:Website Blocks
Reset:Fast
Reset:IT
Reset:Password
Reset:Unlock
Resources:Delegation of Authority

Resources:Financial Billing
Resources:Time Allocation
Responsbility:Region
Responsibilities
Responsibility:Call Centres
Responsibility:Confidentiality
Responsibility:Region
Responsibility:Security Policy
Restrictions:NDA
Retrieval:Software
Retrival:Index Calls
Risk
Risk Awareness:Low
Risk Awareness:Positive
Risk Mitigation:Shredding faxes
Risk Perception:Aware
Risk Perception:Low
Risk Process:Risk Mitigation
Risk Register
Risk Understanding:high
Risk Understanding:Low
Risk Understanding:Negative
Risk Understanding:Neutral
Risk Understanding:Positive
Risk Undestanding:Negative
Risk: Personal Consequences
Risk:Appropriateness
Risk:Behavioural
Risk:Compliance as Collusion
Risk:Duplicate Passwords
Risk:Encryption
Risk:Hacking
Risk:Mitigation
Risk:Organisational
Risk:Organisational Consequences
Risk:Password Document
Risk:Passwords Synched
Risk:Perception
Risk:Personal
Risk:Technology failure
Risks:Awareness
Risks:Lack of Awareness
Role
role - customer facing
role - deals with health, safety and environmental teams
role - finance
role - infrastructure repairs
role - planning
role - security
role - sees confidential information
role - started as a contractor
role - technical
role - work does not involve critical national infrastructure
role - works away from the office often
Role Function:Demolitions
Role Function:Service upgrades
role: critical infrastructure
Role: Security Access Control Team Leader
Role:Access and Registration
Role:Access live systems

Role:Analyst
Role:Behaviour Change
Role:Business
Role:Business & IT
Role:Business Analyst
Role:Business Analysts
Role:Business Management IT
Role:Business Requirements
Role:Buying Team
Role:Change & Project Manager
Role:Contractor
Role:Controller for NERC CIP information
role:critical infrastructure
Role:Customer identity, access and authentication
Role:DGT Engineer
Role:Director CIPS
Role:Electricians and customers
Role:employee
Role:Employee and Contractors
Role:Enrichment
Role:Ex-teacher
Role:External facing
Role:Financial Analyst
Role:Graduate Development Programme
Role:Group Manager
Role:Head of Integration Delivery Depot
Role:Head of Internal Telephony
Role:Head of Service Management Transformation and Governance
Role:Head of Telephony
Role:Health & Safety Consultant
Role:Health & Safety Mgr
Role:Investment Finance Manager
Role:IT Business Partner
Role:IT Director
Role:IT Infrastructure Architect
Role:Manager
Role:Market Research/Trends
Role:No CISO
Role:Order Processing
Role:Problem-Oriented
Role:Program Mgr IT Operations
Role:Project Manager
Role:Responsibility for Internal Telephony Systems
Role:Strategy and Market Intelligence Analyst
Role:Supervisor
Role:Team Leaders
Role:Technology
Role:Telephony Design Mgr
role:transmission planning
Roles:Organisation
Roles:Projects
Roles:Support Management
Safety
Safety Risk:Pipelines Hit
Safety:Electrical
Safety:Faulty parts
Safety:Gas pipelines
Safety:Pipelines Hit
screen lock - always does it
screen lock - challenges people

screen lock - don't do it
screen lock - due to peer pressure
screen lock - knows about it, don't do it
screen lock - most others do it
screen lock - other's don't do it
Screen Lock:Enforced
Secure Disposal
Secure ID:Regular access
Secure:Technology
Security
security - area for improvement (outdated systems, adoption on new technologies)
security - awareness exists not reinforcement
security - awareness not as good as previous employer
security - blanket rules fore everyone not much value
security - business continuity well planned
security - by obscurity
security - current implementation provides adequate protection
security - need to be a bit more proactive
security - need to use 'common' sense
security - not excessive
security - not sure how secure the system is
security - reported problems not seemed to be followed up
security - risk tight policies are a necessity
security - thinks they should be doing more on security
security - thinks too much security is bad
Security Aware:Customer Passwords Confidential
Security Awareness
Security Awareness Training:Background Checks
Security Awareness Training:CIP training
Security Awareness Training:Consequences
Security Awareness:Badges
Security Awareness:Contractual
Security Awareness:Customer Passwords
Security Awareness:Improving
Security Awareness:Increased
Security Awareness:Low
Security Awareness:No company data on laptop
Security Awareness:Policies
Security Awareness:Policy
Security Awareness:Question Urgent Access
Security Awareness:Responsibility
Security Awareness:Security Risks
Security Awareness:Sensitive Data
Security Awareness:Sharing Documents
Security Awareness:Team
Security Awareness:Time
Security Awareness:Training
Security Awareness:Transgression
Security Breach:Front Desk
Security Breach:Identified
Security Breach:Receptionist
Security Breaches:None
Security Breaches:Not Aware
Security Breaches:Unaware
Security Communication
Security Communication:Emails
Security Communication:Induction
Security Communication:Ineffective
Security Communication:Irrelevant to user
Security Communication:Line Managers

Security Communication:Not Aware
Security Communication:Posters
Security Communication:Safety
Security Communications:Classification of data
Security Competence:Effective
Security Compliance:Lack of sanctions
Security Compliance:Most employees
Security Compliant
Security Conscious
Security Conscious:Project Managers
Security Contact:Line Manager
Security Culture
Security Culture:Challenge
Security Culture:Change
Security Culture:Cognitive Effort
Security Culture:Compliance
Security Culture:Decreasing
Security Culture:Deteriorating
Security Culture:Different companies
Security Culture:Encrypted laptop
Security Culture:Evaluation
Security Culture:High
Security Culture:Improved
Security Culture:Lack
Security Culture:Locked Screens
Security Culture:Locking Screens
Security Culture:Low
Security Culture:Management
Security Culture:Negative
Security Culture:Screen Lock
Security Culture:Security Conscious
Security Detection:Low
security driver - backup
security driver - balance for canteen on security card
security driver - chinese wall needs to be enforced
security driver - habit
security driver - health and safety
security driver - information availability
security driver - Information sensitivity
security driver - management pressure
security driver - past events
security driver - policy
security driver - productivity
security driver - regulation, standards-based security
security driver - responsibility
security driver - rewards
security driver - sanctions
Security Driver:NERC CIP
Security Flaw:Access Pedestal
security implementation - awareness better than previous employer
security implementation - logging - data not audited - location, deletion etc
Security Implementations:High Standard
Security Incidents:No Evidence
Security Induction:Short
Security Information:Passwords
Security Information:Safety Messages
Security Message
Security Messages:Yammer
Security Mitigation:Mgr Signs off
Security Non-compliance:Challenge

Security Non-compliance:Intentional
security perception - email and websiite blocks
security perception - if people try too much they can break through firewall
security perception - needs improvement
security perception - systems and network are secure
Security Policies
Security Policies:Changed
Security Policies:Enforce Password Rules
Security Policies:Guidance
Security Policies:Knowledge
Security Policies:Unsure compliant
Security Policy
Security Policy Breach:Consequences
Security Policy: Read
Security Policy:Accessing Blocked Websites
Security Policy:Adhered to
Security Policy:Appropriate
Security Policy:Aware
Security Policy:Blocked Sites
Security Policy:Breached
Security Policy:Can't Connet Personal Devices
Security Policy:CBTs
Security Policy:Check
Security Policy:Cognitive Effort
Security Policy:Communication
Security Policy:Company Website
Security Policy:Compliance
Security Policy:Consequences
Security Policy:Consult
Security Policy:Documents, Personal Security, Customer Info
Security Policy:Effort
Security Policy:Encryption
Security Policy:Exceptions
Security Policy:Flexibility Required
Security Policy:Guidance
Security Policy:Important
Security Policy:Internet Restrictions
Security Policy:Intranet
Security Policy:Issues
Security Policy:Locked Screens
Security Policy:Low Awareness
Security Policy:Necessary
Security Policy:No Encryption Policy
Security Policy:Not aware of
Security Policy:Not enforced
Security Policy:Not flexible
Security Policy:Not read
Security Policy:Onerous
Security Policy:Passwords
Security Policy:Perceived Restriction
Security Policy:Personal Browsing
Security Policy:Physical Security
Security Policy:Protect
Security Policy:Refresh
Security Policy:Responsibilities
Security Policy:Responsibility
Security Policy:Review
Security Policy:Review Date
Security Policy:Rule-focused
Security Policy:Rules

Security Policy:Screen Lock
Security Policy:Secure documents
Security Policy:Supported by Process
Security Policy:Time
Security Policy:Transit Laptop
Security Policy:Unaware
Security Policy:Understanding
Security Policy:Unreadable
Security Policy:USBs
Security Policy:Visitor Access
Security Policy:Visitors
Security Pragmatism?
Security Process:Consequences
Security Process:Risk
Security Process:Slow
Security Protocols:Customer Information
Security Protocols:Strictest Confidence
Security Protocols:Unauthorised Access Attempts
Security Requirements:Agreement
Security Requirements:Documentation
Security Review:Delay in Software Deployment
Security Risk
Security Risk: No Security Training
Security Risk: Reduced due to no home-working
Security Risk:Access
Security Risk:Access Control
Security Risk:Access Customer Information
Security Risk:Admin Rights
Security Risk:Agents Access Calls
Security Risk:Authentication Process
Security Risk:Awareness
Security Risk:Belief Unauthorised Access Monitored
Security risk:Cancelling the account
Security Risk:Circumvention
Security Risk:Concrete
Security Risk:Conference calls
Security Risk:Confidential Data
Security Risk:Confidential Data in Waste
Security Risk:Consequences
Security Risk:Considerable
Security Risk:Contractor Spoofing
Security Risk:Cookie Sniffing
Security Risk:Customer Access
Security Risk:Customer Service Agents Access Calls
Security Risk:Data
Security Risk:Data Streaming
Security Risk:Duplicate Passwords
Security Risk:Email Data
Security Risk:Email Familiar
Security Risk:Eradicate
Security Risk:Files on desktop
Security Risk:Fraud
Security Risk:Group Log in
Security Risk:Hacking
Security Risk:Identification
Security Risk:Identify risks
Security Risk:Illusion of Security?
Security Risk:Information Exchange
Security Risk:Insecure Data Storage
Security Risk:Insider

Security Risk:IPR Breach
Security Risk:Lack of Interest
Security Risk:Laptop
Security Risk:Laptop in car
Security Risk:Leavers
Security Risk:Legacy Systems
Security Risk:Limited Enforcement
Security Risk:Local Storage of Docs
Security Risk:Lose Secure ID Cards
Security Risk:Low
Security Risk:Low Awareness
Security Risk:Malicious Insider
Security Risk:Mitigated
Security Risk:No Backups
Security Risk:No Encryption
Security Risk:No enforced clear desk policy
Security Risk:No Password
Security Risk:No Review
Security Risk:No Sensitive Data
Security Risk:No Verification
Security Risk:Open Plan
Security Risk:Organisational Security Culture
Security Risk:Paper Shredding Delay
Security Risk:Password
Security Risk:Password Pattern
Security Risk:Password Reset
Security Risk:Password Sharing
Security Risk:Password Storage
Security Risk:Password System
Security Risk:Passwords
Security Risk:Passwords Synched
Security Risk:Passwords Visible
Security Risk:Perception Password Protected
Security Risk:Personal Data
Security Risk:Personal Email
Security Risk:Personal Information
Security Risk:Physical Security
Security Risk:Pin
Security Risk:Pipelines Hit
Security Risk:Policy
Security Risk:Potential
Security Risk:Reduced
Security Risk:Refuse Access
Security Risk:Revoke Access
Security Risk:Same password across systems
Security Risk:Security Code for Conference Calls
Security Risk:Sell Customer Information
Security Risk:Share Passwords
Security Risk:Sharepoint
Security Risk:Short-cuts
Security Risk:Shoulder Surfing
Security Risk:Signed Security Document
Security Risk:Social Phishing
Security Risk:Spam
Security Risk:Spoof customer data
Security Risk:Starters & Leavers
Security Risk:Tailgaiting
Security Risk:Taped to laptop
Security Risk:Theft of laptop
Security Risk:Unaware of policies

Security Risk:Unencrypted laptop
Security Risk:Unencrypted USBs
Security Risk:Unlocked Screen
Security Risk:Unquestioning
Security Risk:USBs
Security Risk:Write down passwords
Security Risks
Security Risks:Access
Security Risks:Awareness
Security Risks:Concrete
Security Risks:Consequences
Security Risks:Data
Security Risks:Documentation
Security Risks:Documentum
Security Risks:Lack of Awareness
Security Risks:Managed
Security Risks:Outsourced IT support
Security Risks:Registration
Security Risks:Threat of Attack
Security Rules:Doesn't Follow
Security Rules:Workable
Security Standard:Payment Card Industry Data Security Standards
Security Strategy:Same Password
Security Theatre?
Security Threat:Malicious Insider
Security Trade-off
Security Training
Security Training:Business
Security Training:CBTs
Security Training:Confidentiality
Security Training:Consulting
Security Training:Efficacy
Security Training:Guidelines
Security Training:IT Helpdesk
Security Training:Lack of
Security Training:Mandatory
Security Training:Not Memorable
Security Training:Not Received
Security Training:Online
Security Training:Positive perception
Security Training:Unmemorable
Security Transgression:Password Sharing
Security Transgressions:USBs
Security: Access
Security: group
Security: Lack of awareness
Security: No encrypted USB drives
Security: Risk Communication
Security:Access
Security:Access Control
Security:Action
Security:Agreement
security:agreements
Security:Attitude
Security:Audits
Security:Authentication
Security:Awareness
Security:Awareness Training
Security:Backups
Security:Blocked Sites

Security:Bureaucratic
Security:Business
Security:Business Objectives
Security:Buy-in
Security:CBT
Security:CBTs
Security:Challenge
Security:Circumvention
Security:Clear-desk Policy
Security:Cognitive Effort
Security:Commercially Sensitive
Security:Common Sense
Security:Communication
Security:Competitors
Security:Compliance
Security:Compliance Standards
Security:Confidential Data
Security:Confidential Documents
Security:Confidentiality Documents
Security:Consequences
Security:Convenience
Security:Costs
Security:Credit Card Details
Security:Culture
Security:Cusmomer Credentials multiples places
Security:Customer Data
Security:Customers
Security:Data
Security:Data Classification
Security:Data Storage
Security:Delete inbox
Security:Different Meanings
Security:Different Systems
Security:Discretionary
Security:Document Shredding
Security:Email
Security:Encrypted Calls
Security:Encrypted devices
Security:Encrypted Hard Drive
Security:Encrypted laptop
Security:Encrypted Memory Sticks
Security:Encrypted USBs
Security:Encrypted VOIP
Security:Encryption
Security:Evolving
Security:Exceptions
Security:Exemption
Security:Expectation
Security:Firewalls
Security:Follow Protocols
Security:Fraud Investigations
Security:Friction
Security:Frustrating
Security:High Level
Security:High Priority
Security:Important
Security:Improve Awareness
Security:Improved
Security:Improved Printing System
Security:Inappropriate Rules

Security:Incidents
Security:Induction
Security:Information
Security:Integral to Project Planning
Security:International Boundaries
Security:IP Information
Security:IT Testing
Security:Lack of enforcement
Security:Lack of Engagement
Security:Lack of implementation
Security:Lack of Interest
Security:Lack of technological support
Security:Lack of understanding
Security:Laptop
Security:Laptop Boot
Security:Laptop Home
Security:Laptop Location
Security:Laptop Storage
Security:Laptops
Security:Learn Via Colleagues
Security:Legislation
Security:Location
Security:Lock PC
Security:Locked cabinet
Security:Locked down
Security:Locked Screen
Security:Locked Screens
Security:Loss
Security:Low Priority
Security:Lower Priority
Security:Mandatory
Security:Memorable
Security:Messages
Security:Micro-Culture
Security:Mitigation
Security:Narratives
Security:Need for Encryption
Security:No Customer Data Access
Security:No Incidents
Security:No monitoring
Security:No perceived friction
Security:No Review
Security:No sharing restrictions
Security:No visible breaches
Security:Non-compliance
Security:Not Enforced
Security:Not mentioned
Security:Paperless
Security:Password
Security:Password Changes
Security:Password Protected
Security:Passwords
Security:Perceived Important
Security:Performance Impact
Security:Permissions
Security:Personal Sensitive Data
Security:Policies
Security:Policy
Security:Previous Organisation
Security:Primary Task Friction

Security:Priority
Security:Process
Security:Procurement
Security:Project
Security:Project Design
Security:Property Access
Security:Questions
security:regulations
Security:Remote access
Security:Report Inappropriate Access
Security:Report Inappropriate Behaviour
Security:Restricted access
Security:Restrictions
Security:Restrictive
Security:Revoking Access
security:risk
Security:Risk Based Approach
Security:Risk Communication
Security:Risk Mitigation
Security:Role Specific
Security:RSA login
Security:Safety Online
Security:Screen Lock
Security:Secondary Task
Security:Secondary to Safety
Security:Secure ID
Security:Self Awareness
Security:Sensitive Data
Security:Sensitive Information
Security:Sharepoint
Security:Show & tell
Security:Staff
Security:Tailgate
Security:Technology
Security:Theft of GPS
Security:Time-Consuming
Security:Training
Security:Ubiquitous
Security:Unlocked Screens
Security:Validity
Security:Virus Checker
Security:VPN
Security:Vulnerabilities
Security:Vulnerability
Security:Work Laptop
Security;Communication
Securty:Improved
Self Awareness:Trusting
Senior
Senior:Overworked
Sensitive Data:Accident Investigations
Sensitive Data:Credit Card
Sensitive Data:Limited exposure
Sensitive Data:Non-disclosure Agreement
Sensitive Data:Shared Drives
separation - personal from work devices
Service Work:Short time period
Services
Services:Different Passwords
Share Computer:Shoulder-Surfing

Share Documents:Shared Drive
Shared Authentication:Mapping System
Shared Documents:Shared Drive
Shared Documents:Sharepoint
Shared Service:Improved Security
Sharepoint:Advantages
Sharepoint:Document Search
Sharepoint:Ease of use
Sharing Data:Email
Sharing Data:Encrypted USB drives
Sharing Data:Sharepoint
Sharing Documents:Email
Sharing Documents:Shared Drive
Sharing Documents:Sharepoint
Sharing Information:Learning
Shredder:Locked
Sister Groups:Corrosion & Asset Replacement
Smartphone:Password Protected
Social Circumvention:Does not engage in
social engineering - 'nature of the company doesn't allow for this'
social engineering - does not know what it is
social engineering - not aware of any social engineering attempts
social engineering - relatively easy to do
social engineering - reluctant to give information to someone they do not know
Social Media:Risk
Social Phishing
Social Workaround:Authorisation
Software
Software:Distribution Tool
Software:Encryption
Software:Filtering Spam
Software:Function
Software:Global product
Software:Installation
Software:Manipulation
Software:Not functioning
Software:Retrieve Lightening Data
Software:Test
Software:Tests
Staff:Access
Staff:Contractors
Staff:Inaccessible
Staff:Overworked
Staff:Trained
Staff:Turnover
Storage
Storage:Data
Storage:Data Storage Facility
Storage:Encrypted USBs
Storage:Increased
Storage:Personal Network Drive
Storage:Server
Storage:USBs
Subscription
support - line manager
support - requests for help send
Support:Audit trail
Support:Spoof customer data
System 1
System 1:Emotional upset

System 1:Frustrations
System 1:Process
System:Customer Profile Information
System:ID
System:Lock Out
System:Password Rules
System:Storms
System:Time Entry
System:Timesheet
Systems:Access
Systems:Hardware & Application
Systems:Learn on job
Systems:Lost Cards
Systems:Numerous
Systems:Passwords
Systems:Unauthorised access attempts
Systems:Usability
Tailgaiting
Tailgating:Unlikely to Challenge
Team leader:Responsibility
Team Meetings:Weekly
Team:Incident Analysis
Team:No Direct Reports
Team:Share Documents
Team:Virtual
Technical Implementation:Secure Flash Drive
Technical Security
Technical:Development
Technology
Technology:Browser Preference
Technology:Changes
Technology:Communication
Technology:Competence
Technology:Computers
Technology:Critical Information
Technology:Dependent
Technology:Email
Technology:Failure
Technology:Functionality
Technology:Functioning
Technology:Information
Technology:Installation
Technology:Intranet
Technology:iPod
Technology:Knowledge
Technology:Laptop
Technology:Microsoft Link
Technology:Network Drive
Technology:No Encryption
Technology:Not Functioning
Technology:Personal Laptop
Technology:Project Budget
Technology:Reliability
Technology:Set up
Technology:Sharepoint
Technology:Smartphones
Technology:Software
Technology:Tool
Technology:Updates
Technology:Website

Technology:Wifi
Technology:Work-related
Technology:Work and Personal
Technology:Work laptop
Technology:Work password
Technology:Yammer
Techology:SharePoint
Telephony System:Computer Telephony Integration Control
Telephony System:Different Locations
Telephony:Customer Calls
Telephony:Different Systems
Telephony:Office Type Systems
Telephony:Systems
Telephony:Traditional & IP based
Tenure: 2 years
Tenure:1 year
Tenure:13 years
Tenure:18 months
Tenure:2 years
Tenure:5 years
Tenure:8 years
Theft:Laptop
Third Party:Software Provider
Time
Time:Access to System
Time:Encryption
Time:Locked Screens
Time:Office-based
Time:Password Changes
Time:Technology
Tradeoff: Deadlines vs Security
Training
training - based on colleague initiative
training - believes they have not been given appropriate guidance
training - induction physical security and health and safety
training - never been trained on information security
training - sure they have been told some stuff when started - no further training
Training:Appropriate Level
Training:Awareness
Training:Business-Specific Talks
Training:CBTs
Training:CIP
Training:Confidential Information
Training:Conflict Management
Training:Content
Training:Easy to Comprehend
Training:on the job
Training:Questions
Training:Regulatory
Training:Repetitive
Training:Security
Training:Talks
Training:Technology
Transit:Laptop
Transit:Laptop in Boot
Transit:Laptop on Person
Travel:Technology
Travelling:Laptop
Trust
trust - beleives more trust could be shown towards employees

trust - each other
trust - each other so no screen lock
trust - less trust could be shown towards employees
trust - need to trust other users to use sharepoint
trust - new starters not trusted early
trust - nothing stops you from harming company
Trust:Colleagues
Trust:Consequences
Trust:Contractors
Trust:Employees
Trust:Not Security
Type:Naive?
Type:Rule-breaer
Type:Rule-breaker
Type:Rule-breaker?
Uncooperative:challenge security
Understanding:Problematic
Unencrypted USBs
Unenforced Policy:USBs
Uninformed
Uninformed?
Usability
USB - can bring own USB if encrypted
USB - cannot buy secure USBs themselves as it creates problems with audits
USB - company ones are too small
USB - company ones take time to get
USB - not aware of a USB policy
USB - not uses those to avoid virus transfers
USB - unencrypted one, shared around in the office
USB - unencrypted ones are used
USB - uses company provided
USB:Encryption
USBs:Encrypted
vendor - heavy reliance on security of IS partners
vendor - need to sign confidentiality agreements to share information
vendor access - information sharing done through known contacts/individuals
vendor access - quite relaxed about vendor access
Verification:Account Holder
Verification:Credentials
Verification:Customer
vetting - background checks for vendors
vetting - different levels exist depending on the projects
vetting - employees need to go through it
violation - emails missent to them because they have a common name
violation - person managed to get in the building
Voicemail:Access
VPN - problematic access
VPN - provides full access to company systems
website blocking - access problem was addressed through the phone
website blocking - blocks business related education information
website blocking - cannot access personal sites
website blocking - no business access has been blocked in the past
website blocking - unreliable
Website:Blocked
Websites:Blocked
Websites:Permission Rights
Wireless:Access
Work Around
Work Machine:Personal Work
Work Pattern

Work Pattern:Flexible
Work Process
Work:Assigned Desk
Work:Collaboration
Work:Computers
Work:laptop
Work:Less Collaboration
Work:Network Dependence
Work:Personal Time
Work:Transit
Workaround
Workload:Prioritising
Workplace:Assigned Desk
Yammer:Infrequent use

31/10/2014 – Refined Code List
Access Control
Access Control: Document
Access Control:Account Management
Access Control:Administration
Access Control:Permission
Access Control:Remote Access
Access Control:Review
Affective Security:Neutral
Affective Security:Strong Positive
Affective Security:Strong Negative
Affective Security:Weak Positive
Affective Security:Weak Negative
Attack:Phishing Email
Authentication
Authentication:2 Factor
Authentication:PIN
Authentication:RememberMe
Clear Desk Policy
Clear Desk Policy:Enforced
Clear Desk Policy:Screen
Clear Desk Policy:Secure
Communication
Communication:Incident
Communication:Policy
Communication:Policy:Ben
Communication:Privacy
Communication:Reporting
Communication:Social Media
Data
Data:Classification
Data:Confidential
Data:Confidential:Anonymous
Data:Confidential:Commercial
Data:Confidential:Leaked
Data:Confidential:NDA
Data:Confidential:Person
Data:Confidential:Secure
Data:Confidential:Storage
Data:Loss
Data:Printing
Data:Sharing

Data:Sharing:DRM
Data:Sharing:Email
Data:Sharing:Sharepoint
Data:Sharing:Workaround
Data:Storage
Data:Storage:Backup
Data:Storage:Dropbox
Data:Storage:Encrypted
Data:Storage:Encryption
Data:Storage:Local
Data:Storage:Shared Drive
Data:Storage:Unencrypted
Education and Training
Education and Training:Behaviour
Education and Training:CBT
Education and Training:Effectiveness
Education and Training:Relevance
Human Factor:Behaviour
Human Factor:Behaviour:Memory
Human Factor:Challenging
Human Factor:Culture
Human Factor:Culture:Change
Human Factor:Culture:Excuses
Human Factor:Culture:Resistance
Human Factor:Expertise
Human Factor:Insider Attack
Human Factor:Personal Relationship
Human Factor:Responsibilility
Human Factor:Social Engineering
Human Factor:Trust
Identity:Verification
Internet Access:Bandwidth
Internet Access:Restriction
Internet Access:Restriction
Internet Access:Personal
Laptop
Laptop:Backup
Laptop:Encrypted
Laptop:Ownership
Laptop:Theft
Laptop:Transit
LaptOpencrypted
Passwords
Passwords:Attacks
Passwords:Coping Strategy
Passwords:Generation Strategy
Passwords:Number of Passwords
Passwords:Password Management
Passwords:Reset
Passwords:Reset:Frequency
Passwords:Sharing
Passwords:Sharing:Legitimate
Passwords:Temporary
Physical Security
Physical Security:Access
Physical Security:Access
Physical Security:CCTV
Physical Security:Extern
Physical Security:Hardco
Physical Security:ID Badge

Physical Security:Staff
Physical Security:Tailgate
Physical Security:Visitors
Physical Security:Lockable
Policy
Policy:Awareness
Policy:Effectiveness
Policy:Effectiveness:Workaround
Policy:Enforcement
Policy:Exception
Primary Task:Friction
Primary Task:Productivity
Primary Task:Reputation
Regulatory Compliance
Remote Working
Remote Working:VPN
Risk Understanding:Neutral
Risk Understanding:Strong Positive
Risk Understanding:Strong Negative
Risk Understanding:Weak Positive
Risk Understanding:Weak Negative
Risk:Management
Risk:Perception
Service:Contractor
Service:Helpdesk
Software
Software:Delay
Software:Installation
Software:Operating Syste
Software:Patching and Up
Software:Workaround
System:Vulnerabilities
Technical Control
Technical Control:Firewall
Technical Control:Monitoring
Technology:Hardware
Technology:Malware Protection
Technology:Mobile Device

APPENDIX 5: CASE STUDY 3 (ORGANISATION D) QUALITATIVE THEME ANALYSIS

1. Participant 2

P2 refers to the SIRO role being part of their day-to-day role. They highlight the need for more training for SIROs, such as a buddying system, which helps individuals develop into the role:

"SIRO, part of day to day role…so there's something about how the centre trains SIROs…they should have some form of closer buddying mechanism…".

P2 also suggests that the SIRO could benefit from some some of regulation or professional community, hence their comment:

"…a regulator who is very experienced at it…something like health, make the community stronger, with lawyers you have to do so many days, SIROs need to professionalised or regularly refreshed, if not keeping contact with a Government Department….".

The main theme here is conceptualising the SIRO as a professional job, such as a lawyer, which requires the job-holder to engage in continual professional development (CPD) to maintain and update skills.

AS & RU

In line with the rest of the cohort, P2's perspective on "*fictional colleagues'*" security behaviour is a *Positive Affective Security* score. P2 talks about various strategies to select usable technical mechanisms to improve staff security behaviour. One example of this is the introduction of Boardpad, which encourages "*fictional senior colleagues"* to manage confidential data more prudently by not making it read-only and not printable for instance:

"Boardpad put information into an application where a board member can access it, does not allow them to print (read only tool) – use the pen and make notes etc, information goes up before the board meeting – so they can't retain information – refusal to circulate paper by post – if hard copy needs to signed out before they leave…".

This strategic focus on integrating technical mechanisms into work processes to improve security is a theme within this interview. Another exemplar of this includes the introduction of Egress which is a software system which automatically classifies documents and manages the flow of these documents depending on their level of sensitivity to ensure highly sensitive data is not emailed out of the organisation:

"…introduced Egress, automatic classification – it will say what the classification is – force people to think about it, won't let you send something other than official sensitive…".

As with the other SIRO interviews within Case Study 3, this interview is coded as demonstrating *Positive Risk Understanding*. Examples of *Positive RU* include the P2's description of how "*fictional colleagues"* had inadvertently released confidential data linked to employee salaries because they had not fully completed the security process around the data management system. They recognised that the main risk here was that the process was not clear enough for the employee to follow since they had completed "*95% of the process*". P2 notes that this was not motivated via maliciousness but rather a procedure that was not comprehensively documented and subsequently not fully completed by the staff member. Overly complex security tasks may therefore create organisational security risks as people are likely to either not complete them effectively or circumvent due to frustration.

Security Policy: Data, Passwords and Circumventions

The employee notes that many "*fictional colleagues*" are not fully aware of security policy. For instance, they may struggle to classify different types of data and may also be unsure what documentation is appropriate to share:

"Don't see the differences between different types of data… something they struggle with, we are used to not sharing information…".

On the other hand, the employee identifies that new software assists staff in making data classification judgements, which suggests that the technical mechanisms are positively enabling security tasks:

"Introduction of Egress forces you think about the classification of documents so they now are more familiar…".

However, P2 suggests that "*fictional colleagues*" may be familiar with certain parts of the such as the security guidance on passwords, despite not being fully conversant with security policy:

"Most fictional colleagues don't know about security policy. They know about passwords perhaps…".

Interestingly, P2 goes on to acknowledge that one of the main circumventions has been around fictional colleagues sharing passwords with their Personal Assistants. P2 described this incident as a circumventions, but some "*fictional colleagues*" may discount the risk, because the individual was known to them, i.e. it was their assistant, so the familiarity of the risk acted to reduce the strength of the risk:

"Had an issue, did an audit –[fictional colleagues] share passwords – they do – lot of PA sharing because you can give access to your email, if you go on leave & you have a contractor… circumvention 'It was only my PA, I needed the thing on my system'…".

2. Participant 3

The SIRO cohort interviewed for this study included individuals with a technical and also non-technical background. This particular employee characterises their background as non-technical and highlights that their approach is consequently less technical but more pragmatic in relation to security decision-making:

"…pragmatic approach to decisions in relation to security. Not an expert, removed from it, quite healthy, taking decisions based on evidence presented, based on risks and operational needs…".

In terms of gleaning the requisite information to make risk management decisions, P3 refers to using a combination of experts but also getting opposing views particularly from trusted individuals. P3 highlights that given there is a lot of noise in relation to sources of data and consequently there is a tendency to get "*someone to tell you headline points*" and revert to using one key source. As mentioned however, the employee demonstrates that there are a plethora of views to be taken into account in order to make a balance decision. For instance, they refer to conflict between the security team and the operational teams and the need integrate both perspectives:

"Usually a bit of a conflict with security team & teams building websites…get a balanced view – sometimes doesn't support the security view – operational impact – you make an informed decision…".

In terms of SIRO needs, the participant suggested that a supportive network of people is important in assisting them fulfil their role:

"What would help SIROs [is] personal development. One of those roles gets given to someone to in the organisation, when people think they'd rather not have that. I came in and got given the role bit of upskilling being able to identify people who I can trust but something about development of the individual – the right support mechanisms, had a colleague – get a good support mechanism & do some self development...".

Senior Management – Communication of Risks

One of the key themes that this employee referred to related to the communication of risks within senior management, and specifically how that was managed within the confines of the executive committee meetings. The employee described some "*fictional colleagues"* feeling as though they were being reprimanded by the security team for incidents and possible breaches and this resulted in some of them 'opting out':

"How do you communicate risks? Executive management team meeting once a month ,other communication via the system, monthly meetings as a group one of the successes, share successes. Security would churn through pages of data, just felt like there was too much to do, people come along to be humiliated, people had opted themselves out of it. Those that should have been there didn't want to be told off by security...".

P3 not only identified a perception amongst "*fictional colleagues"* that security were going to rebuke senior members of staff for their honesty in relation to security incidents, but that this approach directly resulted in individuals not wanting to attend the meeting.

However, as the SIRO, P3 is required to manage the risks, which involves understanding what the key issues are and developing skills to unearth these issues. Consequently, P3 describes meeting "*fictiona*l" senior members of staff to identify their concerns regarding security separately so that these key individuals could "*talk openly*" without being 'rebuked' by security:

"…4 main senior people- talk openly; 'what's worrying you now?' Did that for 4 months – took the approach – people avoid disclosing everything, they didn't want to expose too much. Met with them separately, security had a spot to update on…got individuals to talk about what they had done – progress made,…a more consistent way of reporting…".

P3 describes building a culture of openness, that allows the truth about security to be discussed where "*fictional colleagues"* feel able to discuss the issues and how they have "*moved forwards*" on them:

"Got to the point needed to know specific things – all related to what have you moved forward on – they are not the most pleasant, but now people turn up and we encourage people to share – biggest success guys in the security team, generally nice relationships in the dynamics…".

P3 describes how this approach has yielded a more positive forum i.e. the reference to "*generally nice relationships in the dynamics*" to talk specifically about security threats and what has been achieved.

AS & RU

In line with the rest of the Organisation D cohort, P3 scored positive on *AS*. P3 suggests that although "*fictional colleagues"* may not be aware of a specific security policy, they were positive about security in that they wanted to "*do the right thing*" and further, they felt they had an attachment to the organisation:

"Security policy – yes we have one. If you asked fictional colleagues, they probably couldn't say. We did a comprehensive survey, we asked all of staff, staff survey more than half completed it. Key thing, number 1 we were impressed by [the] response rate. Also the sense, they really are very conscious of security and really care – attachment to the organisation –

wanting to do the right thing – there were things that might stop them feeling that they can...".

This theme around adopting a practical approach is reflected in the employee's focus on how, as a SIRO, they attempt to manage security risks:

"Pragmatic; weighing up the pros and cons, the risks the organisation is undertaking, the impact that has on individuals & data & trying to decide whether that risk is worth taking. Important to be risk averse in real life [you] need to be more pragmatic…".

This approach indicates that the participant perceives risk as embedded in the organisational context.

Security Culture and Non-Compliance

P3 refers to security becoming "*part and parcel*" of "*fictional colleagues'*" day, conceptualising security as something that is an inherent part of the culture that is "*quietly in the background rather than top of mind*". This follows through into the employee's observation of employee security behaviour, suggesting that most people follow the rules:

"it's like that most of people most of the time behave in a way that's security conscious…"

Another theme that emerged from the interview was how Organisation D was trying to build a security culture that encouraged employees to report problems associated with security without fear.

"…create environment where people can say something has happened. People might think it's worth reporting – lots of little things, trying to encourage people tell us about everything – goes back to health & safety you need to know about the little incidents….".

Further, the employee talked about how security messages were being used to improve the security posture and specifically obtain information about security incidents:

"How to encourage? Lots of little messages – survey, sent a note out please help us, might be every 4-6 weeks important to [disseminate] constant underlying message".

They also referred to instances of security non-compliance, suggesting that despite some "*fictional*" staff feeling '*nervous*' about revealing that they had transgressed security rules, most "*fictional colleagues"* would probably feel there were able to express what was happening in relation to security behaviour:

"Non-compliance – still think some people would be nervous about saying stuff – the people that know the most, there's enough of them, it's a culture thing, I would know if there were issues out there – still some individuals, enough people out there who feel safe to do that…".

On the other hand, there are instances of non-compliance noted. For instance, P3 suggested that "*fictional colleagues"* do not always adhere to the Clear Desk Policy and indeed, that it is not enforced:

"Clear desk – something we have need to do better – some people leave things on their desk at night, people work, lots of desks where there's nothing on them, certain individuals will leave stuff. Not enforced – people know it's bad habits, certain things for a long period of time…".

3. Participant 5

AS and RU

The participant was scored positively in respect of the *AS* dimension, suggesting that s/he demonstrated a positive stance towards security. P5 indicates a positive intention throughout the security provision within the organisation, e.g. wanting to introduce a clear desk policy to reduce the paperwork "*strewn around*" in the office environment.

The SIRO cohort demonstrated positive levels of *RU* which is perhaps unsurprising given their job focus is on the evaluation of risks. However, the employee expresses negative sentiment in terms of whether the "*right risks*" are being assessed within the organisation:

"…my concern; are we measuring the right risks, not that the risks we are measuring are incomplete or inadequate – are we looking at the right thing? Intuitively, they've got to be your key worry beads – some of them are, & some of them aren't…"

The visibility of risks is also referred to by P5. For instance, they identify "*front of mind"* risks - such as foreign governments and criminal gangs - but suggest that "*fictional colleagues*" may be less aware of the risks associated with technology, since they are less concrete:

"If someone could pick a lock you can see it, understand, as a non-technical person breaching firewalls is fantasy stuff – how do I know that my protections are adequate? If someone shows you a strong lock you can see that – computer firewall – placing trust in a computer program…".

P5's analogy between a lock and a computer firewall is relevant to understanding how "*fictional colleagues"* may recognise physical security more fully than computer security. Indeed P5 explicitly makes the distinction between "*fictional colleagues'"* understanding of physical security risks and information security risks, highlighting that staff tend to be more aware of the former:

"*People seek security risks – [they are] more aware of physical security rather than cyber security – much of the threat around cyber security implied rather than implicit – phishing & spoofing, dongles passwords – they're more aware of escorting visitors; the physical, tangible physical - ironically that's not* *where the true threat lies – how do you drum it in people that they think about these things?".*

In relation to risk culture, P5 comments that it is "*immature*" and individuals do need to consider risks more frequently:

"The culture of risk in the agency is immature – [this is] one of the things I'm targeting - trying to change risk culture – you should be thinking about risk in your everyday job…"

Further, P5 identifies areas for change in relation to risk management. For instance, they highlight issues such as developing a new risk register which incorporates information security risks that are not fully delineated currently. This demonstrates a positive understanding of cyber risks as well as a generally positive attitude towards security (*AS*).

Security culture and policy

P5 indicates that security is ingrained within the culture because they note that "*fictional colleagues*" do not "*give it a thought*" in that it is behaviour that has become habitual and part of their daily routine at work. Similarly, P5 notes that "*fictional colleagues*" adhere to policy, because it is ingrained in the culture, although they may not be aware of the *specifics* of security policy since it is set by the overall department colleagues:

"We reflect the department's security procedures – we do ***adhere*** *to those [procedures], we don't produce our own policy. Not something most "fictional colleagues" give a great deal of thought to…".*

P5 gives many examples of compliant security behaviour throughout the interview e.g. "*fictional colleagues*" tend to lock computer screens and are aware of physical security risks. Staff do certain email material to their personal accounts but P5 says that security training covers the risks associated with this, such as who may have access to the account so that staff are aware of the consequences of their actions.

SIRO role

P5 refers to what would help them in role as a SIRO in managing risks and suggests that creating more of a community of learning and practice would be of benefit in terms of improving performance. For instance, s/he cites a learning experience within Government with other SIROs, during which they learned more about hacking and exchanged information with knowledgeable colleagues which was useful:

"What would help SIROs? SIRO network meeting across government, I was in a room with another 100 SIROs…a Government Agency did their hacking presentation - that was a really good learning point, panel experts…retired senior bods then talking to people over coffee & round table discussion. I'd go again. Also [I] get a SIRO newsletter – government SIRO he's got a small team within [a Government department]…keep up to date, look at it, read it, look at headlines forward it on to the security chap…".

Control

Related to *RU* is the issue of control in relation security. For instance, P5 discusses how the various government departments may manage security differently, which ultimately means they are not able to mitigate all the risks:

"Programs become more vulnerable, [so we deploy] security patches, maintain version control so maintenance of that really important – [we] don't control all of that. IT in Another Government Department - not under my control, so say [the] virus protection - if that's hit with a hitch I'm vulnerable…".

Security actions - Clarity

One of the other key themes is around managing security risks is lack of clarity in terms of what security actions to take. P5 notes that sometimes there is a sense of not recognising what "*proactive*" actions they should take to mitigate risks:

"Don't know all the issues, controls/access points – password account access to our twitter account, who has the password, how often do we change it? But that's reactive; my concern should I be more proactive? That's my real concern, don't know where to be proactive…".

This sentiment links to the theme around SIRO training, where there is a sense of lack of professional development to help SIROs identify proportionate responses to security risks.

3. Participant 6

AS & RU

All the participants within this Organisation D cohort expressed positive levels of *Affective Security*, suggesting a supportive attitude towards security. Specifically, P6 actively makes suggestions about what interventions or ideas to improve security culture and technical systems, indicating a proactive attitude towards security:

"*What would help? One of the things – security & cyber champions, people out there what would work well messaging wise – who are the risk takers? Could network of people issues are either nipped in the bud early or dealt with swiftly. Work in hand also to improve systems…".*

Nevertheless, this participant expressed lower levels of *Affective Security* than the rest of the cohort, excepting 1 other employee. Therefore, whilst this interview does reflect a positive stance overall, there are some less positive perceptions about security within this transcript. For instance, participant F notes that for many "*fictional colleagues*" security is "*not [at] the forefront of their minds, quite reactive…*". P6 scored positively on *Risk Understanding*, demonstrating competence and awareness of cyber risks. One exemplar of this is the disclosure of information and how it is possible to track "*fictional colleagues"* email logs to mitigate this risk:

"…a lot of people don't realise how much information you can get from email logs & think they can get away with it. We've had info disclosed to the press, with monitoring you can catch people out. Every time you log in to clear the message – reminding people of the Computer Misuse Act – amazing what you pick up through email logs…".

Security Messages

P6's perspective on the SIRO role suggests that there is a need to adjust the security messages for different user groups, understanding the different communities they are required to serve and the related risks. For instance, in this specific interview, P6 refers to the need to tailor security messages appropriately for different countries and agencies:

"…more mindful of the risks, mixture of backgrounds – important for the SIRO to recognise differences, getting the messaging right…".

Regarding the security policy itself, P6 suggests that the language is too jargonised and that it is not accessible to all:

"Security policy – yes they are aware. They don't always understand them, we use too much jargon…Anecdotal evidence is great – people still don't get it – not written with the lay person in mind…".

Evidently, getting the language and tone of the security message right, including the way the policy is written, is a factor in ensuring effective security communication. Also, in relation to security messages, the employee highlights that a loss of an organisational asset, such as a laptop, may be a catalyst to reinforce security communications:

"Getting messages across to them [staff], if someone has lost a laptop – usually the catalyst for communications to go out to people – an incident needs to trigger security interest…".

This implies, however, that security messages are not always disseminated regularly, but may require a prompt. P6 notes that "*fictional colleagues*" may only be mindful of security messages when something goes wrong:

"…issue communication to staff bulletin, glance over bits that affect their security – not in the forefront until things go wrong…".

Safeguarding Assets

Additionally, P6 talks about the specific risks associated with their particular organisation, in particular, how contractors pose a potential risk since they may leave with commercially sensitive information:

"We have international…advisors talk to people about [certain] opportunities – one of the risks is that they could just walk out the door and take the knowledge with [them]…".

P6 refers to the risks associated with hiring someone from the private sector since Organisation D is within the public sector, in that external contractors are not bound by civil servants code:

"…Attract private sector expertise, wealth of knowledge about customers…locally employed staff not bound by civil service code - so we could have issues with local laws, how they protect local employees".

Specifically, P6 refers to the risks of contractors stealing data from the *fictional* department and the implications of such an event:

"Hypothetically – if someone stole info from [the fictional] agency we'd need to take forward a civil prosecution, take through the courts in that country or it could be a law has been broken in that country, so it gets complicated, engage with legal advisors…".

Passwords

Passwords, as with most of the participants throughout this cohort, were highlighted as an issue. P6 suggested that although single-sign on, which clearly requires only one password, is in place internally to access the main system, multiple passwords are required to access systems remotely. This opened up vulnerabilities that lead to "*poor [security] behaviour*" as P6 suggests that "*fictional colleagues"* might feel the need to write down passwords as well as re-using passwords in order to manage the cognitive load.

In addition, P6 also referred to the issue of senior staff sharing passwords with their secretaries and also fictional colleagues sharing passwords as a workaround if IT will not assist them:

"...occasionally people will share passwords to get around what they consider a constraint with the way the system works – some secretaries would have access to their bosses password. Not consistent with policy – known secret – at that level difficult to do anything about it – if the IT doesn't help them work around, people will find a workaround if they haven't got permissions in order to get their job done...".

4. Participant 7

AS & RU

Overall, P7 expressed attitudes that were consistent with being positively on the *Affective Security* dimension. For instance, one of the main themes that runs throughout the interview is the notion of improving security culture and taking responding to incidents. One example, is where the employee describes a leak they and how they need to "*tighten up things*", hence this comment:

"Last year had a leak...someone had printed up the draft board minutes – tightened up the access controls so sys admins, when interrogated knew who it was…These little things remind you to make sure we tighten up things and we investigate it...".

P7 demonstrated *Positive RU* in their awareness of cyber security risks. For instance, in relation to securing defences against incidents and breaches, the P7 demonstrated awareness of the risks. For instance, s/he describes security using the analogy of a burglar who is being restricted in their entry:

"Every time we have an incident – formal escalation of incident… analogy of a burglar; the burglar has gone into the entrance hall, but not into the apartments, there might be something silly a developer hasn't closed a window, changed that so that a 2nd someone [can enter] – layers of defence…".

Similarly, P7 refers to security practices that help mitigate potential information security incidents and thereby manage ongoing risks. For example, they refer to raising an incident if some printed documentation disappears:

"If you print something off that's sensitive – goes missing – raise as an incident. You'd take a risk judgement if not many people are around...".

Risk appetite and risk management

Additionally, P7 refers to the changing risk appetite of the organisation, indicating that it is moving from being a risk-averse climate to one more willing to take risks:

"Risk appetite; quite mature in relation to this, it's changing, there's been a tendency to treat all of our data with equal security, trying to be more granular…tendency to be very risk-averse…very rigid risk appetite – it used to

end up everything saying no – it's easing a bit…we're an operational organisation balancing against screwing things down too tightly".

SIRO role

P7 describes how it is useful to network to improve knowledge and skills in relation to risk management i.e. "*go to the SIRO conference – great networking, talk to other people, make links with them, work with Government Depart...".* Further, the participant highlights the need to share information and be open about mistakes in order to cultivate a culture of learning in relation to security, hence their comment:

"...Two main issues, the world is changing so quickly everyone is learning as much as everyone else, the need to be open rather than concealing things that are going wrong – one of the hardest things is that you know what you need to know…".

P7 goes on to provide an example of where a government minister wanted their department to work on a complaints handling process but was not aware that the data was not adequately secured:

"One incident when a minister wanted us to work on a complaints handling process – security of emails & where it was – identified this isn't secure – you can get caught out – it isn't their day job…".

This anecdotal example demonstrates P7's awareness that colleagues may not have sufficient knowledge of judgement to ensure risks are mitigated within the organisation. P7 recognised that it is important to acknowledge that security is not everyone's main job, or primary focus, and therefore technical security solutions need to be managed effectively.

The employee also suggested that a peer mentoring programme might help support SIRO's in their role, but "*was not happening"* within the organisation at the current time.

Security culture – Security champions

P7 suggests that there are policies and mechanisms in place at Organisation D congruent with security values. They refer to the Clear Desk Policy, for instance, which has evolved to a "*flexible desk policy*" which has resulted in attempts to make sure documentation and other material are not is left on desks. P7 acknowledged that although there were papers on desks, they were "*getting there*" in the process. They also indicated that there was a security champion to foster the process and escalate security incidents if appropriate. This demonstrates that there were organisational interventions directed at embedding new security practices into the culture.

Remote Working

P7 also identifies how "*fictional senior colleagues"* may hold encrypted remote devices such as laptops and blackberries. In the event that "*fictional colleagues"* accidentally leave a device in a given location, s/he is aware that they should tell the support desk to get the data wiped:

"Senior people [have a] blackberry, laptop – work remotely – occasionally get left in the pub, usually go back & find them again, protocols tell IS service desk, they wipe them, data is encrypted...".

Clearly, this remediation is in place in order to mitigate the risks of remote working, reflecting a healthy security culture in this regard.

5. Participant 8

AS & RU

P8 demonstrated a positive stance towards security within Organisation D and this was reflected in a *Positive AS* score. They described "*fictional colleagues"* as being aware of security policy and generally compliant:

"Colleagues – aware of security policy in the org – aware of data handling is the main issue – yes and we do annual refresher training for all staff…hopefully a cultural thing; a secure desk policy, can't leave papers out. Most staff are aware…".

Overall, P8 has demonstrated a *Positive Risk Understanding* score, in line with the rest of the Organisation D cohort. This is perhaps unsurprising since the individuals hold SIRO roles within their organisations. Specifically, P8 refers to general organisational risks which are not only internal to the company but also external factors such as unions and the dissemination of information:

"The biggest risk lies with unions; they have got a political stance, may be privatised, unions ran big campaigns, if they get hold of info they misuse it in some way…".

In addition, P8 refers to other risks such as disaffected "*fictional colleagues"* who may be facing redundancy:

"Generally the risk is disaffected staff – we're downsizing, matter of record – IT staff have asked awkward freedom of information security questions…".

P8 also refers to risks posed by external cyber threats from hackers for instance and are aware of the threat of attacks on the organisational security perimeter:

"1000s of threats a day, 1000s of attacks, mask the IP address, tonnes of attempted sabotages – public constant attack – requests that keep going 1000 requests a second – intelligent hackers of the system to attack your systems….myriad of cyber threats…".

Other vulnerabilities that are mentioned include being connected to unsecured wireless networks and "*the risks that are attached to it*".

SIROs role

The SIRO role the incumbent occupied was only part of their day job and was not their main focus since the individual mentioned their role was more legally oriented. P8 referred to an information management committee which was responsible for managing issues such as data losses and cloud-related issues. P8 suggested this committee was "*pretty good*", that they would like to see more of it and that the committee has supported the goal of helping staff to gain greater awareness of handling information.

Security Culture

P8 suggests that *"fictional colleagues"* at Organisation D tend to follow security policy and are generally compliant partly due to the profile of their fictional employees. Hence their observation:

"Most people follow the general policy rules – the profile of our workforce – average age 50 …the staff are very mature – very aware of the responsibility…highly qualified not into disaffected generally – generally take a pride in their work – explains why we don't employ casuals…".

P8 refers to the fact that technical controls within the Organisation D infrastructure are "*quite tight*" so there have been few security incidents. S/he highlighted, nevertheless, that there are potential risks when contractors work within the organisation. Indeed, P8 indicates there was one leak within the organisation attributed to a contractor but since then there have been contractual clauses in place to manage this:

"Levels of control are quite tight – bit of a worry about the use of shared folders, try and restrict use, risk you've got a contractor in & you've not removed their permissions – but don't have any incidents. Contractor leaked something once – tightened up clauses in contracts – claim for restitution…".

Another act of non-compliance that emerges for this interview, is an example of a "*fictional colleagues"* who emailed data to his personal email simply to allow them to work at home. P8 stresses that this transgression was not malicious in any, instead the result of a conscientious employee prioritising their work in order to get it completed:

"Another guy forwarded data home, curiously an IT guy wanted to work on it at home, it went across a non-secure system – no evidence of misuse, not malice, inadvertence, over conscientiousness – [used] personal email...".

6. Participant 9

This participant refers to the importance of having senior sponsorship or influence as a SIRO to improve attitudes towards security.

"SIRO is something [that] fell to me, I'm on the board…good platform if there are security things that need to be addressed. I'm on an executive committee, make sure they take it seriously wouldn't claim to be an expert on IT side, there to help make sure it's running…and address behaviour...".

They also indicate that more information or training would be helpful as the SIRO instead of assuming the individual already had the requisite knowledge:

"The [more] accessible the better – mix of practical workshop type stuff would be good, it wasn't an induction – a lot of assumed knowledge…".

AS & RU

The employee demonstrates a positive attitude towards security and as such, this interview is coded positively on the *Affective Security* dimension. P9 highlights that security does fit into "*fictional colleagues'*" working day and that security is front of mind:

"Security fits into most people day – the building is security sealed – helpful, puts security in people's mind, to some extent a higher level of security consciousness than in 'Another Government Depart'…".

P9 also highlighted that there had been thefts within Organisation D, but security had improved on this front and "*fictional colleagues*" developed an awareness around not leaving their laptops unattended:

"Had quite a few thefts, people sitting near the main exit their laptop disappeared – even a difference between this floor and the floor below – had to have a bit of floor near the exit.[At this organisation] security got better, you do make sure you don't disappear for 1 hour & leave computer on the desk…".

What is interesting here is that it appears to be the *consequences* of the incident, i.e. the theft of laptops, which is changing security behaviour influencing fictional colleagues to be mindful of their property in this case laptops.

The employee demonstrated awareness of security risks and scored positively on this dimension. For instance, the participant highlighted a security incident, where '*alarm bells'* should have been noted given that the data download occurred at the weekend:

"...there was a big data leak ... country overseas – someone who went in at the weekend, potentially – the most serious issue…should have been alarm bells if someone is downloading data on a Saturday...".

Other examples of *Positive RU* include their view that whilst "*fictional colleagues"* may be aware of the sensitivity of data, there may be a tendency to overestimate levels of sensitivity resulting in restricting data sharing: "*people are over-estimating sensitivity – break that cycle, sharing data*".

However, P9 also highlighted that one of the biggest risks for Organisation D is that which is posed by disgruntled "*fictional colleagues"* who may be affected by organisational restructuring:

"What's the biggest risk for fictional colleagues – in a world where there are 25% - 40% cuts disgruntled staff will go up & those left, lots more to do – malicious threat goes up – the more discontented you get. Inadvertent – time pressure, stress the easier it is to make genuine mistakes…" .

Security Culture and Policy

There is a recurrent theme within this interview that security culture, whilst imperfect, is improving. For instance, P9 notes that people are less likely to send work material to their personal email, although senior employees may not adhere to this:

"Sending docs to personal email – the cultural has got better on it, general assumption (gut feel) senior people may be more likely to email to a personal email – people have got the message you shouldn't be doing [it]...".

In terms of security practices, the participant acknowledges that some fictional colleagues do not always lock their screen, but they are "getting better" suggesting an improved security culture:

"Lock screens; varies, we have got a lot better – do people remember to take their encryption dongle on their computer when they go to lunch? How many computers are open? Some will be open...".

Similarly, P9 highlights that passwords are not being shared: "*at a basic level - passwords – are not being shared or stuff on post-its on their desk*..." and indicates that "*fictional colleagues"* are aware they should not write down their passwords. However, P9 also suggests that there are too many passwords within Organisation D, and that if they do write down passwords they should have it secured in a locked drawer.

Interestingly, P9 refers to the idea that most "*fictional colleagues"* do not know there is actually a security policy within Organisation D, despite suggesting that "*fictional colleagues"* are generally inclined to demonstrate compliant security behaviours:

"Security policy – most fictional colleagues don't think there is a security policy. Probably because there isn't something that brings it all together in a clear way. Not something that's been communicated particularly well…".

Clearly lack of clear communication in relation to security in terms of actionable behaviours is therefore a key theme.

Technical Mechanisms - Improvements

One of the themes in this interview around driving security improvement within Organisation D relates to the updating of technical mechanisms. The interview makes the comment that "*a Government Departments' system is clunky –a lot of people linked to them*" but describes the many improvements made within Organisation D. For instance, P9 refers to Organisation D using less USB sticks to using encrypted mechanisms such as dongles:

"Not using removable media – encrypted dongle comes with storage facility. With the laptops now – less need for the USB sticks…"

S/he also suggests that "*fictional colleagues"* who request encrypted devices will receive one, representing an improvement with IT security:

"The IT infrastructure has got better – everyone who wants one has an encrypted phone & encrypted laptops – the IT takes the need away, and there has been cultural improvement".

P9 also describe how accessing repositories for shared data remotely is much easier using the dongle and token system, facilitating the improvement of security behaviour:

"Shared repositories – and you can access that from your laptops. Plug it in, stick dongle in it & load up, token tap number in it. Used to be a dial up which wasn't as secure, not usable, just what you've got in front. Infrastructure has taken away the risk".

7. Participant 10

AS & RU

P10 acknowledges that there are challenges in terms of the security behaviour within Organisation D, but highlights the changes that are being made to improve security culture:

"Suggested all was not well so my 1st challenge was to assess how poor the overall security arrangements programme of activities – some of them became part of a major investment programme to upgrade IT systems, improve security…".

In a similar vein, P10 also talks about how the organisation is trying to improve security within the organisation, including measuring "*fictional colleagues"* behaviour as well as updating technical mechanisms:

"Fictional colleagues baseline, training programme – shore up information security, getting more up-to-date kit…"

These summaries indicates efforts to diagnose security behaviour and take action to improve security.

In line with the rest of the Organisation D cohort, the *Risk Understanding* dimension within this interview is coded as positively. This is unsurprising as the employee highlights that the SIRO role is focused on risk management and awareness of what levels of risk the organisation is willing to accept:

"SIRO role very much to ensure information risks are being managed…Do I accept the risk – based mostly on what are the controls in place, what [is] the likely impact, balance of the likely impact and the reputation risk?"

The interview clarifies their role as a SIRO which is ensuring the team tasked with managing risks within Organisation D are "good enough" to carry out the task:

"...is that good enough to manage the risk – checking whether people in the org are good at managing the risk. Also have head of assurance services, also have the corporate risk team, legal & compliance & audit team – responsible for the risk being managed...".

Seniority and control

P10 notes that their senior position within Organisation D, in particular the access to the board that they have, allows them to raise the issue of information risks to senior decision-makers.

"Things like, IT stuff developed offshore – levels of authority has to come to me, look at the controls, has it been maintained?...Because I am the Organisation D secretary, I sit on the board, inform the board from these risks, ultimately report[upwards]...[they] takes my advice…".

P10 also talks about the importance of being "*a heavy hitter*" to influence security policy hence their comment that the "*SIRO needs to be a big hitter, for other than being a SIRO, SIRO needs to be someone at board level*". In addition, P10 highlighted being supported as key to enable them or indeed others to be successful in the SIRO role:

"I feel very well supported, I have a mentor, 2 Government Departments – customer relationship manager, brilliant, loaned member of staff, & also internally in the organisation…".

Security behaviour

P10 describes the security behaviour of "*fictional colleagues"* as security compliant stating "*most people try to comply with policies*" although they also note that it "*depends where they work*".

In relation to security policy, P10 refers to the fact that some "*fictional colleagues"* may not be familiar with some aspects of policy. In particular, they suggest that many of the policies are actually new and therefore "*fictional colleagues"* are not necessarily conversant with them:

"53 security policies use of own devices, transfer of data, disclosure updating, some of them existed previously, some of them are new, not familiar. Some people are familiar with some policies, some people who do the data transfer, some of them don't need to know that. Most people are familiar with the policies relevant to their role, 80%....".

Another example of being unaware of policy is that "*fictional colleagues"* are described as using their own devices but not necessarily being aware there was 'bring your own device' (BYOD) policy:

"Bring own device – people don't know what it is, so people are using their own ipads… people are doing it because they don't know…".

However, P10 mentions that "*fictional colleagues"* are provided with training, for example they attend data protection training to help embed security awareness:

"We do data protection training, security training as part of induction – get people thinking that this is quite an asset – see it as that...".

8. Participant 11

The participant describes their SIRO role as something that is closely allied to their day job which is technically focused. This is different from many of the other employees in this cohort who do not hold technically oriented posts. The see themselves as "*someone who understands data & systems, particularly the interaction between internal & external systems & networks. Eyes and ears open for issues relating to that trying to intercept things...*".

AS & RU

This employee demonstrated positive *Affective Security*, in other words, a positive stance towards security and in particular, the user-experience of security within Organisation D. For instance, P11 describes how they attempt to balance the requirement of usability with security in order to make the right trade-off for the users:

"My job has 2 competing interests; security & risk, user needs on the other hand, rolling out office 365 much better for internal users – from any device – usability...".

They also suggest that most "*fictional colleagues"* are aware of policy and are generally compliant hence their comment: *"most people are aware of the content of the policy – compliance with it*". The employee also suggests that if it happens that staff transgress security rules, it is often motivated by a desire to assist customers rather than any sort of maliciousness:

"...people understand or slip into bad habits, try and do something genuinely to help. Customers losing passwords for 1 of our systems, [fictional colleagues] store plain text database so we could look them up so it was helpful to customers. Not malicious but people just trying to help...".

P11 demonstrated an awareness of security risks and subsequently, this interview was rated as positive in relation to the *Risk Understanding* dimension. P11 referred to organisational security risks such as fictional colleagues using devices, suggesting that policy will not always mitigate against risky behaviour:

"What do they perceive as the biggest barrier to safeguarding organisational risks? Easy answer people using devices that is the problem. As many policies as you like people will always do stupid things...".

In terms of their philosophy on security and potential risks, P11 also emphasises the shift from thinking about security in terms of physical boundaries to a much more holistic view. For example, P11 highlights that some people need to be made away that security boundaries can be penetrated that that there may always be "*someone inside your network*":

"A good example – the very old fashioned thinking, we've built a big wall, as long as its big enough everything inside is fine, so the view was; they've come through the security barriers, but its about getting people to understand…there is always someone inside your network"

This demonstrates that an awareness of the risks inherent in perceptions of security within Organisation D staff.

Another example of the P11's awareness of security risks is the recognition that certain job roles such as developers are not focused on security per se, but more creatively focused. This implies that there is a risk around the security aspects of software not being fully considered in the develop process. P11 draws attention to the purpose of the 'security development' role who will work with the developer to ensure security requirement are fully integrated in an attempt to mitigate risks from hackers for instance:

"*Developers – who are working with big data sets – exposing to the outside world their natural mindset is to be creative rather than security focused. Two strands of activity; ethical hacking training, puts them in the shoes of the mindsets & vulnerabilities. Also have [the] security developer role, someone who reviews code, someone acting as a champion, they will do code reviews, work with scrum at different times, big data load into a new database, they'll review the scripts, so it's somebody with a technical mindset – security…".*

Security Behaviour

P11 refers to the fact that many security behaviours are likely to be habitual, and that visual cues can improve security awareness and influence various security behaviours. For instance, s/he refers to the visual impact of the clean desk policy and how it can remind "*fictional colleagues"* to maintain clear desks in line with the policy:

"People need the visual & physical cues to keep the awareness high, more people are in a routine the more habits slip, so hot desking & clean desking, makes it easier to enforce a clean desk policy – really good example of the intervening in people's normal habit, have to consider the security implications of things…".

Passwords

There are, however acts of non-compliance mentioned within the interview which relate to users struggling to remember their numerous passwords. P11 does acknowledge that "*fictional colleagues*" may use lastpass to remember their passwords, however, they note that some may write down their passwords despite the security policy advising against that. Furthermore, they suggest that a minority of "*fictional colleagues"* who may share passwords in order to remember them:

"Passwords - for work they need about 5 passwords, for some users up to 10. How do they remember? They write them down. The policy is you can't write them down. Share passwords – just because of balance of usability. Minority of people who do that…".

Security Training

Another theme that emerged from this interview was the SIRO's perception that security training is not effective for "*fictional colleagues*". They suggest it is not engaging and therefore could be an area of development for Organisation D:

"*Don't think security training is very effective – not very engaging, repetitive it's e-learning, present some info, pictures, here's some more info – how much have you absorbed. Because it's a dry topic – put some effort to make it engaging…*".

APPENDIX 6: SURVEY QUESTIONNAIRE

Questionnaire

This short questionnaire is designed to better understand more about "fictional" staff security behaviour within your organisation. It is not focused on any one person's specific behaviour, but is looking at the *general pattern* of behaviour within the organisation.

Instructions:

Please decide if the statements below broadly represent "fictional" colleagues' security behaviour.

-If you think the statements reflect fictional colleagues' security behaviour rate them as True by putting a T next to that option.

-If you think the statements do not reflect fictional colleagues' security behaviour, rate them as false, but putting an F next to the option.

-If they fall somewhere in between, choose the option (True or False) that you think they most closely resemble.

1. Colleagues generally lock their computer screens, you never know who might be passing by and what they might do with the data.

2. Most people follow the security policy here because they understand the organisation needs to ensure confidential assets are safe.

3. People tend to dispose of paper documents safely, as they are aware of the impact it could have on the organisation's reputation if it got leaked.

4. Everyone needs a pass to enter the building and if they forget their pass, they need a member of staff to verify their identity.

5. The team is completely trustworthy and so occasional password sharing is not a problem.

6. People tend to copy security behaviours from their team as they are unsure of the contents of the official security policy.

7. Most people bend the security policy rules from time to time but it is not an issue because everyone is trusted here.

8. Sometimes colleagues put work data on unencrypted USB sticks if they do not have an encrypted one so they can work from home.

9. Security has never been perceived as a business enabler here, it interferes with your main job.

10. The information systems are difficult to access so employees sometimes have to use someone else's account to log on.

11. There are too many passwords to remember so most people write them all down so they are easily accessible when they need them.

12. The wrong emails sometimes disappear in spam filters, which can be annoying, but people understand the need to screen emails in case they infect their machine.

13. Colleagues often leave work documents on their desks and do not always lock them away when they leave the office.

14. Sometimes staff may use their personal devices to respond quickly to work emails as it is more convenient than using the technology provided by the organisation.

15. People sometimes leave confidential documents on the printer; no one is going to look at them as the team is like a family here.

16. Staff email work documents to their home account, it is simpler and unlikely to cause any real problems.