Unpacking security policy compliance: The motivators and barriers of employees' security behaviors

John M Blythe
PaCT Lab
Department of Psychology
Northumbria University, UK
john.m.blythe@northumbria.ac.uk

Lynne Coventry
PaCT Lab
Department of Psychology
Northumbria University, UK
lynne.coventry@northumbria.ac.uk

Linda Little
PaCT Lab
Department of Psychology
Northumbria University, UK
l.little@northumbria.ac.uk

ABSTRACT

The body of research that focuses on employees' Information Security Policy compliance is problematic as it treats compliance as a single behavior. This study explored the underlying behavioral context of information security in the workplace, exploring how individual and organizational factors influence the interplay of the motivations and barriers of security behaviors. Investigating factors that had previously been explored in security research, 20 employees from two organizations were interviewed and the data was analyzed using framework analysis. The analysis indicated that there were seven themes pertinent to information security: Response Evaluation, Threat Evaluation, Knowledge, Experience, Security Responsibility, Personal and Work Boundaries, and Security Behavior. The findings suggest that these differ by security behavior and by the nature of the behavior (e.g. on- and offline). Conclusions are discussed highlighting barriers to security actions and implications for future research and workplace practice.

1.1 INTRODUCTION

1.2 Employees and Information Security

Recently, attention has been drawn to the accidental disclosure of sensitive information and the role employees play in both its protection and leakage. In the UK, the governance of sensitive data belonging to living individuals is under the jurisdiction of the Data Protection Act (DPA; 1998) and governed by the Information Commissioner's Office (ICO). The ICO can sanction organizations up to £500, 000 for breaching the DPA as the leakage of sensitive data can cause harm and distress to individuals, including reputational and financial damages. The information stored by organizations is not restricted to living individuals as organizations also store information sensitive to their business operation, e.g. their intellectual property. Leakages of this sensitive information can negatively affect businesses' operation and reputation.

Despite the many negative consequences resulting from information disclosure, the prevalence of security breaches is high. For example, the PWC 2014 Information Security Breaches Survey found that 81% of large organizations and 60% of small businesses experienced a security breach in the previous year [1].

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22-24, 2015, Ottawa, Canada.

This survey indicates that breach rate is high but the severity of these breaches is wide-ranging. More severe cases can have repercussions to organizations; for example, in 2011 the Sony PlayStation Network was hacked leaking the personal information of its gamers. Alongside service disruption and damage to Sony's reputation, they were also fined £250, 000 by the ICO [28] for breaching the DPA (1998).

Employees are a mixed blessing when it comes to information security. They act as both a major cause of breaches and as the last line of defense. Research indicates that 46% of data breaches in the UK are due to insider negligence [32] and erroneous behavior when handling information [54]. To protect their organization's systems and data, employees must follow a number of security procedures to counteract security threats. These may include using strong passwords, encryption, anti-malware software and installing software updates. The specific responsibilities will differ by organization and be dictated within the Information Security Policy (ISP). These policies detail security actions employees are expected to take, some of which may be easier to follow than others.

Security procedures such as antivirus updates are now being automated to reduce the burden on employees [24]. However, other procedures such as password design are the direct responsibility of the employee. The degree to which an employee behaves securely may differ depending upon the level of effort required. Required effort is one of the many factors that influence employees' behavior.

A number of theories of behavior have identified different factors that influence behavior. In this paper we will review these factors and identify whether or not there is support for them in the security literature. We then present the findings of a qualitative study investigating these factors in two different research institutions.

1.3 Security Research Paradigms

Previous research into ISP compliance has been largely underpinned using models from behavior change literature to identify influencers of security behavior. These include Protection Motivation Theory, the Theory of Planned Behavior and the Health Belief Model. Studies exploring the validity of such models, which do focus on single behaviors tend to focus on private use of technology rather than workplace use [e.g. 22, 40].

The use of this "compliance paradigm" is criticized for its operationalization of security behavior as a single behavior referred to as 'compliance' [9]. ISPs dictate many different security behaviors (See appendix A for summary of ISP topics

identified). Furthermore, there is little consensus on the content of security policies between organizations. This approach assumes employees' awareness of the content of these policies and finally when questioned about ISP compliance, different people may adopt different frames of reference depending on what is most salient to them at the time. These issues raise concerns about the validity of quantitative, survey research on policy compliance conducted across multiple organizations. Such research is often interested in exploring what motivates compliance behavior, but what influences compliance for one behavior might not influence it with another. For example, self-efficacy might be important to motivate compliance with password behaviors but not important for downloading software updates.

By reducing compliance to a single behavior it therefore limits our understanding of what influences individual security behaviors. Behavior change research acknowledges that motivation of behavior differs by behavior and context [20]. It is important within a work context to explore specific security behaviors rather than focusing solely on compliance with ISPs.

1.4 What influences secure behavior?

Models from behavior change are useful to understand the processes that underpin security behaviors. These can aid the design of interventions to promote secure behavior based upon the strength of the relationships between the theoretical constructs and the security behavior of interest. The two most frequently used theories are the Theory of Planned Behavior (TPB) [e.g. 12, 30], which identifies a link between attitudes and behavior, and Protection Motivation Theory (PMT) [e.g. 25, 33] which is a risk-perception theory exploring an individual's threat and response appraisal and their motivation to protect themselves.

The use of theoretical models facilitates the identification of factors that lead to employees' compliance with their organization's ISP or why consumers engage in a specific security behavior. In this section, the factors that have been consistently explored in research on security in the workplace and in home-users are discussed.

Self-efficacy is *an individual's beliefs about their competence to cope with a task and exercise influence over the events that affect their lives* [5]. In a security context, employees who have high self-efficacy are more likely to follow security procedures, as they are more effective in learning how to follow them and believe they are able to perform the required behavior. Self-efficacy is within many behavior change theories including PMT and social learning theory. Self-efficacy is consistently shown to influence security policy compliance [12, 25, 29, 30, 40, 55]. Furthermore, support has been found for a relationship between self-efficacy and virus protection behaviours [36], using a personal firewall [39], being cautious with emails that have attachments [40], and anti-spyware adoption [22, 37, 51] for consumers.

Social influence *is the extent to which an individual's behavior is influenced by what relevant others (e.g. colleagues) expect him/her to do and the extent to which they believe others are performing the behavior.* In a security context, employees are more likely to behave securely if those around them behave securely and expect such behavior of others. Employees' work environment and the individuals within this environment are therefore important drivers of security actions. The role of social influence is consistently shown to relate to compliance intention [12, 24, 25, 29, 30].

Attitude is *the individual's positive or negative feelings toward engaging in a specified behavior,* in other words towards behaving securely or complying with the ISP. The TPB argues that attitude is a predictor of behavior, alongside subjective norms and perceived behavioral control (a form of self-efficacy) [3]. The notion is that a positive attitude toward behaving securely influences intentions to behave securely. The influence of attitude on compliance intention has been consistently supported [12, 25, 29, 41]. Support has been found for a relationship between attitude and anti-spyware adoption [16], online privacy protective strategies [13, 59] and firewall adoption [35]. This suggests that attitude may be an important antecedent of security behavior.

Research has also explored individuals' threat and response evaluations in the context of security which stems largely from PMT [45]. The theory argues that individuals are motivated to protect themselves based upon their threat and coping appraisal. An individual's threat appraisal assesses the perceived susceptibility to the threat and the severity of the consequences. The coping appraisal is their evaluation of the response to the situation and consists of response efficacy and self-efficacy.

Perceived susceptibility is *an individual's assessment of the probability of events happening to them*. Individuals that have a sense that security attacks are unlikely, may not engage in security practices. On the other hand feeling susceptible to security attacks may result in protective behavior. The role of perceived susceptibility on compliance intention [30, 49] and use of anti-virus software by consumers [36] is supported. The relationship between perceived susceptibility and anti-spyware usage is not always supported [14, 22]. Recent research found perceived susceptibility did not play a role in employees' security breach concerns [25].

Perceived severity is *the assessment of the seriousness of a security threat and its associated consequences*. If an employee perceives a threat to the information resources of their organization to be severe, they are more likely to engage in security actions and adopt secure behaviors [12]. The relationship between perceived severity and secure behavior is not always supported. Support was found for the relationship to information security compliance [25, 49, 55]. However, other research found that perceived severity was not supported, attributing this to differences in the conceptualization of severity in previous studies [30]. The support for a relationship between severity and anti-spyware adoption [14, 22] has been found but its role in being cautious with emails that have attachments [40] and anti-virus protection has remained unsupported [36]. This further highlights that factors do not play the same role in all security behaviors.

Whilst some research [41] supported the role of susceptibility and severity on compliance intention, they combine these constructs so it is difficult to disentangle the effects.

Response efficacy is *the belief in the benefits of the behavior* [45] i.e. that a specific security behavior will reduce security breaches. On the other hand, if an individual has less belief in the efficacy of the behavior, they are less likely to adopt it. Response efficacy, which is part of PMT, has received less attention in research compared to other factors. The research that exists supports the relationship between response efficacy and ISP compliance [30], attitude toward security policies [25] and intention to adopt anti-

spyware software [14, 22, 33]. Recent studies found a negative relationship with ISP compliance [55] or no relationship [49].

Response costs refer to *beliefs about how costly performing the recommended security behavior will be. These costs include money, time, and the effort expended*. If an individual perceives that a considerable cost is associated with a behavior, they will be unlikely to follow through with it. Conversely, if a small cost is incurred, the behavior may be adopted. The compliance budget [8] supports the role of response costs, they found that individuals and organizations place different values on the cost and benefits of different behaviors within ISPs. They argue that an employee's compliance or non-compliance is determined by the perceived costs and benefits of it. Mixed findings are reported in the literature; a negative relationship with ISP compliance has been found [25, 55] whereas other research has found no relationship [30]. Mixed findings are also reported for anti-spyware adoption [14, 22].

Despite the identification of factors that influence security behaviors, there is a lack of research that has explored these factors qualitatively, and how they may be moderated at the individual-level and within the organizational context. In other words, we are interested in what may cause high or low levels of these researched factors in the workplace. Appendix C provides an overview of the literature-driven framework to be explored in the current study.

1.5 Methods in Security Research

Quantitative methods have been primarily adopted in security research such as questionnaire studies that adopt regression models to investigate the degree to which factors influence ISP compliance [e.g. 24, 30], or security behaviors [e.g. 40].

Behavioral intention is seen as most proximate to behavior and is viewed as the best predictor of behavior [56]. Intention is the individual's motivation to undertake the desired behavior. Most existing research explores intention as it's easier to measure (self-reports) than actual behavior (objective measure). With the exception of some studies [58] which obtained objective security data about employees, there is over-reliance on this subjective measure. Research has indicated that intention only accounts for a third of the variance in actual behavior [48]. Research needs to focus on actual behaviors rather than focusing on intention to act.

Qualitative methods have been used to explore security behavior but have received less attention. This research has adopted a number of techniques including one-to-one interviews [4, 8, 53] and diary studies [31]. The lack of adoption of qualitative methods might be due to the potentially intrusive nature of information security research and concerns for business reputation of recruited organizations [34]. These concerns may be heightened due to rises in the number of security breaches in recent years and the imposition of fines on organizations by bodies such as the ICO.

Qualitative studies are useful to explore the motivators of and barriers to information security behaviors. Exploratory and inductive in nature, they aim to generate data pertinent to a research question that is not necessarily confounded by a particular theory or paradigm. However, there has been little research using a deductive approach. Deductive approaches within behavior change literature are quite common. Elicitation studies are one form of a deductive approach. These are useful for ensuring that beliefs and attitudes are data-driven from the population rather than pre-determined by previous research and the research team's preconceptions [18]. They can be used prior to questionnaire development [3, 38]. As the current study is interested in the interplay of factors that are part of these behavior change models for security behaviors, a deductive approach was considered more appropriate as it made space to understand how these factors may differ for different security behaviors and allowed additional themes to emerge that may have not been identified within previous research.

Behavior change models have been used to categorize qualitative data as they allow the exploration of the constructs of the theory with a target group [e.g. 46] and as a framework to analyze existing qualitative data in finance-related security behavior [15]. Apart from some research [15], this approach has remained relatively untapped in the information security domain.

1.6 Research Aims and Research questions

The present study aims to explore what influences secure and insecure practice within the workplace by understanding employees' attitudes, beliefs and security behavior. This study adopts a deductive approach to elicit behavioral determinants which have been previously explored in IS research. The following research questions are to be addressed:

> **RQ[1]**. What are the influencers of employees' secure and insecure behavior and how might they differ across behaviors?
>
> **RQ[2]**. What are the potential barriers to security behaviors?

2. METHOD

2.1 Approach

This study used a semi-structured qualitative approach and employed framework analysis to elicit factors that influence security behaviors through one-to-one interviews. Interviews were chosen over focus groups as the topic of security was deemed sensitive due to its links to employees' job performance.

The vignettes formed the focus for the interviews. 16 vignettes were developed for the current study covering the security behavioral categories identified from a review of ISPs collated from organizations (see appendix A). Vignettes were used as a tool to help engage participants with cyber security discussion in interviews. The nature of this research requires the disclosure of insecure practice and honest discussion from employees, the social desirability of this behavior and because it is directly linked to job performance may mean that this information is difficult to elicit from employees. Vignettes are versatile and can be used for a number of purposes including icebreakers to build rapport with participants, elicit attitudes and beliefs about a topic, and investigate topics that are sensitive to respondents [7]. They have been used for a variety of sensitive issues [26], and with vulnerable groups [6] in research.

Following advice from previous research, the vignettes were designed to remain relatively mundane and avoid unusual events and characters, whilst also appearing realistic [6, 19]. They also provided enough contextual information to enable a clear understanding of the situation but were ambiguous enough to ensure that multiple solutions exist [57]. The vignettes were designed around common security incidents related to the eleven

categories identified from the ISPs (appendix A). Additional vignettes were provided for categories, which had many sub-categories. Common security incidents were identified through security provider's reports (e.g. McAfee, PwC), news reports, and the researcher's knowledge and experience. The vignettes focused upon low expertise behaviors, what research [53] has defined as "naïve mistakes" rather than focusing on malicious behaviors. The wording of vignettes was particularly important to ensure that they did not influence the respondent [57] so we designed the vignettes to avoid the consequences of the character's action (as we were interested in assessing perceived severity). The vignettes therefore remained ambiguous in whether the behavior and situation portrayed was secure or insecure. By avoiding the consequences of the characters action, we would be able to assess participants' perceptions of the consequences. This approach is emphasized in research [47] which argues that vignettes should have unresolved issues and finish at the high of tension in the story. The vignettes were neutral and covered behaviors people may not perceive as insecure but are known to be risky from a security perspective.

2.2 Participants

A purposeful sample of 20 participants was recruited from two organizations from the North East of the UK. We initially only had access to interview 10 participants from organization 2. We had the intention of interviewing more however we found that during data analysis that the same comments were emerging which suggested that interviewing more participants would not have led to further insight. The final sample size was adequate for framework analysis [43] and we were fortunately granted access to external companies, despite the known difficulties of sample access with this research topic in qualitative research [34]. All participants met the following criteria: (1) currently in full time employment, (2) used a computer for work on a daily basis and (3) dealt with sensitive information classified under the DPA or information sensitive to their company's intellectual property.

2.2.1 Organization 1: A University

5 males and 5 females took part, aged 25-49 years (mean 33.5, SD=9.07). Job tenure ranged from 9 months to 15 years with an average of 3.78 (SD=4.25) years. 4 participants had permanent contracts whilst 6 had temporary. All participants used a computer for more than 4 hours daily. Only 1 participant had read the ISP. All participants used personally-owned devices in the workplace and 9 conducted work tasks on their personally-owned devices. 7 participants also stored personal data on their work devices.

2.2.2 Organization 2: Industry Research Group

4 males and 6 females aged between 26-57 years (mean 39.10, SD=10.61). Job tenure ranged from 5 months to 27 years with an average of 11.12 (SD=10.89) years. 8 participants had permanent contracts whilst 2 had temporary. 9 participants used the computer for more than 4 hours daily whilst 1 used the computer for 3-4 hours. 9 participants had read the ISP: 2 had read the policy in the last 1-6 months, 2 had read the policy 6-12 months ago, and 5 in more than 12 months ago. All participants used personally-owned devices in the workplace and 6 conducted work tasks on these. 7 participants stored personal data on their work devices.

2.3 Procedure and Interview Guide

The study received approval from the faculty ethics board. Participants who met the criteria for participation were recruited using internal emails in the participating organizations. Participants were interviewed individually, in a private room at their organization and upon arrival were asked to read an information sheet covering all aspects of the investigation, including the purpose of the study and what they were required to do. They then provided written informed consent. Upon study commencement, participants were first required to complete a demographic questionnaire. They then took part in a semi-structured interview lasting 45-60 minutes. The interview was designed to be semi-structured to allow exploration of the initial framework and key issues and themes pertinent to the research question, while also allowing flexibility to probe unexpected topics raised by the participant [27]. An interview guide (see appendix B) was developed to elicit the behavioral influencers, which have been previously investigated in security research.

Participants were first introduced to a topic area (from the review of ISPs - see appendix A for full list of topic areas covered) in which the researcher provided a short description of the topic to ensure that the broad scope of information security was covered within the interviews. Participants were then presented with a vignette related to individual behaviors from the topic area. The vignettes were used to provide a safe way to open discussion around security for each topic and to encourage honest disclosure from participants. Upon presentation, participants were asked to imagine, drawing on his or her own experience, how they would react in that scenario. Following this, discussion centered on how participants currently behave in the workplace in relation to the ISP areas. At this point, the interview guide was used to elicit behavioral influencers for the behaviors discussed. We were also interested in potential factors that were not covered by the previous research and as such, further discussion for potential factors or reasons for their behavior not covered by the interview guide was encouraged.

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

3. ANALYSIS

The data was transcribed verbatim and analyzed in NVivo 9 using the principles of framework analysis [44]. The five-step procedure was used [52]: (i) the researcher is immersed in the data by transcribing and re-reading transcripts; (ii) identify emergent themes from the data. The current study identified these a priori from previous research, which formed the basis for the initial framework. However, new themes were allowed to emerge that were unaccounted for by the *a priori* framework and allowed the data to dictate the themes [44]. (iii) The data was then indexed in correspondence to the themes within the framework. (iv) Charts are used to arrange the data that was previously indexed in the third stage. The use of charts and maps allowed the data to be classified under headings that relate to the thematic framework. (v) The final stage, mapping and interpretation, involved the development of a schematic diagram from the analysis to guide the interpretation of the data. It was important that in the final stage that any conclusions drawn from the data echoed the underlying attitudes, beliefs and values of the participants [52]. Upon completion, two other researchers conducted a mini-audit of the analysis done by the lead researcher who were given the initial

coding, quotes and identified any emerging themes for stages 2 and 3 of the framework analysis. Upon data completion, the two researchers also checked the final themes and associated quotes.

4. THEMES

Seven themes emerged from the framework analysis of the data. Appendix C provides a visual comparison of the initial and final framework. From the initial framework, self-efficacy, attitude and social pressures were not present however knowledge, experience, personal and work boundaries and security responsibility did emerge from the framework analysis.

Appendix D provides visualizations for each of these themes and Table 1 provides an overview of these themes.

Table 1. Emergent themes from the framework analysis

Theme	Brief description
Response Evaluation	Assessment of security behaviors as characterized by response efficacy, perceived benefits & response costs
Threat Evaluation	Appraisal of the threats to information security as influenced by individual threat models, susceptibility, severity & information sensitivity appraisal
Knowledge	Knowledge of security risks and security actions & the sources that contribute to this
Experience	Previous experience of security including security breaches & work experience
Security Responsibility	Employees perception of who is responsible for security in their workplace
Personal & Work Boundaries	Boundaries between personal & work life
Security Behavior	The actions employees take to ensure information security, categorized as high, medium or low security hygiene

Overall, we found no major differences between participants from each organization. The findings will therefore be discussed together; however any identified differences will be explained.

4.1.1 Response evaluation

Prior to undertaking a security action, employees evaluate the response and its associated outcomes. This is referred to as response evaluation, which is characterized by response efficacy, perceived benefits and response costs.

4.1.1.1 Response costs

Findings suggest that employees make a decision about whether to behave securely based upon an appraisal of the costs associated with the behavior. The major cost is the degree to which it impacts upon job productivity as there appears to be a "productivity threshold" regarding security actions. When the productivity threshold is reached, it can lead to a number of behavioral outcomes. For instance, the employee may circumvent the security process or disregard the security behavior. This was apparent for behaviors relating to information access such as password restrictions on information or accessing documents stored on servers. Furthermore, tasks such as restarting the work computer for security updates were also seen as impacting upon productivity. Employees recognise the disturbance these prompts for restart cause to their workflow and will subsequently postpone the task until a period of low activity or until the end of the working day.

"I will postpone it, postponing security updates happens a lot because they usually time them at really inconvenient times.. it's like well do you want me to do my job?...." (P14, Org2)

This security vs. productivity imbalance is also evident in software acquisition procedures. Organizations often place restrictions on the software employees can install on their work machines, requiring administration rights and authorization for the installation of new software. There were organizational differences in the current study with regards to how the companies mandate software acquisition. The university has a very restrictive policy in which employees do not have administration rights and must seek IT services to approve and install additional software. The industry research group had a less restrictive system allowing employees to freely install software. Both organizations had the option of allowing employees to install authorized licensed software from the company network. However, the lack of installation restriction within the research institution meant that employees did not consider the licensing agreements of certain software and would download software (such as freeware) without consultation. The official procedures for software acquisition were considered "time consuming" and requiring budget approval indicating monetary costs associated with acquiring legitimate software. Employees assumed that they would not gain budget approval and had developed a "don't bother" attitude with regards to official procedures which leads to risky software acquisition.

"because I know it is going to end up as a no anyway I just don't bother with that.. just save yourself the grief and go and get the free thing, that does the job equally well without the hassle.." (P14, Org1)

Correct software acquisition had the largest response cost – reduced productivity as it directly affects employees "*doing their job*". Monetary costs typically referred to the acquisition of software for personal devices (such as purchasing anti-virus).

Cognitive demands were another major cost which occurred as a result of using passwords. Employees have a number of passwords to remember and different password requirements are set for different systems, resulting in high cognitive demand.

"Well passwords.. after many years using computers the passwords just get longer and more complicated to remember, most of them are just randomly generated letters and numbers which can make them hard to remember especially if you.. well especially if you have to change them" (P6, Org1)

Not all security behaviors have response costs, as some actions require minimal time and effort by the user. Specifically the security behaviors of locking the computer, keeping a clear screen and desk policy, and checking physical environments when working in public locations were seen as having minimal costs. Employees identified that although these behaviors have smaller costs, a "habit" was required to ensure they follow through with the action.

".. there is no real effort on my part and I mean ultimately it is CTRL ALT DEL and you have locked your computer and that's all it is.. so it's not exactly an effort from my perspective.. that's probably it.. it doesn't delay me or put a burden on what I am

doing generally.... I would be a little bit more resistant if there was a lot more effort for me to do stuff..." (P14, Org2)

Previous research has mixed findings with regards to response costs and security behaviors [14, 22, 25, 30]. The current study suggests that each security behavior may have a different set of response costs that are not equally as costly as suggested by the ISP compliance paradigm. These differences in response costs for each security behavior may account for the mixed results in the security literature. The findings also support the "compliance budget" which suggests that individuals' choice to comply or not comply is determined by the perceived costs and benefits [8].

4.1.1.2 Perceived benefits

Overall, employees' understood the benefits of security behaviors in terms of protection of information and technology from malicious others, and maintaining confidentiality of data.

"advantages are that you can keep your information secure.. you can be confident that you're taking responsibility" (P2, Org1)

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

"It's like having a burglary, if you leave your door open it's like inviting someone in but if you put extra locks on, it's deterring them so I think the stronger your password is, the more of a deterrent it is to people.." (P8, Org1)

Employees also gain reassurance that their actions are aiding information security and they feel safer in what they are doing.

"I like it (anti-virus) because I think it's important, it gives you an element of security that what you are using is safe… so you don't have to worry as much.." (P18, Org2)

"..well I think having it there, whether its effective or not just makes me feel just a little bit safer.." (P1, Org1)

4.1.1.3 Response efficacy

The findings indicated that employees struggle to evaluate the effectiveness of security actions as they lack awareness and feedback of the result of their behavior.

"I don't know, if you password protected it whether somebody could still access it, I don't know. I guess they probably could" (P4, Org1)

Feedback appears to be playing a major role when employees evaluate the effectiveness of a security behavior. Employees don't receive information about their efforts so they are unaware of the utility of the security action. This indicates an "action-feedback" gap in employees' information security efforts.

"They say that if you don't notice something has gone wrong that is a sign of effectiveness, that's what they say so I am gonna go with I think it is working (anti-virus software)" (P14, Org2)

Furthermore, employees' response efficacy is capped as there was an overall "sense of insecurity" in that they believe hackers or the IT savvy will always be able get access, undermining the effectiveness of their efforts. However, they do perceive their efforts as effective against the average person or criminal.

"I think it's (encryption) effective.. if someone really wants to find out what is on there.. they will find out.. if they are a hacker.. but it's enough to stop.. like if Joe picked it up and put it into his computer and it said you can't read this file because it is password protected or encrypted in some way.. it may be enough to stop him and just hand it and say I have found this.. so again I think it is a good enough deterrent and as I say if someone for whatever reason really wanted what was on that stick.. I am sure they could find ways of cracking the encryption but it is a good enough deterrent for 90% of the population.." (P19, Org2)

Perceived benefits and response efficacy are types of outcome expectancies. Outcome expectancy is present in many of the theories of behavior. An individual's perceived benefit of security behaviors has received little research within security. Research has investigated users' perceived benefits of email security behavior, using the health belief model, on security behavior and supported the relationship [40]. However, this conceptualization refers to a user's perceived effectiveness of the behavior or "response efficacy". Perceived benefits in the current study, refers to individual's estimation of the advantages of engaging in security behaviors which may be distinct from an individual's efficacious perceptions.

At the end of the session, participants were asked to pick three security behaviors that they perceived to be most important for information security. The findings indicated that access control behaviors were perceived to be most important for security (n=19; such as using strong passwords and changing passwords regularly), followed by offline security behaviors (n=9, such as locking computer or using locked cabinets) and an awareness and responsibility of security (n=7, such as personal responsibility and treating information confidentially). Using security software (n=6) and security with removable media (n=4) were also seen as important. Internet (n=3) and email (n=2) security, company procedures (n-2), business continuity practices (n=1) and personal usage (n=1) were less prevalent. The findings indicate that whilst employees struggle to evaluate security actions, they do place more importance on some security behaviors over others, particularly behaviors related to access control.

The role of response efficacy has received little attention in research to date. Previous research has supported the relationship between response efficacy and factors such as intention to comply with security policies [30], attitude toward security policies [25], and intention to adopt anti-spyware software [14, 22, 33]. However, recent research has found contrasting findings [49, 55]. The current study highlights a potential barrier to high response efficacy, as employees cannot evaluate their security efforts as they lack feedback on their performance. However, they did indicate which behaviors they think are most effective for security with those relating to access controls having most perceived utility. Protection motivation theory argues that response efficacy is part of a person's coping appraisal and that higher levels of response efficacy will increase the likelihood of engaging in the behavior. This study suggests that employees do not receive feedback or information regarding security actions and the effectiveness of these actions. Response efficacy may therefore be a potential barrier to security behavior within the workplace.

4.1.2 Threat Evaluation

A number of factors that affect threat appraisal were identified.

4.1.2.1 Information Sensitivity Appraisal

Employees felt that the information they work with has different levels of sensitivity. However, perceptions of low data sensitivity were more prevalent in this sample. Their appraisal seemed to be

based on an assessment of the "value" of the information. This entailed a comparison to data with a perceived higher value such as health-related and financial-related information.

"Again, vulnerable in the respect that I could probably do more but at the same time, I am not sure what other people could do with the stuff that I leave lying around, it's not highly confidential or anything like that... I haven't got peoples' bank details or anything like that.." (P9, Org1)

"I think you have got to think of a better way of giving yourself a reminder than having that exposed especially if it has got patient.. at that level healthcare that's.. you couldn't take any chances with that sort of thing so.." (P12, Org2)

Furthermore, employees' appraisal involved consideration of the information's "audience" and their preconceptions of who can use the data.

"..there is no objective value to this information that somebody has given us.. because to the vast majority of people it means absolutely nothing.. it's pointless and they would not be bothered even if they were found out"(P2, Org1)

These findings support research that found that employee's perceptions of information sensitivity interacted with their perceptions of organizational security [2], rated information about individuals as more sensitive than commercially sensitive information and placed security as a higher priority on some information. This study demonstrates this appraisal through employees' evaluation of the information's value and audience.

4.1.2.2 Susceptibility

Perceptions of susceptibility to security threats appeared to be an important factor in the employees' behavior. The perception varied between employees and the nature of the threat - offline or online.

Offline threats to information and systems involve physical attempts to infiltrate the information security of organizations, which can include the attempts of outsiders or malicious employees. Perceived susceptibility to these kinds of threats appears to be low amongst most employees. Individuals perceive that offline threats will be malicious others acting in a more opportunistic manner rather than pre-meditated. They appear to hold an optimism bias with offline threats, believing they are not at risk of being a victim and comparing the likelihood of a physical threat to other employees or other organizations.

"Yeah the physical security I feel fairly protected.. I would say also because of the likelihood of people who surround me to come and search through my files is just next to zero so yeah I feel very secure" (P3, Org1)

"so in that respect it's probably absolutely safe 99.99% of the time to leave completely personal information all over your computer and leave it unlocked because the majority of people that come into contact with it will not be interested and not want access to it and not want to do anything with it.. so it's only to protect for that minority of times.. for that possibility that somebody might want it and want access to it.." (P2, Org1)

With regards to online threats, the employees perceived themselves to be highly susceptible. There appeared to be an overall sense of insecurity or learned helplessness when it comes to behavior online. This is particularly related to employees' response efficacy. Individuals' have an estimation of the effectiveness of different types of security behaviors and practices, however they feel that *"hackers can still get access*" and the *"IT savvy can still bypass security"*. Employees understand the importance of security behaviors but feel that their efforts can be circumvented regardless.

"I have no idea.. probably they are (passwords) effective if you are going to protect yourself against somebody.. if you wanna kind of see security from the person next to you however in terms of people whose job it is to break passwords.. probably not very effective and I do realize that there are people out there whose vocation is to break peoples' passwords and virus peoples' computers…" (P3, Org1)

"For somebody like me I think your password would be enough to bar me from accessing your information, logging into your computer but I think somebody who had good sound IT knowledge could probably bypass them and get into other peoples' information" (P16, Org2)

The relationship between levels of susceptibility and engagement in security behaviors has mixed support in the literature. Its relationship with ISP compliance intention has consistently been supported [30, 49] as has its role in anti-virus software usage [36]. A potential reason for the lack of support in previous studies is that their conceptualization of threats is often non-specific and they do not refer to types of threat [e.g. 55]. This study demonstrates that an individual's threat assessment differs depending upon an online or offline threat, with online having higher perceived vulnerability amongst employees. Previous studies do not make this distinction when assessing perceptions of susceptibility. Perceived susceptibility to online threats is closely linked with response efficacy, i.e. they do not believe they are protected even if they behave securely.

4.1.2.3 Threat models

Employees appear to have a variety of security threat models. This is dependent on their knowledge of security risks, their perceptions of appropriate security actions and perceived likelihood of threats. For example, there appears to be a large discrepancy in attitudes towards writing down passwords. Some employees perceive this as being highly insecure and would not engage in this behavior, suggesting that they are more concerned with physical threats than online threats in password security.

"I am quite conscious that someone can find a scrap of paper that I have written with important company stuff on so I don't do that.. even for my personal stuff I don't do it" (P11, Org2)

Some employees may perceive this as being insecure but determine the likelihood of an online threat as greater than an offline threat.

"I just have like a note.. well.. I have a note with all passwords for all the different places where I need stuff, like online because there is too many passwords to remember so I need to have them written down somewhere.." (P1, Org1)

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

4.1.2.4 Severity

There was disparity in perceived severity of security breaches and of security non-compliance across different domains. Employees were mainly aware of the consequences to their organization's reputation and the potential implications of this. For example, competitors getting hold of their company's intellectual property and breaching government legislation.

"again other than the competitive threat that we are developing something that we don't want the competition to know about and they get access to that information... you know something like that I guess would be of value to the competition so that they would then have time to put a counter strategy together"(P16, Org2)

Employees were highly aware of the impact to technology from a security breach. This was primarily the consequences of downloading a virus or other malicious software.

"I suppose technically it could affect the whole university system which would cause massive outrage and whatever, so I think you would get into a lot of trouble for doing stuff like that and I think it would have large consequences" (P9, Org1)

Perceptions of personal consequences were mixed; employees were not aware of how their company would react if they caused a breach in security. Employees assumed it might lead to disciplinary action or impact their own and companies' productivity. Employees seemed to consider the consequences to others less although did mention dissatisfied service users and distressed service users.

"I am aware of the kind of potential problems that you could cause, and the stress you could cause people if any information was disclosed about a particular person but I don't know if I did something that caused a problem within the university systems I don't know what action would be taken" (P7, Org1)

Previous research has focused on the role of perceived severity in ISP compliance [25, 49], and anti-spyware adoption [14, 22]. The role of perceived severity on anti-virus adoption [36], being cautious with emails that have attachments [40] and other ISP literature [30] is unclear. Our findings suggest there are different levels to an individual's perceived consequences or perceived severity. These are consequences to the organization, technology, 3rd parties and to the self. Within these levels, knowledge of the consequences also differs with less awareness of consequences to others and to oneself. This suggests that an individual's perceived severity is not one overall construct but may comprise of different types of severity implications. This may account for the differences in existing research.

4.1.3 Experience

Experience related to individuals experiences of security beaches and previous work experience.

4.1.3.1 Security breach experience

The current study suggests that previous experience appears to be important for current behavior. Previous job roles and experiences of security threats (including viruses and phishing emails) appear to promote awareness and secure behavior. An employee's experience of security breaches can lead to different courses of action depending upon their evaluation of an effective response to the breach. Employees' reported "security overreactions" in which they undertake inappropriate continuity behavior or take a "scattergun approach" to dealing with the breach by engaging in multiple behaviors to ensure recovery and continuity (e.g. deleting all contacts and changing all passwords).

"I mean once.. something must have happened to my email address, my yahoo email address because people were just getting emails just saying "try this money making scheme" so as soon as I got that.. I deleted everyone off my contact lists because I had them somewhere else and changed my passwords and things like that.." (P2, Org1)

Other reported "security overreactions" were non-use of accounts and concluding that devices should be thrown out following a virus infection.

"I could see that it is not a right file and I have no idea why I clicked on it and the computer is now very slow and unusable so we are going to be binning it or selling it for parts.. no reason for that and it shouldn't be happening.. and we know that we should never disable the anti-virus" (P3, Org1)

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

"this is not some pen pusher saying don't use pen drives.. It's actually really serious and that was a good lesson for me and I think a lot of people don't understand the importance of things like that but because I have got experience of what happens.. of what could go wrong.. when it goes bad.. when it goes wrong it goes wrong really badly.." (P15, Org2)

4.1.3.2 Work experience

Organizations differ in their approaches to information security and subsequently their methods to promote security awareness and practices amongst employees. This is known as the "security culture" of an organization, which are the shared values and assumptions regarding information security. An organizations' culture is idiosyncratic so there will be differences in the levels of security culture across companies. Employees discussed transfer of their behavior from previous organizations; this appears to be more evident in employees who come from organizations with a higher security culture than their current employer.

"Again from my previous job there was.. it was a very secretive company and there was a lot of examples where there was competitor espionage and things like that.. it was a very regular occurrence and a very serious thing so security was.. it was like Fort Knox over there most of the time so it just got drilled into you to lock your computer work station so that is just something that I brought with me to this job.. I notice that a lot of people don't lock their work stations here" (P11, Org2)

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

"I have had the same password for the last 6 and a half years ... I know I should change that, in my previous employer we got sent a

reminder to change the password,…every three months we had to change our password… I know I should change it but I just don't have the memory space to do that.. I would forget what I had changed it to" (P9, Org1)

Experience has received little investigation in previous research and has largely been supported in terms of anti-spyware usage [51], adoption of online privacy protections [59], and adoption of virus protection behavior [36]. These findings suggest that previous breach experience is important for current behavior. Furthermore, employees' experiences of security in previous jobs are also important and potential transferability of behavior has not been formally explored in employee security behavior.

4.1.4 Security-related knowledge

The theme of security knowledge comprises of sources of knowledge and knowledge of specific domains (i.e. security risks and security actions).

4.1.4.1 Security risks

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

4.1.4.2 Security actions

Employees' knowledge of security actions was also mixed, particularly with regards to those that are formally set in their organizations' ISP. Analysis revealed differences in employees' knowledge of the security policy and its associated procedures between the two recruited companies. Information from the demographic questionnaire indicated that in the academic institution only 1 employee had read the policy compared to the other organization in which 8 had read their companies' policy. Whilst reading the policy does not indicate compliance to it or awareness of the entire content, it does appear to be a source of reference for some employees when determining appropriate security actions. Those who are unaware of their ISPs rely on their own awareness of appropriate security actions when behaving with information and technology. Consequently, they report relying on other sources of knowledge to inform appropriate security actions (such as recommendations from fellow employees).

In terms of security actions, encryption for removable media and work devices was the security action in which employees lacked most awareness of and sometimes there was clear confusion between the differences between encryption and password protection. Other security actions employees appeared to be knowledgeable of were those associated with authenticating users, physical security of information and technology, and the prevention of malicious software. Two-factor verification for account access (e.g. cloud storage) was mentioned less and could be a potential behavior that requires further awareness.

4.1.4.3 Sources of Knowledge

Employees sourced security information from individuals within their workplace or social circle whom they regard as having "IT expertise". In the workplace this was employees from the IT department or colleagues/friends with IT expertise.

".. I think it's pretty good.. I have got windows laptops and I have got a mac and.. I have done research on the different virus software that you can use which is freely available.. I only use the freeware stuff.. and I have asked my friends as well who are quite up on computers and what not and I make sure that I use kind of the same ones that they do.." (P1, Org1)

To a lesser extent, fellow colleagues and line management were sources of knowledge and this most commonly related to the receiving of suspicious emails or files, in which case they would seek information from their immediate peers before contacting "IT expertise" sources. Other sources of knowledge reported were company procedures such as the information security policy or professional codes of conducts, which cover aspects relating to the integrity of information and its security. For example, one employee has to sign non-disclosure agreements (NDA) with service users and this influences her behavior.

"I probably used to leave my computer unlocked more.. but in the job that I do now we have to sign non-disclosure agreements so if you are working with a university on certain things or different companies you have to sign NDAs and there have been some projects which have been deemed as pretty secret I guess so you have to sign them and say that you won't talk to anybody about them.. you won't.. and as part of signing them it says when you leave your desk you must lock your PC.. you will adhere to this and stuff so I am very aware of doing that.." (P19, Org2)

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

"Well.. so far it's not too bad other than there has been a few cases where we have seen.. Facebook or LinkedIn passwords being cracked so the information that I have got on Facebook isn't particularly of interest but of course then when you go into online banking and everything that's when it starts to get a bit scary.." (P17, Org2)

4.1.5 Personal and work boundaries

An important factor influencing secure and insecure behaviors is the degree to which individuals engage in personal activities on their work devices and the boundaries they have between home and the workplace. Those who reported strong boundaries between home and work limit the personal usage they conduct (e.g. using work email for work-use only and limiting personal browsing).

"Well actually when I am at work I just do work and usually the sites and places that I visit on the web are educational resources.. I don't really surf the web and stuff and don't just click on

random links... I just stick to work related things and like I assume those kind of resources are pretty clear" (P12, Org2)

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

"Don't let anyone else use the computer. No one would want to use the computer anyway but I don't let anyone else use it... I don't like leave it in anyone else's care.. it's always kind of, under my own care because it's not my computer to pass around" (P8, Org1)

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

"*Try not use personal devices.. that is as close as it gets.. I just view it as a work one, it's just that I am using it with two different works.. I don't use.. I think it's important in my mind having that line for a couple of reasons.. the information that is coming out of work, I don't want it stored on my home stuff for any trace of it..*" (P4, Org1)

The role of technology in employees' work/life balance is well documented in organizational psychology literature. Ubiquitous access to the workplace can enhance individual productivity but can also inflate individual's stress levels leading to job burnout [42]. A strong work life balance may also be important for security. Limiting working remotely is important for security as it can reduce security risks associated with working outside of the workplace. Individuals with a high work/life balance limit doing work tasks outside of the workplace.

".. once I leave work that is me done but for serious work.. I know for example my boss and other people they have work laptops and they can work from home.. they get special equipment where they can do that.. it's not really applicable to me.." (P14, Org2)

Employees report feelings of high psychological ownership of their personal devices and limit work-related information.

"Yeah I don't even know if it is a security conscious thing.. I think it is more just.. work/life balance of this is my phone.. I don't want to contaminate it with work stuff... yeah it's mine, it's not the company's" (P19, Org2)

Individuals with blurred boundaries between personal and work usage reported being less restrictive in their boundaries and engage in personal tasks on work devices. For example, email usage for work and personal.

"I kind of do receive emails from my friends at work coz they also work here but I don't receive emails from my friends who don't work here on that account but at the same time I also have it set up so that I do receive my Gmail stuff to that computer as well so it sort of kind of blurs the boundaries a little bit" (P6, Org1)

When working remotely these boundaries are more blurred, employees may use work-issued devices for personal usage and allow others to use the work devices.

"I have done it myself if my nieces have been up and there is only one laptop.. like my own personal one and someone wants to do something else then I would give them the work laptop to do it.."(P19, Org2)

Employees reporting less distinctive boundaries between home and the workplace consequently have a lower work/life balance, they prefer ubiquitous access to work information so may use their own personal devices to stay connected to work. These employees also engage in more personal risky tasks on their work machines and disclose their own sensitive information such as discussed by the following employee who uses online banking on their work computer as they rely on the security of their organization and assume that it is more secure than their own devices.

"Because everything on mine (home computer) is what I have put onto it or set up to work on it or adjusted the settings and I don't really understand what I am doing with stuff like that so you assume that because you get an email from IT services periodically that goes to all users that says that we have identified a machine which is running malware on the network and they will give you the work station name of it and you eventually track it down, you assume that because it's a corporate computer system that there is some money and some resource and expertise at keeping it safe.." (P13, Org2)

The use of personal devices in the workplace or BYOD (Bring Your Own Device) can bring many advantages for businesses including enhanced employee productivity, satisfaction and mobility [10]. Despite this, BYOD also leaves organizations open to information breaches. Despite calls for organizations to implement more stringent BYOD security strategies [10], there is little research exploring employee attitudes towards BYOD, the factors that influence this form of behavior and the role of personal device ownership on information security. This study sheds some light on security behaviors and BYOD activities relating to work/life boundaries.

4.1.6 Security responsibility

Employees rely heavily on "security experts" in their company to maintain their systems, particularly for anti-virus, encryption, and installing updates. Employees recognize that it is their responsibility to handle passwords and protect data.

"To be honest I assume that if that's what the company tell us to use then somebody in the technology area has decided that it is secure enough and that our firewalls are there and whatever" (P16, Org2)

Relating to the prevention of viruses and other malicious software, employees appear to rely heavily on their organization with assumptions that "*somebody else is taking care of it*" and relying on the expertise of IT to ensure that they are protected.

"Yeah actually I haven't checked what it is and how it works and whether I should do something about myself or if it's something that just works in the background.. I'm hoping that it's just something that's in the background and then its updated automatically.. I haven't checked so far, I always just assume that's updated centrally from the IT services" (P10, Org1)

In adoption of new security practices, diffusion of responsibility was apparent. Employees would only adopt a new security behavior if the company enforced it, diffusing responsibility to the organization to force them.

"Yeah I would be quite happy to do it if the company came out and said every USB stick that you put in has to be encrypted and yeah I would do it.. again it becomes that another hurdle to get through in the productivity of work but I can understand that reasoning for it.." (P19, Org2)

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

"I have got a mac at home so as far as I know I don't need any security on it.. it has got its own inbuilt" (P12, Org2)

The current study supports the findings of existing research [17] which found that individuals delegate responsibility to one of four modalities: technology, individuals, organizations and institutions. However, its relationship to specific security behaviors in existing quantitative studies has remained relatively unexplored.

4.1.7 Security behavior

Security behavior refers to an employee's ability to engage in appropriate and effective security actions. Three aspects to security behavior were identified and employees categorized accordingly, referred to as "security hygiene", which indicates the effectiveness of the security actions employees undertake. The previous themes affect the degree to which an individual engages in high, medium or low security hygiene. Security hygiene is determined by prevention strategies and security citizenship.

4.1.8 Prevention strategies

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

Employees with high security hygiene take appropriate action and take fewer risks with their security behavior. They rely less on their organization for security and have a more proactive stance towards security. They can also correctly identify whether a physical or cyber security deterrent is most suitable for the security threat. For example, they will adopt encryption on removable media rather than rely on keeping it on oneself.

"Yeah I use a USB stick with encryption and it's just a bit of a reassurance because having in the past, I haven't lost a USB stick but I have not been able to find it for a few hours, dunno where I have put it and so feel a lot more comfortable now where there is using a USB stick with actual encryption on and knowing that if it did disappear then, you know, there wouldn't be staff information going into the wrong hands.." (P4, Org1)

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

"I put them in the filling cabinet but I didn't actually lock it but they were out of sight so I suppose that is as far as I went.. I didn't lock but I do remember going I shouldn't just.. because they are so easy.. it's not like a computer or a laptop that you would be seeing walking out with, the mobile phones were just too easy to pick up so yeah I put them out of sight but I don't think I actually locked them" (P10, Org2)

Employees with low security hygiene, lack awareness of appropriate security actions and engage in inappropriate security behaviors. They rely heavily on "security defaults" such as using the default security password and relying on the computer to auto-lock when leaving their desk. They are more reactive towards security needs and rely on security enforcement by their organization for their security behavior. They lack awareness of appropriate security actions for physical or cyber security threats and as such, they may engage in non-technical deterrents when a cyber-security deterrent would be more beneficial. For example, relying on physically securing a USB rather than using encryption.

"however the advantages are that I am much more consciously aware because 15-20 times a day I need to pick my keys up and I would notice if the USB.. because the USB stick is attached to a.. like a lanyard thing that goes around your neck so if that was missing I would be really consciously aware of it.." (P2, Org1)

Their behaviors are considered more negligent as they may be aware of security actions but fail to perform the behavior.

"I have kind of blurred the lines a bit by having a laptop, it mostly stays at home but when I do take it to work, it's sensible to have a password on but I just don't for ease of access" (P6, Org1)

4.1.8.1 Security citizenship

This refers to actions individuals engage in which aid the organization in business continuity and recovery. Individuals with high security hygiene seemed to engage in practices such as backing up data and informing colleagues of security issues.

"Well.. the phishing thing.. they are all set up.. I don't mess around with them, I just leave it as it is.. if I see anything dodgy I have emailed like IT before and made them aware of it and sent them the email" (P1, Org1)

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

"No.. that's the one thing that I am really a bit confused about, I don't know if there are like official procedures for backing up or if I should do it myself.." (P20, Org2)

5. CONCLUSIONS

Overall seven themes emerged through the use of this deductive approach that explains why employees engage in security actions. The findings of the study suggest that the following relationships between the factors may be present (see appendix C for graphical overview of the initial and final framework). This study suggests that employees' security behaviors are influenced by their security knowledge and prior experience. Prior to carrying out the behavior, employees undergo threat and response evaluations. Knowledge and prior experience also influence these evaluations. Additionally, their perceptions of responsibility and boundaries

between personal and work influence behavior. Finally, the interplay of all these factors influences the degree to which employees engage in security behaviors. This study indicates that there are different levels of security behavior characterized by prevention strategies and security citizenship.

The use of the deductive approach incorporated factors from many behavior change theories which allowed the comparison of the final framework with existing theory. The final framework suggests an extended PMT model with other security-contextual factors that may be able to explain additional variance in behavior if it was to be explored quantitatively and with regression analysis. By exploring these constructs qualitatively, we were able to explore what leads to high or low levels in these constructs and the individual, system and organizational components that may influence different perceptions. In doing this, it has provided better clarity of the use of PMT in security and may explain the disparate findings for a number of PMT constructs (severity and response costs).

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

Secondly, response efficacy was shown to be a potential barrier to some security behaviors, response efficacy is low because employees lack feedback on how effective their security behavior is at reducing threats. Systems rarely provide enough feedback or positive reinforcement to users on their *proactive* security behavior although sometimes provide information on their *reactive* behavior (e.g. weak password or non-updated system). Systems need to provide more feedback on their efforts and provide information on the effectiveness of these for prevention of security threats. Furthermore, employees perceive that their security efforts may be in vain as they don't receive reinforcement from their organization/management to keep up their behavior. Research shows the importance of management feedback on employee performance [23] and the importance of positive reinforcement in shaping behavior [50]. One approach may be for organizations to include security behavior as part of the performance appraisal of employees. As security is part of an employee's job role, it should be given more focus and feedback from the attention of management during day-to-day business operation and more specifically, as part of their employees' performance appraisal.

Thirdly, the current study showed that employees undergo an information sensitivity assessment, evaluating the sensitivity based upon their perceptions of the value of the information and the audience for it. The study highlights differences in individuals' threat evaluation; employees' perceived susceptibility differs depending upon off- and online threats. Within information security research, off- and online threats are often given equal weighting or not specified. However, this study suggests that research needs to consider these as two separate information security issues (on- vs offline) and campaigns need to focus on communicating susceptibility to these threats differently to employees and being specific when framing susceptibility questions. More work is required to provide concrete definitions of sensitivity levels, rather than it being determined in relation to other types of information.

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

The initial deductive framework included the factors social pressures, attitude and self-efficacy however these did not emerge within the final framework. Attitude emerged more broadly across the other constructs rather than as a separate construct. For example, security responsibility and personal/work boundaries have attitudinal components within them. For social pressures, when discussing security behavior, employees didn't appear to be concerned about the behavior of others and of their line management, with regards to their motivations for behaving securely. However, this factor may play more of a larger component within the security culture of both of the organizations. Previous research has explored the role of security culture, which is the shared beliefs, norms, values and learned ways that have developed through the organization's history [11] and are captured in the mission statements and the vision of the organization as they are the values they wish to be known for. A poor security culture is one where security is not built into these shared assumptions and is not part of "*the way things are done around here"*. In the absence of a security culture, individual-level motivational factors may play more of an important role as information security is at the level of the employee rather than driven top-down and across the organization. This may account for the lack of discussion around social pressures in the two participating companies.

Self-efficacy proved difficult to assess within an interview context and this could be due to difficulties in tapping into an individual's perceived capabilities of engaging in security tasks. Self-efficacy may play a latent but difficult to assess role due to impression management in organizations [21]. Employees may wish to maintain the perception that they are competent in their job roles so may not wish to disclose information that may negatively affect these perceptions (i.e. an inability to undertake security actions).

The use of a deductive elicitation approach proved a useful application for exploring the factors that influence security behavior. Refinement of the initial framework through the qualitative data allowed the emergent factors to be driven fully from the data set but also allowed comparison with the behavioral determinants identified *a priori* from the existing literature. Furthermore by using this approach it allowed exploration of theoretical constructs with target populations ensuring that behavioral motivators are data-driven rather than pre-determined by the research. This is important for behavior change as it allows the data from the qualitative interviews to be used for questionnaire and intervention development in future research.

6. REFERENCES

[1] 2014 Information security breaches survey: Full technical report: 2014. *http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml*.

[2] Adams, A. and Sasse, M.A. 1999. Users are not the enemy. *Communications of the ACM*. 42, 12 (1999), 41–46.

[3] Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. 50, 2 (Dec. 1991), 179–211.

[4] Albrechtsen, E. 2007. A qualitative study of users' view on information security. *Computers & Security*. 26, 4 (Jun. 2007), 276–289.

[5] Bandura, A. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*. (1977).

[6] Barter, C. and Renold, E. 2000. "I wanna tell you a story": exploring the application of vignettes in qualitative research with children and young people. *International Journal of Social Research Methodology*. 3, 4 (2000), 307–323.

[7] Barter, C. and Renold, E. 1999. The use of vignettes in qualitative research. *Social research update*. 25, 9 (1999), 1–6.

[8] Beautement, A., Sasse, M. and Wonham, M. 2009. The compliance budget: managing security behaviour in organisations. *In Proceedings of the 2008 workshop on New security paradigms* (2009), 47–58.

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

[10] Bring your own device: Agility through consistent delivery: 2012. *http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf*.

[11] Brown, A. 1998. *Organisational Culture*. Pitman Publishing.

[12] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*. 34, 3 (2010), 523–548.

[13] Burns, S. and Roberts, L. 2013. Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*. 15, 1 (Feb. 2013), 48–64.

[14] Chenoweth, T., Minch, R. and Gattiker, T. 2009. Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences* (2009), 1–10.

[15] Davinson, N. and Sillence, E. 2014. Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*. 72, 2 (Feb. 2014), 154–168.

[16] Dinev, T. and Hu, Q. 2007. The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information System*. 8, 7 (2007), 386–408.

[17] Dourish, P., Grinter, R.E., De La Flor, J.D. and Joseph, M. 2004. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*. 8, 6 (2004), 391–401.

[18] Downs, D.S. and Hausenblas, H.A. 2005. Elicitation studies and the theory of planned behavior: a systematic review of exercise beliefs. *Psychology of Sport and Exercise*. 6, 1 (Jan. 2005), 1–31.

[19] Finch, J. 1987. The vignette technique in survey research. *Sociology*. 21, 1 (1987), 105–114.

[20] Fishbein, M. and Cappella, J. 2006. The role of theory in developing effective health communications. *Journal of Communication*. 56, (2006), 1–17.

[21] Gardner, W. and Martinko, M. 1988. Impression management in organizations. *Journal of management*. 14, 2 (1988), 321–338.

[22] Gurung, A., Luo, X. and Liao, Q. 2009. Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*. 17, 3 (2009), 276–289.

[23] Hackman, J. and Oldham, G. 1976. Motivation through the design of work: Test of a theory. *Organizational Behavior and Human Performance*. 16, 2 (1976), 250–279.

[24] Herath, T. and Rao, H.R. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*. 47, 2 (May 2009), 154–165.

[25] Herath, T. and Rao, H.R. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*. 18, 2 (Apr. 2009), 106–125.

[26] Hughes, R. 1998. Considering the vignette technique and its application to a study of drug injecting and HIV risk and safer behaviour. *Sociology of Health and Illness*. 20, (1998), 381–400.

[27] Hutchinson, S. and Wilson, H.S. 1992. Validity threats in scheduled semistructured research interviews. *Nursing Research*. 41, 2 (1992), 117–119.

[28] ICO 2013. Sony Fined £250, 000 after millions of UK gamers details compromised. *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2013/01/sony-fined-250-000-after-millions-of-uk-gamers-details-compromised/*.

[29] Ifinedo, P. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*. 51, 1 (2014), 69–79.

[30] Ifinedo, P. 2011. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 31, 1 (Nov. 2011), 83–95.

[31] Inglesant, P. and Sasse, M. 2010. The true cost of unusable password policies: password use in the wild. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), 383–392.

[32] Institute, P. 2010. *2009 annual study: UK cost of a data breach. Ponemon Institute*.

[33] Johnston, A.C. and Warkentin, M. 2010. Fear appeals and information security behavior: An empircal study. *MIS Quarterly*. 34, 3 (2010), 549–566.

[34] Kotulic, A.G. and Clark, J.G. 2004. Why there aren't more information security research studies. *Information & Management*. 41, 5 (May 2004), 597–607.

[35] Kumar, N., Mohan, K. and Holowczak, R. 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*. 46, 1 (Dec. 2008), 254–264.

[36] Lee, D., Larose, R. and Rifon, N. 2008. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*. 27, 5 (Sep. 2008), 445–454.

[37] Lee, Y. and Kozar, K. 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*. 45, 2 (2008), 109–119.

[38] Montaño, D.E. and Kasprzyk, D. 2008. Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior and health education: theory, research, and practice*. K. Glanz, B. Rimer, and K. Viswanath, eds. Jossey Bass. 67–96.

[39] Ng, B. and Rahim, M. 2005. A socio-behavioral study of home computer users' intention to practice security. *PACIS 2005 Proceedings* (2005), 234–247.

[40] Ng, B.-Y., Kankanhalli, A. and Xu, Y. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*. 46, 4 (Mar. 2009), 815–825.

[41] Pahnila, S., Siponen, M. and Mahmood, A. 2007. Employees'behavior towards is security policy compliance. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences* (2007), 156b–156b.

[42] Peeters, M., Montgomery, A., Bakker, A. and Schaufeli, W. 2005. Balancing Work and Home: How Job and Home Demands Are Related to Burnout. *International Journal of Stress Management*. 12, 1 (2005), 43–61.

[43] Ritchie, J., Lewis, J. and Elam, G. 2003. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. Sage: London; Thousand Oaks; New Delhi.

[44] Ritchie, J., Spencer, L., Bryman, A. and Burgess, R. 1994. Analysing qualitative data. *London: Routledge*. (1994).

[45] Rogers, R.W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*. 91, (1975), 93–114.

[46] Searle, A., Vedhara, K., Norman, P., Frost, A. and Harrad, R. 2000. Compliance with eye patching in children and its psychosocial effects: a qualitative application of protection motivation theory. *Psychology, Health & Medicine*. 5, 1 (2000), 43–54.

[47] Seguin, C.A. and Ambrosio, A. 2002. Multicultural vignettes for teacher preparation. *Multicultural Perspectives*. 4, 4 (2002), 10–16.

[48] Sheeran, P. 2002. Intention — Behavior Relations : A Conceptual and Empirical Review. *European Review of Social Psychology*. 12, 1 (2002), 1–36.

[49] Siponen, M., Mahmood, M.A. and Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management*. 51, 2 (Dec. 2014), 217–224.

[50] Skinner, B. and Ferster, C. 1997. *Schedules of reinforcement*. Massachusetts: Copley Publishing Group.

[51] Sriramachandramurthy, R., Balasubramanian, S.K. and Hodis, M.A. 2009. Spyware and adware: how do internet users defend themselves? *American Journal of Business*. 24, 2 (2009), 41–52.

[52] Srivastava, A. and Thomson, S. 2009. Framework analysis: a qualitative methodology for applied policy research. *Joaag*. (2009).

[53] Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. 2005. Analysis of end user security behaviors. *Computers & Security*. 24, 2 (Mar. 2005), 124–133.

[54] Thomson, K., Solms, R. von and Louw, L. 2006. Cultivating an organizational information security culture. *Computer Fraud & Security*. (2006).

[55] Vance, A., Siponen, M. and Pahnila, S. 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*. 49, 3-4 (May 2012), 190–198.

[56] Vries, H. de, Dijkstra, M. and Kuhlman, P. 1988. Self-efficacy: the third factor besides attitude and subjective norm as a predictor of behavioural intentions. *Health education research*. (1988).

[57] Wason, K., Polonsky, M. and Hyman, M. 2002. Designing vignette studies in marketing. *Australasian Marketing Journal (AMJ)*. 10, 3 (2002), 41–58.

[58] Workman, M., Bommer, W. and Straub, D. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*. 24, 6 (Sep. 2008), 2799–2816.

[59] Yao, M.Z. and Linz, D.G. 2008. Predicting self-protections of online privacy. *Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society*. 11, 5 (Oct. 2008), 615–7.

7. APPENDICES

7.1 Appendix A- Security behavioral categories and example vignettes

Category	*Description*	*Vignette*
Remote working	Actions for working on mobile devices and in external locations	Miles is a merchandiser for a large menswear store and constantly travels to other stores within the local area. One of the benefits of Miles's job is that he is given a company laptop as he is constantly mobile. Miles has a 15 year old daughter, who he lets use his laptop when he doesn't need it as his laptop is of much better quality than his daughter's PC. Mile's daughter uses the laptop for playing computer games, however she often disables the anti-virus software as it slows down her favorite game.
Removable media	Portable storage devices that can be connected to and removed from a computer (e.g. USB sticks)	Mary works as a Lecturer at the local university, she has an important presentation at a national conference in London, 300 miles away from her home. Due to the long train journey and therefore intermittent internet connection, Mary decides to store her work on a USB stick so that she can continue working on the train from her laptop. The documents stored on the device include assignment results, presentation notes and an excel document listing the names and addresses of the students enrolled on one of her classes. After exiting the train and arriving at the conference location, she realizes that she has lost the USB stick.
User access management	How access controls are allocated and managed e.g. passwords	Matthew is staying late to work on an important assignment which is due the next day, Matthew has limited security access to confidential information stored on a company password-protected server but he requires a certain document to finish this report. Normally, Matthew would have to get authorization from the information owner who accesses the file for Matthew but instead the owner gave Matthew their password to access the server so that he could do it himself.
Prevention of malicious software	Actions to prevent malicious software	The updates for the anti-virus on Laura's work computer are controlled by her organization; however she has to occasionally restart her computer to allow the updates to install. Laura is regularly prompted by the anti-virus software to restart the computer however Laura keeps postponing this task as she is too busy to wait for her computer to restart and for her to re-open the documents she was working on.
Breaches of security	Steps for recovering and reporting security incidences	Chris is about to go on a two weeks holiday from work and on his last day his computer starts acting strangely. For example, the cursor on his computer screen would start to move around on its own and new files would appear on his desktop. Chris only realizes that something peculiar is going on later that day, rather than reporting it to IT, he decides to switch off his computer and deal with the issue on his return.
Physical security	Strategies to physically protect infrastructures, information and information resources	Kimberley works as a secretary in a busy open plan office. Kimberley's work computer has access to a number of highly confidential documents. She is normally stationed at her desk however at lunch she leaves to have her break in the staff room. During this time, Kimberley leaves her computer unlocked.
Information control	Responsibility in protection, storage and processing of information	Lee is disposing of old records which contain sensitive information about clients. His office has two bins for disposing of waste: one for confidential waste and the other for general waste. The confidential waste bin is full so Lee puts the old records in the general waste bin.
Software & Systems	Software and system acquisition, installation and maintenance	Anna requires the latest photo editing software for one of her work tasks, the department has no budget to purchase any new software, however Anna knows a website where she can download an unofficial version of the software. Her work computer allows Anna to download and install it.
Acceptable usage	Appropriate usage of information systems, email and the internet	Beth is a call centre employee and during her work breaks she uses her work computer for personal use. She has just booked a holiday to Tenerife which required her to enter her personal information and credit card details.
Continuity planning	Outlines prevention and recovery from internal and external threats	Michelle's work computer is run by Windows Vista, however she prefers to use her own personal laptop which has Windows 8 installed as its operating system. She brings her laptop into work on a daily basis and does all her work tasks on her laptop. However, Michelle does not back up the data that is stored on her personal laptop.
Compliance with legislation	Compliance to legislation acts such as the Data Protection Act (1998)	Sam is a medical doctor and part of this job role requires him to write notes about patients during his sessions which contain sensitive and personal information that is covered under the DPA (1998). Sam often leaves his notes on his desk in his office. Whilst Sam has an office to himself, other staff such as the cleaners can gain access when required.

7.2 Appendix B: Interview guide

Interview opening:

- Focus of session explained to participant
- Participant provided with an information sheet and informed consent granted from participant
- Emphasize that participants responses will not be shared with their management/company

Participant to complete demographic questionnaire

For each topic area for the policy categories:

- Provide description of category (e.g. for user access management - *Businesses have a number of computer systems to store and process data which employees use. Users have to identify themselves with a user ID and a password to gain access. Employees may have restrictions on their user access to both computer and information*)
- Present participant with vignette
- Ask participant to imagine, drawing on his or her own experience, how they would react in that scenario
- *Optional questions*
    - What advice would you give? / What should they (the character) be doing to protect themselves?

<Researcher to then go back to the topic area>

- Within your workplace, how do you maintain security when/with <topic area>
- Which security behaviors do you perform? / How do you ensure data security?
- What security behaviors do you not perform? / What do you find difficult to do?

For behaviors discussed by participants, the following elicitation questions were used

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

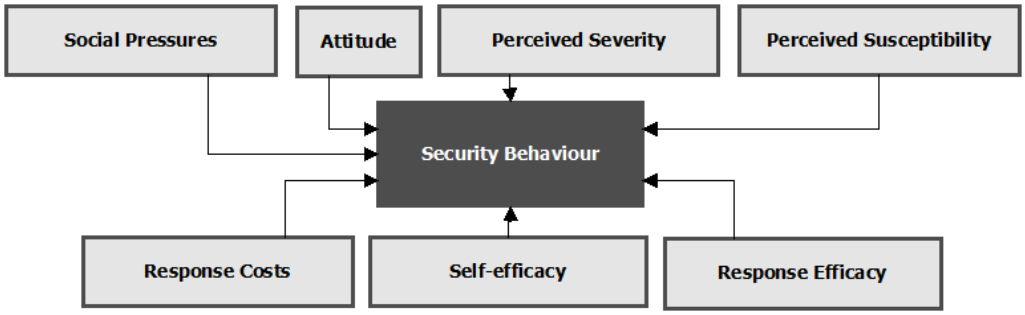
Closing questions

- Anything else that you feel you contribute to security that hasn't been discussed?
- What are the top three security behaviors you think are most important?

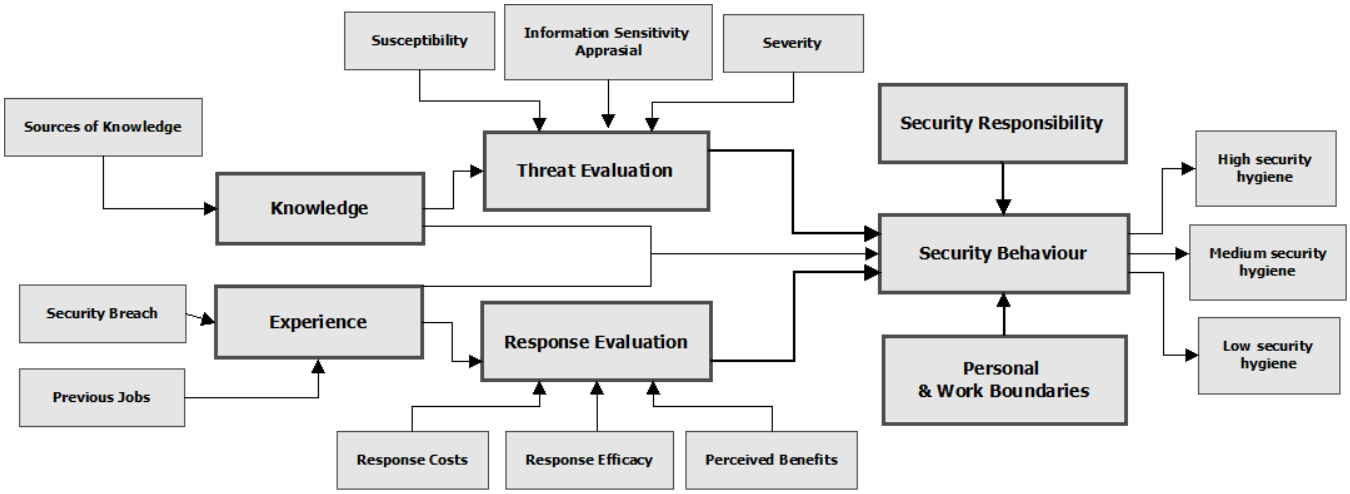
<Participant provided with debrief sheet and thanked for their participation>

7.3 Appendix C: Initial and Final framework

7.3.1 Initial framework based on literature

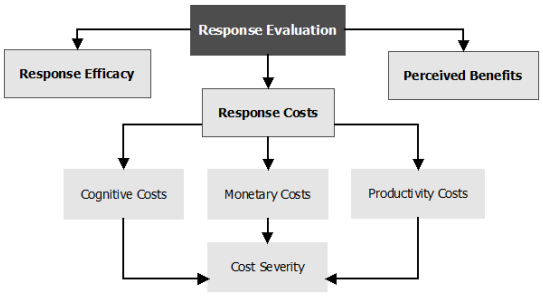


7.3.1.1 Final data-driven framework from framework analysis

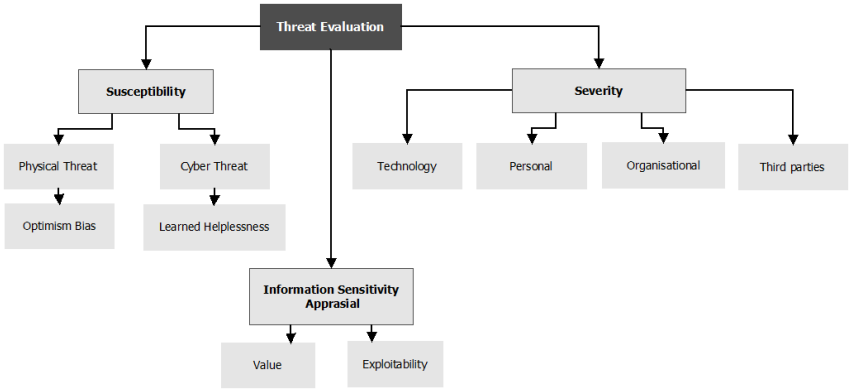


7.4 Appendix D: Theme Visualizations

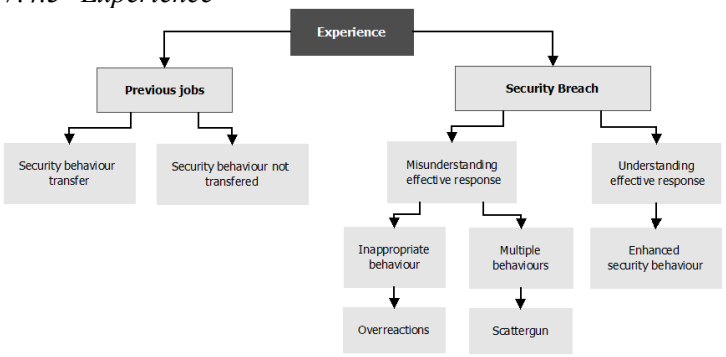
7.4.1 Response Evaluation



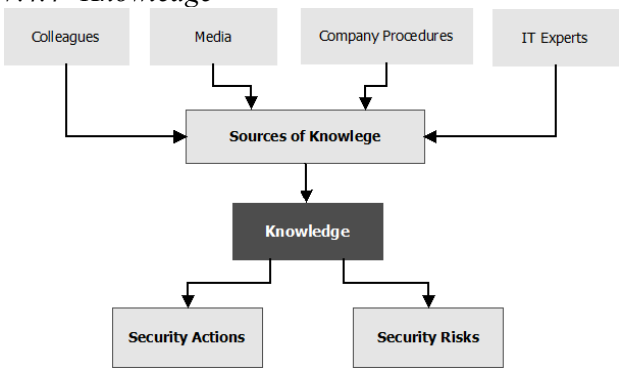
7.4.2 Threat Evaluation



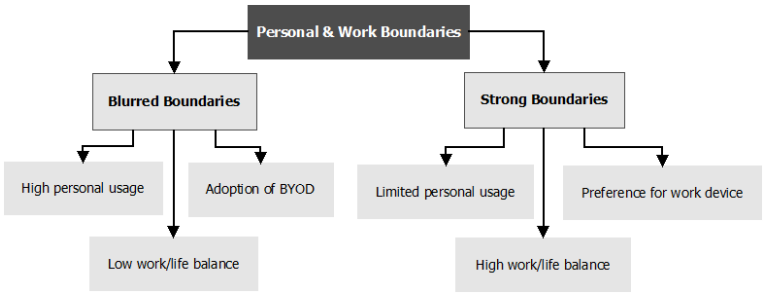
7.4.3 Experience



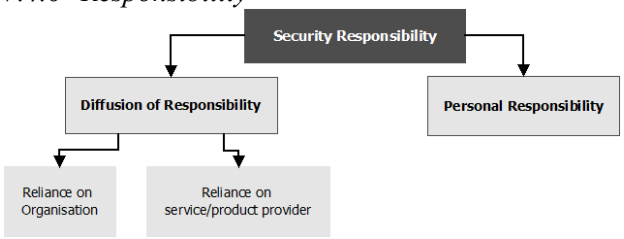
7.4.4 Knowledge



7.4.5 Personal and Work Boundaries



7.4.6 Responsibility



7.4.7 Security behavior