Iiro-Antti Räikkönen

MOTIVATIONS BEHIND EMPLOYEE INFORMATION SECURITY BEHAVIOR

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Räikkönen, Iiro-Antti
Motivations behind employee information security behavior
Jyväskylä: Jyväskylän yliopisto, 2017, 45 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tämän tutkielman tavoitteena oli selvittää mikä motivoi työntekijöitä noudattamaan tai jättämään noudattamatta hyviä tietoturvakäytänteitä. Tavoitteena oli olemassaolevaan kirjallisuuteen pohjustaen, nostaa esiin teemoja liittyen tietoturvakäyttäytymiseen ja löytää selittäviä tekijöitä sekä hyvälle, että huonolle käyttäytymiselle. Tutkimuksen empiirinen osuus toteutettiin laadullisena tutkimuksena, jossa hyödynnettiin teemahaastatteluja. Haastattellut toteutettiin yksilöhaastatteluina ja tulosten analysointi tapahtui aineistolähtöistä teemoittelua hyödyntäen. Tutkimuksen tulokset korostavat erityisesti oppimisen, tietoturvatietoisuuden ja työpaikan kulttuurin merkitystä tietoturvakäyttäytymiseen. Jotta työntekijät saataisiin paremmin huomioimaan tietoturva jokapäiväisessä työssään, on erityisen tärkeää, että he ymmärtävät mitä riskejä tietoturvan huomioimatta jättämiseen liittyy ja mtien he omalla toiminnallaan voivat edesauttaa yrityksen tietoturvan parantamisessa. Tärkeää on myös istuttaa tietoturvallinen ajattelu osaksi organisaation kulttuuria, jotta tietoturva olisi jatkuvasti läsnä jokapäiväisessä työssä eikä vain puheenaihe joka nostetaan esille, kun jotain menee pieleen.

Asiasanat: tieototurva, tietoturvatietoisuus, tietoturvakäyttäytyminen, asenteet, motivaatio

ABSTRACT

Räikkönen, Iiro-Antti
Motivations behind employee information security behavior
Jyväskylä: University of Jyväskylä, 2017, 45 p
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

The objective of this thesis was to find out what motivates employees to comply or fail to comply with good information security practices. Based on earlier literature, the objective was to bring up themes about security behavior, and to find how both good and bad information security can be explained. The empirical part of the research was carried out as a qualitative research utilizing theme interviews. Interviews were conducted as individual interviews and the analysis of the results was done by theme based analysis. The results of the study emphasize in particular the importance of learning, awareness and workplace culture. In order to get employees to better consider information security in their day-to-day work, it is especially important that they understand the risks associated with ignoring it and how they themselves can contribute to improving it. It is also important to implement information security way of thinking into the culture of an organization so that it is constantly present in everyday work and not just a topic that is brought up when something goes wrong.

Keywords: Information security, Information security awareness, Information security behavior, attitudes, motivation

FIGURES

TABLES

CONTENTS

1 Introduction

Information technology is nowadays an essential part of operating a business in almost every field. It is extremely difficult if not impossible to maintain a competitive edge in today's market without utilizing some form of information technology solutions. Data and business processes are also these days considered more and more as strategic and hence there is a need to safeguard them (Subashini & Kavitha , 2011). This is the reason information security should be an essential component for any organization, regardless of its size, location and field of business. Kauppalehti (20.8.2016) reported on the findings of the study done by software company M-Files Oy and AIIM (Association for Information and Image Management) which found that nearly third of organizations lack in their methods to protect critical company data and information. Moreover, in the year 2015 in over third of the companies included in the study, there occurred at least one information security breach. Considering all this it is safe to say that information security cannot be overlooked and every organization needs an information security policy in place to guide people in their daily work.

While technology solutions have their own crucial role to play in protecting organization's assets, it is often the people who are the weakest link in information security. As Chang and Ling (2007) point out, without employees who are committed to doing their part in ensuring that key information assets and systems of the organization are safe, good information security practices are impossible to carry out. Hence it is important to study and try to understand what affects employee information security behavior and how their behavior can be improved.

The purpose of this study is to find out what motivates employee information security compliance in terms of attitudes and consequent behavior. The research questions this study aims to answer are as follows:

- What affects employee information security behavior and compliance with their organization's information security policy and/or guidelines?

- What are the main motivators behind good and bad information security behavior?

First, the key concepts related to information security in organizations are described to generate an overall understanding of the topic. Then the previous research related to the topic is reviewed to see how the topic of information security policy compliance and behavior is approached and discussed in the existing literature and what themes have been brought up. The source material for the literature review was found via Google Scholar and other portals such as EJIS and MISQ. The most used search phrases were *information security compliance, information security management, information security awareness, information security policy* and *information security behavior*. Finally, the empirical part of the study aims to look at employee information security behavior and motivations behind the behavior with the help of theme based interviews.

2 Overview of information security

In this chapter, the key concepts of information security will be described to create an overall understanding of the subject. I will begin the definition of the term itself. Then I will look at the concepts of information security awareness, compliance and information security governance.

2.1 Defining information security

Information security refers to the methods of ensuring that organization's information systems, data and information is safe from malicious use and disruptions (Straub, Goodman & Baskerville, 2008). Whitman and Mattord (2011) define being secure in general as being free from danger, from anything that can cause harm intentionally or unintentionally. They propose that for an organization to be secure, several security layers need to be in place and one of those layers is Information Security. Their definition of Information security is based on the C.I.A triad that is an established standard in the field of computer security. C.I.A stands for Confidentiality, Integrity and Availability of organizational information assets in every context whether it be storing, transmitting or processing information. All the threats that exist and will become in existence in the future will target one of these three key components of information security.

2.2 Information security policy

Information security policy is defined by Höne and Elof (2002) as a document that guides information security inside an organization. It shows the support and commitment that management has towards information security and the role it plays in an organization's overall strategy. It offers the guidelines for organization's employees on how to take into consideration information security in everyday tasks (Bulgurcu, Cavusoglu and Benbasat, 2010; Whitman, 8 2001). Information security policy also defines consequences for instances when information security infractions occur and provides countermeasures to them (Rees, Bandyopadhyay & Spafford, 2003).

There are various information security standards that provide frameworks for organizations related to risk assessment, compliance, regulations etc. These frameworks include standards such as ISO 17799/BS 7799, Control Objectives for Information and Related Technology (COBIT) and Asset and Vulnerability Eval-

uation (OCTAVE). These frameworks are important to organizations that are required to follow certain regulations in their information security practices. (Saint-Germain, 2005.)

2.3 Information security awareness and compliance

Having an information security policy, no matter how comprehensive and effective in theory, is not enough without employees that have a good awareness of information security and motivation to comply with the existing policy. Awareness and compliance in the context of organizational information security will be defined in the following chapters.

2.3.1 Awareness

Information security awareness in general is about user's knowledge and the level of awareness about important aspects of proper information security. Siponen (2000) defines information security awareness as the state of the user of information technology and information assets where he or she is fully informed and aware of the organization's information security policy and guidelines, and ideally, committed to them as well. He also highlights in Siponen (2001) the importance of two characteristics that information security awareness possesses: prescriptive and descriptive. He also highlights the difficulty of internalizing information security policies.

The term prescriptive means that something guides or is used as guidance in one's own actions. In the information security context, this ideally means that the company's information security policy guidelines guide employee actions in an innate manner i.e. they "automatically" refer to those guidelines when using company information technology assets. Descriptive on the other hand is as the term itself suggests, just describing correct actions but not guiding them per se.

With the difficulty of internalization Siponen (2001) refers to the way of thinking about information security as something that is not necessary to be considered often if everything is going as planned and nothing is seemingly wrong. Of course, the problem with this is that the aftermath of an information security incident is usually more costly and difficult to clean up than what it would have been to invest in preventive measures beforehand.

2.3.2 Compliance

Compliance is the most crucial factor in a successful information security policy implementation. After all, it always comes down to having employees who are committed and willing to comply with the policy in place. Good policy and

proper technological solutions are not enough if employees do not behave according to company policies. As stated by Vroom and Von Solms (2004) employees are always the weakest link in information security. Many researchers have tackled the issue of employee compliance and studied the various factors affecting it. These studies have considered, for example, the effects of reward and punishment (Chen, Ramamurthy and Wen, 2012), the roles and responsibilities of the top management and organizational culture (Hu, Dinev, Hart and Cook, 2012). To explain employee behavior, many of these studies have relied on theories from behavioral sciences to help understand the underlying reasons for noncompliance and willingness to comply. These theories include for example, Deterrence Theory, Theory of Planned Behavior and Protection Motivation Theory. These theories have been used as basis for finding explanations and ways to predict employee information security attitude and behavior and ISP compliance. In addition, previous research has also examined the effects of moral reasoning and moral persuasion on employees' compliance with information security procedures (Myyry et al. 2009; Siponen, 2001b). The focus of this research stream has been to examine the effects of moral persuasions on protective information security behaviors.

2.4 Information security governance

Information security governance refers to the role information security has in the executive level of an organization and how it is taken into consideration in the overall strategy of an organization. To successfully protect organization's information assets, information security should have a high priority in the governance strategy of an organization (Posthumus, Von Solms, 2004.) This idea is also supported by Von Solms and Von Solms (2004b) who state negligence of information security in the governance of an organization as one of their ten deadly sins of information security.

A comprehensive definition of Information Security Governance by von Solms (2005), that includes also all the key concepts of information previously described in this paper, summarizes well the key components. The definition goes as follows:

> "Information Security Governance consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained at all times."

Governance includes also the implications for the role management in the implementation and compliance of information security policy.

3 Previous Research

Many perspectives have been used to study and bring to light the factors affecting employee motivation, intention and attitudes to act or not act according to proper information security practices. Theories from different fields such as social and cognitive sciences have been used in the context of information security compliance to help understand employee intentions and motivations. Human mind is not an easy subject to understand and studying why humans act the way they do and what motivates them to comply or not comply with an information security policy is not a simple question to answer comprehensively.

In this chapter, an overview of the previous research that has been done regarding employee information security behavior and compliance with organizational guidelines and policies will be conducted. By reviewing the various approaches taken to study the subject of compliance, this chapter aims to create an overall understanding of what factors seem to be the most benevolent in explaining employee motivations and intentions considering information security policy compliance and overall information security behavior. Many researches have implemented multiple theoretical backgrounds in their papers, deriving from various theories, and thus they will appear multiple times throughout the chapter.

3.1 Theory of Planned Behavior and Rational Choice Theory

Theory of Planned Behavior and Rational Choice theory are widely used and popular theories from social- and cognitive sciences. They have been applied by researchers from various fields to help explain different phenomena. In the TPB an individual's *intention* towards performing a certain behavior is predicted from his or her *beliefs* towards the behavior, *norms* and own *perceived behavioral control* (Ajzen, 1985). RCT on the other hand sees individuals making choices between different options based on their preferences and choosing an option with the best-perceived net benefit (Scott, 2000).

Bulgurcu et.al. (2010) used Theory of Planned behavior and Rational Choice Theory as a basis for studying employee intensions to comply with ISP. The study was conducted as a survey that tested the significance of many various measurement items (i.e. rewards, costs, self-efficacy etc.) They tested several hypotheses and created a model for Antecedents of Information Security compliance of employees based on the Theory of Planned Behavior and elements of Rational Choice Theory (Figure 1).

Their study yielded several significant observations. Firstly, they discovered that attitude, self-efficacy and normative beliefs play a key role in employee compliance with ISP. Attitude towards compliance with ISP refers to how an employee values the compliance behavior. As in does the employee perceive it as something of value and worth the effort? Self-efficacy is about employee's beliefs

about his or her own capability to comply with the ISP. If an employee feels that he has the necessary skills and knowhow to comply with the ISP, more likely he is to comply with it. Finally, normative beliefs are beliefs affected by peers, managers etc. and the extent that their attitudes and expectations affect an individual's own behavior.

Outcome beliefs like benefits of compliance and costs of compliance and noncompliance and their overall assessment were also found to be significant drivers affecting employee attitudes and intention to comply with ISP. Benefits can be innate in nature such as satisfaction, positive feelings coming from complying with ISP and they help people justify their own behavior. Cost of compliance refers to beliefs an employee has regarding possible negative consequences that compliance with ISP might lead to, such as impeding (complicating) daily work. Cost of noncompliance can also, in addition to sanctions, refer to innate costs such as guilty conscience from neglecting ISP.

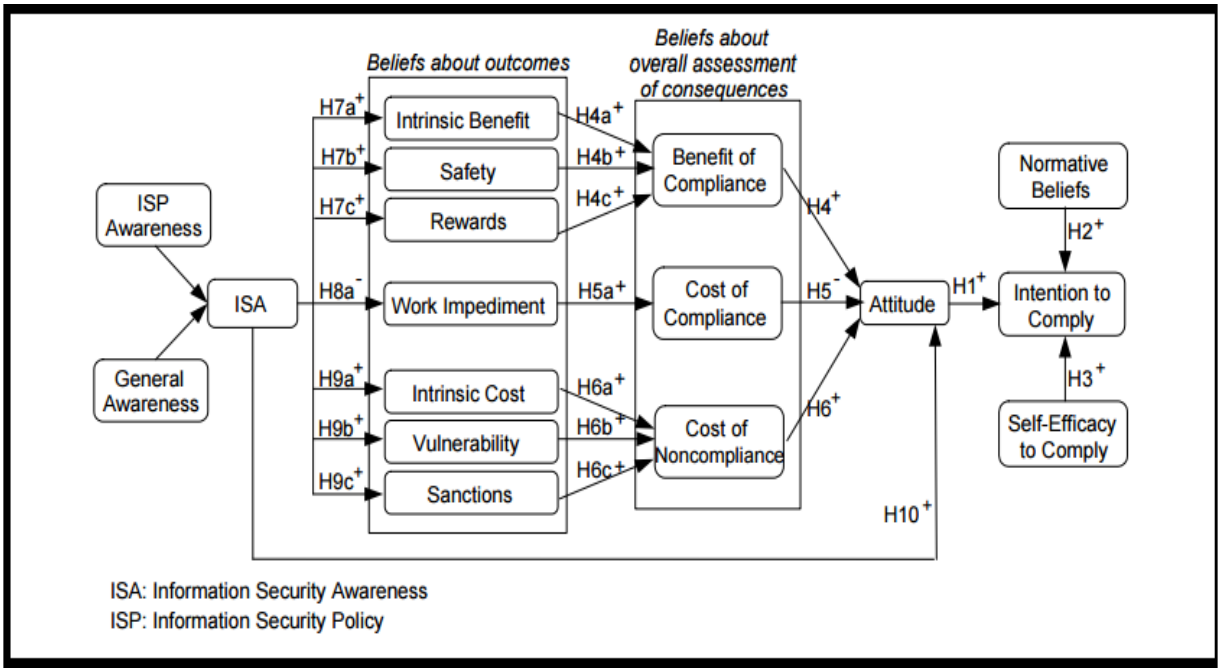

Figure 1 Model of Antecedents of Information Security Compliance by Bulgurcu et.al. (2010)

Ifinedo (2012) conducted a field survey and the results were quite similar compared to Bulgurcu et.al. (2010) in that attitude, self-efficacy and subjective norms all played a key role in compliance behavior towards ISP. In addition to the theory of planned behavior, Ifinedo (2012) also applied protection motivation theory to create a more comprehensive understanding of employee compliance motivations and behavior. Protection motivation theory will be covered more extensively later on.

Supporting the findings regarding elements of rational choice theory Li, Zhang, and Sarathy (2010) found that perceived costs and benefits affect compliance intentions significantly. If for example perceived benefits from violating company policy outweigh the perceived costs, individual might be more likely to engage in negative behavior. The authors also argued that subjective norms might have a more significant effect on an individual's behavioral intentions when he or she has little experience and knowledge regarding company policies. In other words, when knowledge and experience increases, the role of social influence decreases. This once again highlights the importance of educating employees on the key aspects of information security policy and why it is important to follow it. Although the paper focused on policy regarding internet usage, it is safe to say that the results can be applied to a more comprehensive information security policy as well. Vance & Siponen (2012) also applied rational choice theory in their research model and used hypothetical scenario model to extract useful information out of participants regarding their information security behavior. Their findings support the findings of Sarathy (2010), Ifinedo (2012) and Bulgurcu et.al. (2010) in terms of the significance of *perceived benefits* in guiding an individual's behavior. Their findings also indicate that *moral beliefs*, as in what a person considers right or wrong in terms of their actions, significantly guide an individual's intentions to comply with information security policy.

Ifinedo (2014) applied the theory of planned behavior together with the social bond theory and used a field study method to survey business managers and professionals. The study found that social relationships formed within the organization have an effect on employee compliance behavioral intensions regarding ISP compliance. Attitudes and behaviors are influenced by those around us and thus this also has an effect on how compliance behavior regarding ISP and information security overall is perceived. For example, if one's peers view ISP as a hindrance to work and do not take it seriously, this may guide an employee to imitate that type of behavior. This highlights the importance of nurturing a social environment where through socialization employees can learn and internalize organizational values.

Trying to predict and explain employee compliance or noncompliance behavior is certainly quite a complex matter with a lot of different variables, both internal and external. Employees' own values and beliefs affect their attitude and intensions to comply with information security policy and those beliefs and values can in turn be affected by those of peers. However, it does seem that proper knowledge and awareness of information security related issues can help to change attitude and behavior and decrease the effect of normative beliefs.

3.2 Role of fear and punishment

A myriad of literature has studied the effects of fear and punishment has towards human behavior. From criminology to politics, the topic has been an interest in academics several decades. These themes are also extremely relevant when studying the motivations of employees in the context of information security policy compliance and behavior. What follows is an overview of various studies that have, in one way or another, studied the role of fear and/or punishment in the information security context.

3.2.1 Protection Motivation Theory

Protection Motivation Theory is a theory proposed by Ronald W. Rogers in 1975 that sheds light on the role fear appeals in people's behavior and also provides insights into the role of persuasive communication as well. The core of the theory includes four components related to how people perceive threats: perceived probability, perceived severity, perceived self-efficacy and the perceived effectiveness of a suggested prevention behavior (Maddux and Rogers, 1983). In protection motivation theory, the idea is, that if communication invokes fear in a recipient, he or she seeks to alleviate that feeling one way or another. If the communication also suggests that certain behavior will ease the fear, and it does so, then this type of behavior is reinforced and is more likely to occur again in the future. In cases where the suggested behavior does not alleviate the fear, an individual might result to maladaptive reactions to cope with the situation. These reactions might be for example avoidance of the source of fear (the message) and denial of the threat altogether. (Boer & Seydel, 1996.)

Vance, Siponen and Pahnila (2012) applied Protection Motivation Theory together with a theory of habit to form a model and gain insights on employee compliance behavior (Figure 2). The research was conducted as a survey and the data was collected from a single Finnish municipal company. This of course was addressed as one of the limitations of the study but was deemed necessary since the hypothetical scenario method used needed to be relevant and realistic to that particular organization.

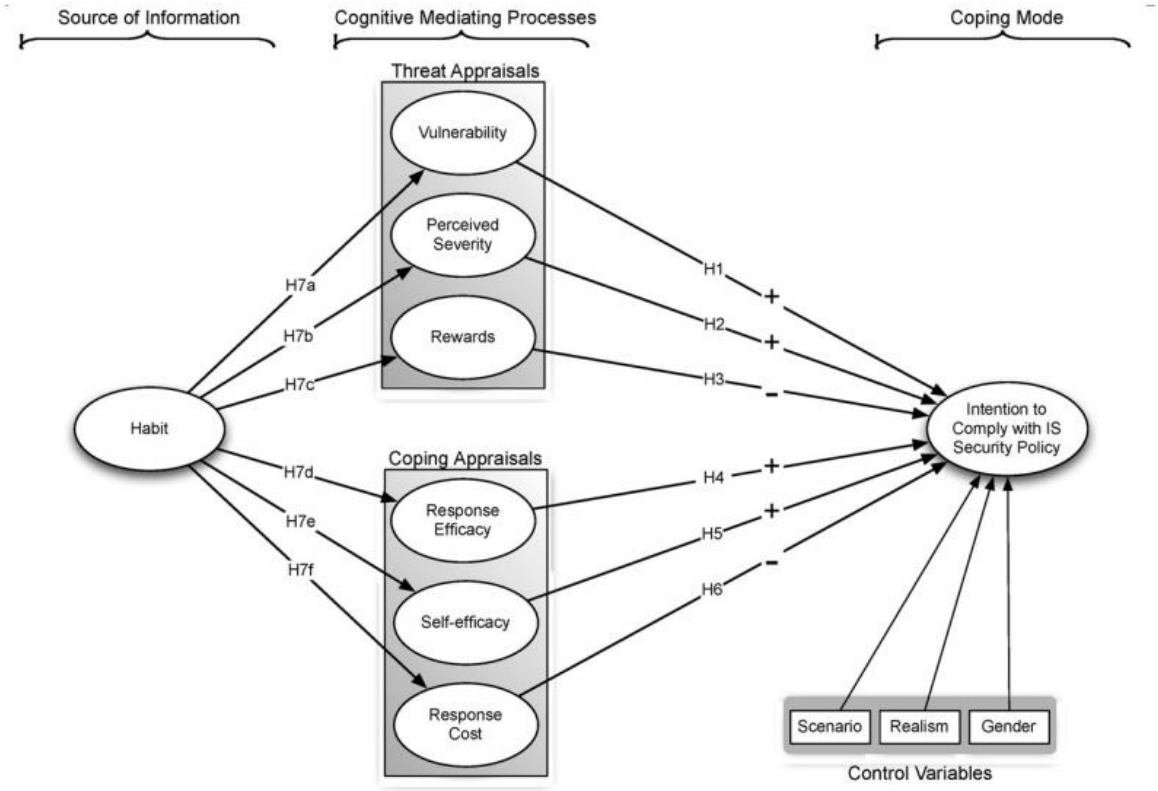

Figure 2 Research model integrating PMT and habit theory by Vance et.al. (2012)

The most important implications of the study have to do with perceived severity of information security threats and the presentation of ISP. If employees do not fully understand information security threats and realize their severe consequences for the organization, it negatively affects their compliance behavior. On the other hand, there are also contrary findings: Ifinedo (2012) found that perceived severity of the consequences to the organization that may occur, after an information security breach, did not positively influence an individual's compliance behavior. The paper did however address, that this might be caused by contextual factors or influences that are irrelevant to the topic at hand. Regardless, better employee awareness and understanding of security threats is one key solution to solving this problem. In regard to the presentation of ISP, Vance et.al. (2012) argued, it is important to communicate ISP in a manner that does not create a mindset of perceiving ISP compliance as an unnecessary hindrance to daily work.

Herath and Rao (2009a) had similar results regarding the importance of understanding the nature of information security threats and additionally brought up the importance of employees perceiving their own actions as positively benefitting the company. When own actions of complying with the ISP by following proper information security behavior guidelines are seen as meaningful and actually being beneficial to the company, more likely this behavior is to occur.

Workman, Bommer and Straub (2008) applied protection motivation theory to try and account for the gap between knowledge in organizations about information security threats and actually acting on that knowledge. They came up

with a model called threat control model (TCM) that consists of elements related to assessments of coping and threat. Coping assessment includes internal and external resources and factors that can help avoid a threat and threat assessment is about how people perceive threats, for instance, in terms of their severity and probability and motivations that help manage the feelings and take action to alleviate them. As can be expected, the study found that the more severe the threat is perceived as, more motivated individuals are to try and avoid it from materializing. The authors also point out that this works both ways and it can lead to neglecting possible threats when too many possible threats are constantly brought up and warned against or the presence of fear is constant in the organization. The motivation to cope with the threat was also indicated to be dependent on the level employees' self-efficacy (as was also previously evident in Bulgurcu et.al. 2010). The importance of self-efficacy was also highlighted by Herath and Rao (2009a). They brought up the role of management (discussed in more detail later) in providing employees with resources regarding information security to enhance their knowledge which in turn increases their self-efficacy. If people feel that they have the ability to respond accordingly to the threat, they are more likely to do so.

3.2.2 Agency Theory and Theory of Deterrence

Agency Theory concerns the relationship between a principal and an agent and the problems that arise from this agency relationship. In this relationship, the principal has delegated work to an agent and the first problem arises when there exists a conflict between the goals of the principal and the agent. In a principal-agent relationship, it is difficult and costly for the principal to confirm what the agent is actually doing. Secondly, there is a problem of different perspectives when it comes to taking risks. The principal might have a stance of avoiding significant risks and the agent may be more inclined towards risk taking. This may lead to actions that are in contradiction with the goals of the principle. (Eisenhardt, 1989.) Agency theory in an information security context concerns the relationship between management and employees where the responsibility to adhere to the organization's ISP is on the employee's side. Thus, employees can choose to either follow or not follow the ISP.

Theory of deterrence concerns the deterrent effect that a threat of consequences in varying degrees of severity have on people and the underlining psychological processes that take place before an individual engages in a criminal or malicious act and how that type of behavior can be deterred (Williams and Hawkings, 1989, 546-547) In the context of information security, deterrence theory has been used to study and explain how the threat of punishment affects employee intension to comply with ISP guidelines. The general expectation in the Theory of Deterrence is, that as the perceived likelihood and austerity of the punishment increases, unwanted/illegal behavior abates.

Herath and Rao (2009b) applied agency theory and elements of deterrence theory in the context of information security to study the motivators, both intrinsic and

extrinsic, affecting the compliance of information security policies. Intrinsic motivations regard to the needs that are satisfied by performing tasks (the task itself satisfies a need) whereas extrinsic motivations such as monetary compensations are the main goal and performing tasks at work are an instrument to achieve that goal (Frey and Osterloh, 2001. 8) The study brings up the principal's (management) role in motivating the agents (employees) with both, explicit and implicit, incentives. The study found that both, intrinsic and extrinsic motivators have an effect on the employee intensions to follow company's information security policies. The intrinsic motivations were observed to be affected in terms of whether or not the employee perceived that complying with the information security policy in their everyday work and actions has a positive effect on the organization. If the view is positive, then the complying behavior is more likely to occur and vice versa. This once again indicates that in order to get employees to comply with ISP there needs to be an understanding of the importance and the benefits that it has for the organization as a whole. Effective communication flowing in both directions and educating employees could be the solution to this.

Additionally, Herath and Rao (2009b) found that social aspects also influence the compliance behavior. These aspects include the perceived expectations and behavior of others (peers, management etc.) in the organization. When perceived that others, including management and superiors, are committed to following the guidelines set by the ISP, it reinforces the positive attitude towards complying.

In contrast to what might be considered effective among managers in various organizations, the study found that having severe consequences for information security violations can affect compliance behavior negatively. Instead of severe punishment, the likelihood of getting caught violating ISP seemed to exert a more positive influence on intention to comply. Siponen and Vance (2012) had similar results regarding sanctions in that *formal sanctions* seemed to be ineffective in deterring employees from engaging in violations of ISP. However, they highlighted the importance of formal sanctions in that they are needed to clearly define the consequences of information security policy violations.

Chen et.al. (2012) studied both, the effects of rewards and punishment on compliance behavior and their results show support for the findings of Herath and Rao (2009b) in that severe punishment alone does not effectively deter people from engaging in actions that violate an organizations' ISP. Their study also indicated that having either low or high rewards for compliance has little difference if at the same time there exists a policy of severe punishment. Instead, the effect of rewards was indicative of being stronger in the presence of milder punishment. Additionally, the findings indicated that the probability of the organization's enforcement strategy being actually and rapidly implemented in cases of violation, had a significant effect on compliance behavior. Interestingly, Cheng et.al. (2013) had contrasting results: They found that the perceived severity of penalties indeed did significantly affect the compliance behavior and the certainty of the punishment seemingly had no significant effect. These differences could be explained by selected research methods (scenario studies were used by

Cheng et.al. (2013) and Chen et.al. (2012) and survey method was applied by Herath and Rao (2009b), and different layout of questions and varying contexts. Regardless, all studies offer interesting practical implications to consider when trying to understand employee motivations to comply with information security policy.

3.2.3 Neutralization theory

In addition to just utilizing the deterrence theory, Siponen and Vance (2010) looked at employee security policy violations through the lens of neutralization theory as well. Neutralization theory originates from criminology and was first described by Sykes and Matza (1957) and has since been further developed and applied in various contexts. Neutralization theory, in a nutshell, concerns the methods by which individuals rationalize illicit behavior and "turn off" certain values in order to commit these actions. The original theory described five different methods that individuals use to justify their actions and Siponen and Vance (2010) incorporated four of these: denial of responsibility, denial of injury, appeal to higher loyalties and condemnation of the condemners. Additionally, they incorporated defense of necessity and the metaphor of the ledger that have been added to the theory later on.

Denial of responsibility is when an individual denies responsibility of his actions and sees himself as powerless to have acted in another manner (Sykes and Matza, 1957). One can for example deny of having knowledge that his actions violated the company policy.

Denial of injury refers to rationalizing one's own actions as being harmless and not causing any damage (Sykes and Matza, 1957) People often use this rationalization when nothing severe happens in consequence of their actions, as in no harm, no foul. This type of thinking is of course severely flawed and can be seen as eventually leading to a situation where these types of actions do cause significant damage.

Appeal to higher loyalties is a method applied when an individual justifies his actions as necessary to get out of a problematic situation (Sykes and Matza, 1957). The actions may also be justified as benefitting the greater good in the long term (Siegel, 2005).

Condemnation of the condemners is a method of justifying actions by arguing that the laws prohibiting the action are not reasonable (Sykes and Matza, 1957). In relation to information security policies, an employee could argue that certain rules are counterproductive and a hindrance to work and use this as justification to breaking them.

Defense of necessity is a bit similar to appealing to higher loyalties in that it too is about individual justifying that there was no other course of action to take. Moreover, it reliefs an individual of any guilt when the action is perceived as necessary. (Minor, 1981.)

Metaphor of the ledger refers to a way of thinking where previous good deeds are seen as outweighing the bad. An individual may think that he or she has done enough good acts in the past so that a single bad one is justified. (Klockars, 1974.)

Siponen and Vance (2010) found that neutralization theory does indeed help in predicting employee intensions to violate information security policy and that when accounting for the effects of neutralization, the effect of informal sanctions seems to be insignificant. Additionally, they suggested that formal sanctions are not an effective predictor of violations regarding information security policy. They offered a possible explanation for this being the nature of neutralization techniques as enabling individuals to justify their actions without compromising their values that go against these actions. This finding is in line with the previously mentioned Siponen and Vance (2012) study.

3.3 Management and organizational culture

The organizational culture that consists of values and beliefs held and shared by the people in the organization has a significant effect on the way employees behave and perceive things in their daily work life- including information security. The relationship of culture and security policies is brought up by Von Solms and Von Solms (2004a) who highlight the importance of making organization's security policies part of the organizational culture. The management of the organization, on the other hand, can have a significant impact on the prevailing culture of the organization and hence they go hand in hand when discussing employee attitudes towards information security policies (Hu et.al. 2012).

Management is also one of the most researched topics in the context business, and for a good reason, since management of an organization plays a key role in a success of a company in many ways. Their leadership and managerial skills reflect on the employee performance and thus for the performance of a company as a whole. More often than not, behind a motivated and highly performing employee who abides with company policies and practices is a management that does exactly the same. Kouzes and Posner (2006) highlight the importance of acting in accordance to one's own values and behaving according to the saying "practice what you preach". They also bring up the factors of enabling employees and recognizing good work. These aforementioned factors can certainly be applied to managing employee compliance with information security policy as well. Taking the security measures and practices outlined in the company policy seriously and abiding by them in the daily work starts from the example of management.

Hu et.al. (2012) studied both, the organizational culture and the role of top management and their relationship with employee ISP compliance. As with many studies before, their study also implemented the Theory of Planned Behavior in explaining how top management and organizational culture affects the employee perceived behavioral control, attitude towards behavior and subjective

norms. In terms of organizational culture, Hu et.al. (2012) focused on the perspective of value. Their conceptual model, shown below (Figure 3), shows the relationships between management, culture, individual beliefs and employee intensions to comply with ISP.

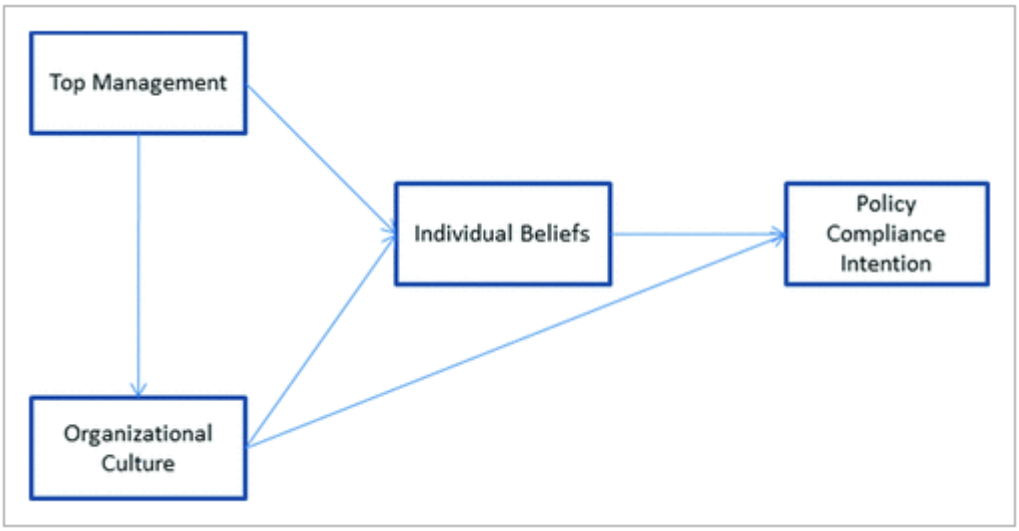

Figure 3 Behavior of individuals in organizations, conceptual model by Hu et.al. (2012)

Hu et.al. (2012) conducted a survey study and found support for their core proposition that the top management can have an influence on the organizational culture through the shaping of employee norms, values and beliefs. This then can lead to the shaping of employee attitudes towards ISP and their intentions to comply with it. The strongest correlation was found between top management participation and employee perceived behavioral control and subjective norms. The relationship between top management participation and employee attitudes proved to be insignificant. They noted that the relationship between top management actions and employee attitudes and intension is not necessarily that strong in larger organizations where the distance between employees and top executives in the hierarchy is more significant than compared to smaller organizations. Puhakainen and Siponen (2010) also concluded that the support of top management towards information security policy is crucial if an organization aims to have their employees to comply with it. Additionally, the role of top management in affecting employee attitudes and behavior has also been found to be important in other information technology related literature. For example, Liang et.al. (2007) and Sharma and Yetton (2003) both found that having a top management actively participating and supporting an implementation of a new information system can have a significant positive effect on the success of the implementation process.

Chang and Ling (2007) looked at the management and culture from a different perspective: they studied the organizational culture and its' influence on the implementation of an effective information security management in terms of four ISM constructs: availability, integrity, confidentiality (see chapter 2.1) and

accountability (employee accountability of their actions). They argued that flexibility as a cultural trait of an organization can be counterproductive for information security development whereas control oriented culture can better benefit information security effectiveness (Figure 4.)

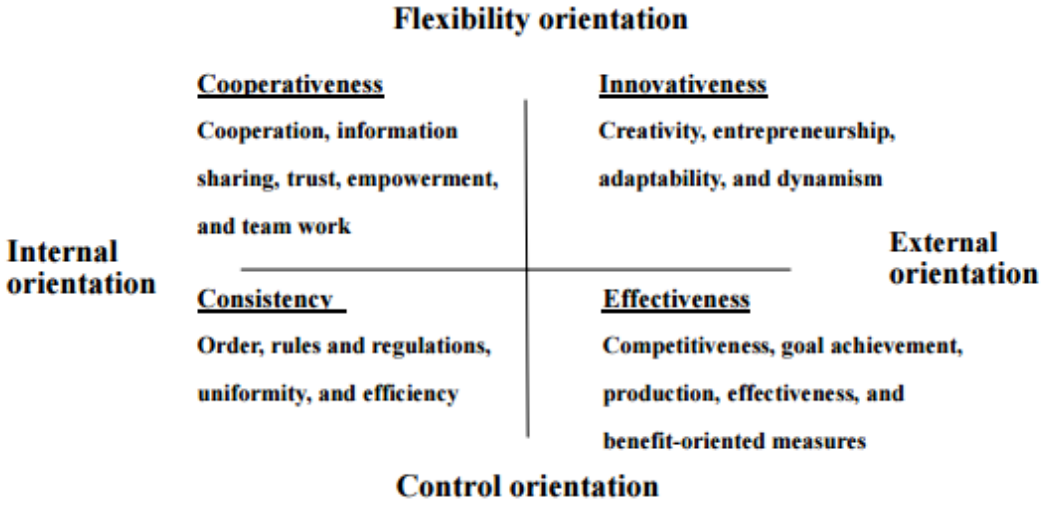

Figure 4 Culture traits of organization applied to ISM by Cheng and Ling (2007)

As presented in figure 4, flexibility traits include cooperativeness and innovativeness related attributes and control traits consist of effectiveness and consistency ones. These observations are not, however, to be mistaken as meaning that flexibility orientation is to be minimized and focus to be solely on control orientation. Obviously, such values as creativity, team work and trust are imperative for organizations to maintain their competitive edge in today's markets. It is however recommendable for organization's management to ensure that the aforementioned four ISM constructs are not compromised (Cheng and Ling, 2007). For example, in a cultural environment where information sharing and cooperation is encouraged but not enough consideration is given to regulating it in terms of information security, situations may occur where unauthorized parties gain access to information they are not supposed to. This can lead to damages of unexpected severity. To conclude, in order for an organization to implement and carry out an effective information security policy, there should be, to some degree, emphasis on the control orientation in the organizational culture.

Organizational culture and actions and attitudes of management have indeed a big role to play in influencing employee attitudes towards information security policies. Culture is the foundation that describes the values and beliefs that those in the organization share and management can have a major influence in that. Having management to emphasize the value and importance of information security and showing their commitment to it can improve employee attitudes and behavior. Management should also emphasize, to a necessary degree,

cultural traits that can support the effectiveness of the organization's information security policy, such as uniformity and rule-orientation.

3.4 Awareness and training programs

As it has already been brought up, employee security behavior and compliance with ISP has a lot to do with their understanding of the information security related issues and their attitudes towards organization's ISP and guidelines. When the severity of consequences of even the most insignificant seeming harmful actions such as using one's own USB sticks in a company computer and writing the password down on a sticky note is not properly comprehended, these mistakes are very likely to happen. Thus, it is important for any organization, regardless of size or type of business, to implement employee information security awareness training. This can help better educate employees on the importance of information security and to change their attitudes towards being more inclined to comply with ISP.

Already at the end of the 20th century, Thomson and von Solms (1998) brought up the importance of educating organization's personnel on the importance of information security through awareness programs and argued on behalf of using social psychology principles, to help develop better training programs. They also highlighted the importance of tailoring the programs to suit the need of specific audiences such as management, users and IT personnel. Programs that are suitable for others, are often not suitable for some because people have different base knowledge and preferred learning outcomes that the program needs to address. These principles, such as how social learning, conformity and acceptance relate to employee behavior and attitude, provide insights into how awareness programs could be designed. Thomson and Von Solms (1998) saw attitude as the ultimate goal that was to be changed through influencing behavior, beliefs, emotions and other cognitive factors. Puhakainen and Siponen (2010) emphasized the importance of education programs that have a strong theoretical and empirical basis. In other words, there should be good reasoning behind every program to explain why and how they work and empirical evidence to support it. It is important for those who apply the program to know how the program enhances learning and what elements of it are expected to change the behavior of IS users. Another important aspect of an efficient security training program that Puhakainen and Siponen (2010) bring up is practicality: in order for the program to be applied properly in practice, guidelines for implementation need to be included.

The aforementioned requirements for an effective learning program in mind, Puhakainen and Siponen (2010) applied universal constructive instructional theory (UCIT) and elaboration likelihood model of persuasion (ELM) to provide a training program for security training supported by an action research study. UCIT is a theory aimed at providing guidance to designing a training pro-

gress and it consists of a framework of four steps: defining the instructional objective, determining the learners present state (in terms of knowledge and attitude), creation and delivering of the instructions and the evaluation of the success (Tennyson et.al. 1997).

ELM proposes that there are two roads of persuasion: central and peripheral. The central road refers to a person handling the achieved information cognitively as in carefully considering the content of the information itself and the peripheral road is more about the person relying on cues such as the perceived influence of the speaker. The central road of the ELM is more likely to lead to permanent change of attitudes. (Petty and Cacioppo, 1984.) If one, for example, is simply motivated by some external reward when taking part in an information security training, it is likely that the changes in attitude are not long term and are more susceptible to change.

From their study, Puhakainen and Siponen (2010) highlight the findings related to cognitive learning and information security communication. As mentioned above in ELM definition, cognitive learning is crucial to ensure a long-term attitude change in the participant. Information security communication is about adjoining information security with other communication in the organization so that it is not just a theme that is discussed once. The communication should also include all the appropriate actors in the organization such as management and users to actively share information with one another.

Shaw et.al. (2009) studied the role of information richness on the effectiveness of awareness training that takes place online. Online training programs can be a cost-effective option for organizations on a tight budget. They looked at how online media in various forms (hypermedia, hypertext, multimedia) can enhance the security awareness of IT user in terms of perception (sensing security risks), comprehension (understanding the nature of various risks) and projection (ability to predict and prevent). Their findings suggest that security training received in the form of hypermedia and multimedia are most effective when the goal is to generate more comprehensive understanding of information security in the learner. On the other hand, if the goal is to just increase overall perception of security risks, relying on just hypertext could be more efficient since more information rich variants can detract users from the subject matter.

To conclude, improving employee awareness of information security by implementing training programs is recommended for every organization. To ensure long terms effects of attitude change towards information security policy, training programs should include elements that help employees to engage in cognitive learning. Additionally, communicating information security in everyday organizational communication is necessary to help keep it freshly in mind. Learning always broadens the mind and educating employees is perhaps the most important factor in changing their attitudes to positive regarding information security policy.

4 Conclusions from the literature review

The objective of this literature review was to create an overview of how employee compliance with information security policies has been studied and explained in the existing literature. The literature review was conducted by reviewing publications found through various research portals such as Google Scholar, EJIS and MISQ. The main goal of the literature review was to find out what are the motivations behind employee information security behavior according to existing literature.

The motivation for studying this issue comes from the fact that information security related incidents are constantly increasing every year and so are the amount of damages they cause for various businesses. While this is happening, it seems that organizations still do not take their information security seriously as studies show that they lack severely in their methods and techniques to protect their information assets (Kauppalehti, 20.8.2016). While technical solutions are important in protecting critical organizational assets, the most common weakest link in information security is people. This is the reason it is important to understand what drives people to behave in an unsecure manner and how their behavior could be improved.

Existing literature on information security compliance clearly indicates that explaining and predicting employee attitudes and behavior is no unambiguous matter. Whether it is intrinsic or extrinsic motivations, communication, management, organizational culture or knowledge and awareness or fear related factors, they all have their role to play in influencing employee attitudes towards ISP compliance and information security behavior overall.

The factor that seems to be brought up in many research papers, is the importance of employee knowledge and awareness of information security risks because it helps them to understand why following information security policies is important. Awareness programs are a good way to enhance employee knowledge of information security and are recommended to every organizations. To enhance learning, there should be discussion sessions built around the learning material: this can increase the cognitive processing of information which can lead to better long-term results. Increasing awareness increases the way employees perceive the information security behavior. When they understand the value of compliance to both them and the organization, they are more likely to follow the organization's policies. In addition, compliance is more likely when employees perceive that they have the skills and the knowledge to practice proper information security behavior.

Information security should also be implemented as an essential part of the organizational culture. Having information security as one of the core values helps to emphasize its' importance to both, inside and outside of the organization. This way, even those who are just applying for the organization are, to some degree, aware of the importance of proper information security practices in the organization. Management of the organization is the key to achieving this goal.

They have the responsibility, with their example, to show that they too are committed to improving and maintaining information security. If employees perceive that management does not take information security seriously, it may leave them with very little motivation to follow them as well.

Another important factor is keeping information security present in the organization's daily communication and as a part of the overall strategy as well. It is not enough that issues and risks related to information security are brought up in an awareness and training sessions once a year. Information security- thinking should be a constant mindset that is present in the everyday work. Communication should also be conducted horizontally and vertically and not just from top to bottom. This is important in order to create proper discussion about the important matters of information security.

Leadership commitment, clearly documented policies, communication, employee awareness and training programs are the key in motivating employees to commit to information security policies and guidelines and to ensure organizations information assets stay safe. Management leads the way for the rest of the organization, so it is only when they realize the importance of information security and commit themselves, that it is possible to begin the process of committing the employees as well. Management needs to implement information security as a part of their organization's business processes and within everyday communication of the organization. This helps build a culture that values information security thinking and open discussion. Changing and maintaining a desired organizational culture is no small task and requires good planning, patience and commitment. Changes do not happen overnight and this type of project is ongoing in nature.

Other factors such as the effects of fear and punishment seemed to have produced contradictory results in the previous research. On the one hand, there should be formal consequences for violating information security policy but organizations should not only rely on fear of punishment as an adequate motivator to get employees to comply.

When all the aforementioned factors taken into consideration organizations have a good chance to increase their capabilities regarding proactiveness and reactiveness in the face of constantly increasing risk of being targeted by cyber criminals, and malicious or unintentional actions of those from within the organization. Without proper awareness and knowledge of information security, and having formal policies in place, organizations, both big and small, are risking their reputation and financial stability.

5 Research methodology

In the empirical part of the thesis the objective is to try to gain insight into how information security is viewed by employees and what are the *main motivators* behind their information security behavior. The approach chosen to achieve this is theme-based interviews. In this chapter, the research method, strategy and data collection approach will be explained in a more detailed manner.

5.1 Qualitative research as a research method

Theme-based interview method utilized in this study is a qualitative research method. Qualitative research can mean a myriad of different approaches to gather and analyze research material to study phenomena of human life within different contexts. (Saaranen-Kauppinen and Puusniekka, 2006) Qualitative research is about depicting real life and thoroughly studying a phenomenon. Typical characteristics of qualitative research can be, for example, theme-based interviews highlighting the viewpoints of the study subjects and analyzing and interpreting research data from the interviews as something that contains unique opinions and convictions (Hirsjärvi, Remes and Sajavaara. 2006)

5.2 Theme-based interviews

Theme-based interview is a semi-structured approach where interviews progress within predefined themes but interviewees can explain their views and experiences freely in their own words. Theme-based interviews are not quite the same as open interviews because the themes that are based on previously studied matters are the same for all the interviewees. The goal of the interviews is to gather information about the subjective experiences of the interviewees. What leads to structuring interview questions in the form of various themes, is that the researcher usually has some expectations regarding the results from the interviews, and these expectations are based on previously studied literature. (Hirsjärvi and Hurme, 2001, 47–48.)

Theme-based interviews can be more conversational in nature and while all themes are discussed with every interviewee, not all are necessarily discussed in a same scope with everyone. The order of the discussed themes can also be free (Saaranen-Kauppinen and Puusniekka, 2006). The themes that the interview is divided in should be general in a sense that they are relevant to all interviewees (Hirsjärvi & Hurme, 2001).

Interviews in general can be a very challenging approach to study a phenomenon. They rely heavily in the ability of the interviewer to conduct inter-

views in a way that yields as much useful information as possible. A lot also depends on how the questions are formed and what methods are used to analyze the interviews. (Hirsjärvi and Hurme, 2001, 34–35.) When people communicate with one another, there is always room for misinterpretations and a chance that the interviewee is not completely honest in his or her answers. The challenge of honesty is especially an aspect that needed to be considered carefully in this study because some of the interview themes considered negative information security related behavior and reasoning behind it.

5.3 Study process

The next chapters will describe the research process, including the selection of interviewees, planning of the interviews and the method used to analyze the results.

5.3.1 Planning and conducting the interviews

Theme-based interviews as a method to conduct the empirical part of this study was chosen because interviews are an effective method to gather information regarding attitudes, values and experiences of individuals (Jyväskylän Yliopisto, 2015) The themes chosen to guide the interviews were based on the topics gathered from the literature review (Table 1). Additionally, more detailed questions were created to support the interview (Attachment 1) but these questions were not meant to guide the interviews. Their role was to keep the discussion going and to gather more detailed information related to each theme.

Interview themes	**Source**
Attitudes towards information security.	Ajzen, 1985: Bulgurcu et.al. 2010
Belief in own capabilities.	Ajzen, 1985: Bulgurcu et.al.2010
Effect of others on the attitude and behavior.	Ajzen, 1985; Bulgurcu et.al. 2010; Ifinedo 2014; Herath and Rao 2009b
Perceived benefits/costs of following information security guidelines/policies in daily work.	Bulgurcu et.al. 2010; Scott, 2000; Li, Zhang, and Sarathy 2010

Perceived role of punishment	Herath and Rao, 2009b, Siponen and Vance, 2012
Effect of incentives on security behavior.	Chen et.al. 2012
Reasoning for unsecure security behavior.	Sykes and Matza, 1957; Siponen and Vance, 2010
Information security culture and role of management.	Von Solms and Von Solms 2004a; Hu et.al. 2012
Motivation and attitudes towards learning and participating in awareness programs.	Thomson and von Solms, 1998; Puhakainen and Siponen, 2010

Table 1 Interview themes

The goal of the interviews was to gain insight into what motivates an individual, in the context of information security, to behave in a certain way. Beforehand, the most challenging aspect of the interviews was expected to be getting the interviewees to be as open and honest as possible. Honesty is a factor that is quite difficult to measure but based on the interviewees responses, it did not prove to be a significant issue.

When using theme-based interviews, the assumption is that all participants have experiences and some knowledge related to the interview topic (Hirsjärvi and Hurme, 2001) When talking about information security, the assumption is that everyone who uses computers or mobile devices in their daily work life and personal life, have some knowledge related to protecting their devices and information within them. In other words, it is safe to assume that most people know what it means when discussing about passwords, USB-devices, spam email, malware etc.

Three individuals were chosen to be interviewed for the study and each of them were interviewed individually. Other possibility could have been to organize a group interview but there would have been the risk that the interviewees would have not been so willing to share their viewpoints and experiences with one another. Interviewing everyone individually proved to be a good decision in terms of how openly everyone was willing to share their own stories of improper information security behavior.

The interviewees were selected based two criteria: interviewees needed to be currently working, preferably full time and in a job where information security is relevant to the organization they work for. Two of the participants were familiar with the interviewee beforehand. All participants were ensured that the interviews will be kept anonymous and that the recordings will be destroyed immediately after they are no longer needed.

Three interviews is not a large number but in the scope of this study, it was enough to gather interesting and useful insight about how individuals from differing backgrounds view information security, what their viewpoints are, and how they reason their own behavior.

One of the interviews was conducted face-to-face, one via Skype video call and on via telephone. Before the interviews, each interviewee was explained what the study was about. All interviews maintained a very casual and, at times, conversational atmosphere and all interviewees seemed to be very open and willing to contribute to the study. The interviews went mostly according to the theme structure.

5.3.2 Analyzing the interviews

All the interviews were recorded and parts relevant to the topic were transcribed in a casual form. The interviewees were codenamed I1, I2 and I3 to protect their anonymity.

After the interview transcripts were simplified, the material was analyzed by matching interview answers with the corresponding theme. This was relatively easy because the interviews mostly followed the predefined theme structure. The goal of the analysis was to see what each interviewee had to say in relation to each of the themes and to determine how the answers reflected the literature that the themes were based on, and to see if there were any new themes to be observed. The results of the interviews will be presented in the next chapter.

6 Results

This chapter will first describe the interviewee background information and then the interview results will be examined by each theme presented in the previous chapter (Table 1.)

6.1 Interviewee background information

Three interviewees were selected to be interviewed for the study. Each of the interviewees were currently working in fields where information security is important in many ways, which of course is the case for most businesses nowadays.

The first interviewee (I1) was a woman who has worked as a sales representative for a large international pharmaceutical company for over 20 years. In her daily work, she uses laptop and mobile devices that can be used to access sensitive customer data and other critical company information. Basic important concepts of information security related aspects were familiar to her.

The second interviewee (I2) was a man who has been working as a real estate inspector for a little over a year. His daily work also includes using laptops and mobile devices and handling of personal information and other critical information that needs to be protected. I2 had a good basic understanding of the importance of information security and its' concepts.

The third interviewee (I3) was a man who has been working 6 months as a programmer and a designer so information security also plays a key role in his workplace as well. Due to I3's educational background (computer sciences), it is safe to assume that he possessed a bit more comprehensive overall knowledge regarding various concepts of information security than the other two interviewees.

As is expected in many fields of work these days, it can be concluded that information security is in one way or another a part of the work of each of the three interviewees. As mentioned before, the weakest link in an organization's information security is usually the employees and so, the next chapters will dive into the attitudes, motivations and behavior of the aforementioned three individuals who were interviewed for this study.

6.2 Attitudes

The first theme was the overall attitudes of the interviewees regarding good information security behavior and compliance with possible information security guidelines of policies in place within the organizations they worked for. As was brought up by Bulgurcu et.al. (2010), attitudes towards certain behaviors is a significant factor that drives people's actual behavior.

Although the overall attitudes of the interviewees towards proper information security behavior seemed to be positive, there was some lack of understanding on part of one interviewee of when and how information security should be taken into consideration. I1 brought up that she felt that she was not at risk of information security incidents because her work was mostly conducted in the field. The problem with this way of thinking is that I1 uses mobile devices that can be used to access company information such as customer data, sales material, emails and so forth. All this type of material was confirmed by I1 to include information that should no end up in the hands of outsiders. I1 did however mention herself that this type of thinking may not be correct and understood that she may have a false sense of being safe from information security related risks.

I2 and I3 both saw information security as something that is important to always keep in mind. I2 mentioned that his company has recently implemented an information security strategy and saw this as a positive thing. I3, while mentioning that information security should be a part of everyday work, noted that during his time at his current job it has been discussed very little and it was also not brought up as part of the introduction period.

6.3 Personal capabilities

For employees to behave in a secure way and according to information security guidelines, it is important that they believe in their own capabilities to do so (Bulgurcu et.al. 2010). All the interviewees said to think they possess good basic capabilities to behave according to good security practices and knew how to comply with their organization's information security guidelines. There were however some clear contradictions between beliefs in own capabilities and actual behavior. One of the interviewees for example said to have stored all of his passwords on a single notepad file and also had a habit of writing down passwords on post-it notes.

6.4 Behavior of others in the workplace

The way others in the workplace behave can have an effect on an individual's behavior as well. If others seem to be neglecting information security it can make it easier for an individual to follow the same behavior pattern, and vice versa. (Bulgurcu et.al. 2010; Ifinedo 2014; Herath and Rao 2009b.)

All the interviewees were on the same line in that the way others behave in the workplace, could affect their own behavior. I3 said that behavior of others definitely has an effect on his behavior and added that it holds through in all areas of life. I2 highlighted that it is more about the overall atmosphere in the workplace. If it seems most people do not take guidelines or good information security seriously, it has a more of an effect than if just few people behave in a

certain manner. I2 mentioned to have spotted some bad information security related behavior such as colleagues sharing passwords with one another, but said he would not follow the same type of behavior.

6.5 Perceived benefits and costs and behavior reasoning

Individuals have been shown to behave in a certain manner based on how they perceive possible benefits or costs of a certain type of behavior (Bulgurcu et.al. 2010; Scott, 2000; Li, Zhang, and Sarathy 2010). If for example, an individual perceives that writing down his password on a piece of paper has more benefits than possible costs to him, then more likely he is to do so. This is also closely related to how individuals reason with their own behavior. As was depicted with the protection motivation theory by Sykes and Matza (1957) and Siponen and Vance (2010), there are a lot of ways for an individual to reason their behavior. All the interviewees had some negative information security behavior habits to share.

I1 said that she had all her passwords written on a single unprotected notepad- file and also had some of her passwords written to post-it notes at her home office. The reason for this was to make her work easier when she did not have to remember each password. But as was mentioned before, while she knew about various information security risks related to this type of behavior, she said that she felt safe in that she did not see herself as being at risk of information security incidents.

I2's bad habits were using same passwords for different accounts and not keeping his personal computer up-to-date. As a reason, he stated part convenience and part laziness. He said that he knows the risks but still convenience often wins. He did also mention that one time he had a scare that someone was trying to tamper with his Facebook account from another country. He said that after the incident he has been taking information security more seriously.

I3 had similar tendencies than I2 in that he also said to use same passwords for various accounts and reason for this was once again convenience. He also mentioned to have plugged in an unknown USB- stick that he found on the ground, into his own computer, even though he knew that there was a good possibility that it could contain malware. I3 said that he was simply too curious to see what the USB-stick contained.

6.6 Perceived role of incentives and repercussions

When asked about how the interviewees perceived possible punishment from unwanted information security behavior all gave similar responses. None of the interviewees were aware if there were specific consequences determined for information security incidents in the organizations they worked for. All interviewees said that if severe consequences were determined for unwanted behavior,

they would be more likely to take information security into consideration more often and make sure that they followed guidelines and good practices more consistently. When asked about if just the fear of consequences was enough, all the interviewees disagreed.

When discussing thoughts on incentives for good information security behavior, all interviewees had similar views. Common notion was that while incentives, such as rewarding good information security behavior would be a good idea, the way something like that could be implemented effectively and fairly seemed problematic.

6.7 Culture and management

As highlighted by Von Solms and Von Solms (2004a), embedding information security policies as a part of organizational culture can be an effective way of enhancing employee compliance. In turn, it is the organization's management that often has the most significant effect on the prevailing culture in the organization as they set the example to others with their own behavior (Hu et.al. 2012).

Interviewees were asked about how they perceive their current culture and management commitment in the context of information security. I1 said that information security is only present once a year in the form of compulsory eLearning course. Other than that, she said that information security is never brought up by the management and that it is never discussed in any meetings or daily communication.

I2 said that in his organization, information security has been on the pedestal a bit more during the past year because they had implemented an information security strategy. According to I2 this strategy is not in any ways currently present in daily work. He also added that no written guidelines were published related to it and that existing guidelines merely concerned password changes and password lengths. Overall, I2 had not seen or felt any changes in the organization's culture but believed that it will change with small steps towards being more security oriented.

In the organization that I3 works for, information had not been present or discussed in any way during the time he has worked there. He said that even when a large cyberattack had wide media coverage and proposed a risk to many organizations, it was not discussed at all. He thought that the lack of focus on information security was odd since sensitive customer data is handled at company on a daily basis. I3 also said that nothing information security related was present in his introduction period when he joined the company.

6.8 Motivation to learn

The last theme discussed with the interviewees was about their thoughts and motivation regarding learning and participating in information security awareness programs/courses. Interviewees were also asked what they thought would be the best approach to improve information security behavior in their organizations.

I1 had experience in information security eLearning courses that were mandatory for every employee to complete once a year. She said that the eLearning was a good way to refresh memory on the topic of information security but felt that they were not very memorable. I1's opinion was that good real word examples of what can go wrong and what the consequences are when information security is neglected would be the best way to help understand and remember the importance of information security.

I2 had attended some information security training but felt that they should be organized more often. He also mentioned that practical examples were a good way to understand and learn better and also said that learning programs should highlight how an individual can enhance information security with his own actions.

As already mentioned, I3 had not participated in any information security awareness training. He did however think that they should definitely be held on a regular basis. His thoughts were that information security training should focus on thoroughly going through the basics of good information security behavior and highlight the fact that human mistakes are the most common cause for incidents.

7 Conclusions and Summary

In this chapter, the research results are discussed in relation to the research question and the existing literature. The applicability of the results and possible future directions of the research topics will also be discussed.

This study was done in order get insights into what motivates employee information security behavior and how they view the role of information security in their workplace. All the interviewees had a lot of similar thoughts about the different themes that were discussed and the most important motivators for both negative and positive information security behavior had a lot of commonalities.

When it comes to attitudes, all interviewees thought that information security is important. Information security related rules and guidelines were not perceived to be a hindrance to daily work.

As could be expected, regardless of having an overall positive attitude towards information security and believing to possess adequate understanding of information security, neglecting it occurs from time to time. Most common reason for this was avoiding inconveniences. This mostly had to with negative information security behavior related to passwords such as not changing them regularly, writing them down and having same passwords for multiple accounts. All the aforementioned behavior types have to do with making it easier to remember passwords. This is very much in line with Li, Zhang, and Sarathy (2010) who argued that when perceived benefits of noncompliance outweigh the benefits of compliance, an individual is more likely to choose the one that they feel benefits them the most. False sense of security was also a theme that was brought up and it could also be seen as an important contributor to neglecting information security. This is closely related to the level of information security awareness: if people do not understand all the ways that they can neglect information security and the possible consequences, more likely they are to neglect it.

Regarding the effect of punishments, the literature indicates that *formal sacntions* are not very effective in deterring bad behavior (Siponen and Vance, 2012), and that more severe consequences could have a more negative effect on information security behavior (Herath and Rao, 2009b). Based on the results of this study however, clearly defined severe consequences were perceived as something that would indeed motivate to better consider information security in daily work. There is of course always differences in what people say when asked about the effects of possible punishments and how they actually behave.

The behavior of others also indicated to have possible effects on information security behavior. This has to do with the overall atmosphere and attitudes around a workplace. If it is perceived by an individual that others do not take information security seriously and choose to neglect guidelines or policies, more likely he is to adapt similar behavior. This was also brought up by Herath and Rao (2009b) who studied the effects of other people's behavior and expectations on an individual's information security compliance behavior.

In line with Herath and Rao (2009b) and Puhakainen and Siponen (2010), the findings also support the importance of educating employees on the concepts of information security. Real world examples of information security incidents and their consequences, and providing employees with knowledge on how they can improve their organization's information security with their own actions, were brought up as an effective way into improving employee information security behavior. Participants in this study were also very willing to participate in awareness programs.

Overall, the results of this study found a lot of support for the existing literature. While the interviews did not provide anything particularly new tin terms of motivations behind information security behavior, they provided a good viewpoint into how people personally view information security and what their behavioral motivators are. What motivates people to behave in a certain way is always a difficult subject to study and involves many variables.

7.1 Evaluation of the study

According to Eskola & Suoranta (1998) qualitative studies can be evaluated based on their credibility, applicability, reliability and verifiability. Credibility can be evaluated based how the interview structure was created. In this study, the interview themes and questions were based on the existing literature. Considering that the results of the interviews were quite well comparable with the existing literature, the interviews can be considered credible.

In terms of applicability, even though the number of interviewees was relatively low, they did however provide enough insights and their answers were very much similar with each other. Considering this, the number of interviews conducted was enough for the purposes of this study. The most significant limitation of the study is that only one research method was utilized.

The study is also reliable in the sense that no expectations were created beforehand that could have guided the results. The interview answers were also not guided in any way and the results base on the views and experiences of the interviewees. And finally, the results of the study are verifiable in the sense that the interview results have a lot of commonalities with the earlier literature.

7.2 Topics for future research

This study focused on the most significant motivations behind information security behavior of employees. The interviewees were selected based on only the criteria that they need information technology in their daily work. For future research, it could be interesting to focus the study on employee information security behavior in specific industries, such as medicine where information security

is in a particularly important role due to the handling of sensitive patient information.

While this study focused on the employee information security behavior, the future research could study information security on the top management level. For an organization to have an effective approach to information security, management needs to understand its' importance and lead the way in making it a top priority. Hence it would be beneficial to study how top management could be better motivated to take action in improving their organization's information security.

REFERENCES

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer Berlin Heidelberg.

Boer, H., & Seydel, E. R. (1996). Protection motivation theory.

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

Chang, E.S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438-458.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447-459.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007, January). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in' Australia. In *ECIS* (pp. 1560-1571).

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, *14*(1), 57-74.

Eskola, J., & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino

Frey, B. S., & Osterloh, M. (Eds.). (2001). *Successful management by motivation: Balancing intrinsic and extrinsic incentives*. Springer Science & Business Media. p. 8.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information management & computer security*, *13*(4), 297-310.

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

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*(2), 106-125.

Hirsjärvi, S. & Hurme, H. (2001). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2006). Tutki ja kirjoita. (12. uud. painos). Helsinki: Tammi.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? *Computers & Security*, *21*(5), 402-409.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Järvenpää, S. L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS quarterly*, 205-227.

Jyväskylän Yliopisto (10.6.2015) Haastattelut. Haettu 6.7.2017 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/haastattelut

Kauppalehti, 20.8.2016: Selvitys: Tietoturva ei paljon yrityksiä hetkauta. Haettu 30.11.2016 osoitteesta: http://www.kauppalehti.fi/uutiset/selvitys-tietoturva-ei-yrityksia-paljon-hetkauta/zT5HUTy9

Kouzes, J. M., & Posner, B. Z. (2006). *The leadership challenge* (Vol. 3). John Wiley & Sons.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635-645.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS quarterly*, 59-87.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency*, *18*(2), 295-318.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, T. (2009). What Levels of Moral Reasoning and Values Explain Adherence to Information Security Policies? An Empirical Study. European Journal of Information Systems 18(2): 126–139.

Petty, R. E., & Cacioppo, J. T. (1984). Source factors and the elaboration likelihood model of persuasion. *NA-Advances in Consumer Research Volume 11*.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 757-778.

Scott, J. (2000). Rational choice theory. *Understanding contemporary society: Theories of the present*, *129*.

Saaranen-Kauppinen, A & Puusniekka, A 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 5.7.2017 osoitteesta: http://www.fsd.uta.fi/menetelmaopetus/kvali/L1_2.html

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management*, *39*(4), 60.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100

Siegel, L.J. (2005). *Criminology: The Core Second Edition*. Thompson.

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and society*, *31*(2), 24-29.

Siponen, M (2000),"A conceptual foundation for organizational information security awareness", Information Management & Computer Security, Vol. 8 Iss 1 pp. 31 – 41

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Siponen, M. (2001b). On the role of human mortality in information system security: From the problems of descriptivism to non-descriptive foundations. Information Resources Management Journal 14(4): 15-23.

Straub, D. W., Goodman, S. E., & Baskerville, R. (2008). *Information security: policy, processes, and practices*. ME Sharpe.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: A holistic approach. *ISSE/SECURE 2007 Securing Electronic Business Processes* (pp. 331-339).

Tennyson, R. D., Dijkstra, S., Schott, F., & Seel, N. M. (1997). *Instructional Design: Theory, research, and models* (Vol. 1). Routledge

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167-173.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: a rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, *24*(1), 21-41.

Von Solms, R., & Von Solms, B. (2004a). From policies to culture. *Computers & Security*, **23**(4), 275–279.

Von Solms, B., & Von Solms, R. (2004b). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Von Solms, S. B. (2005). Information Security Governance–compliance management vs operational management. *Computers & Security*, *24*(6), 443-447.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security*, *23*(3), 191-198.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review*, 545-572.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360-365.

ATTACHMENT 1

Structure of the theme interview

These questions were not meant to provide a strict structure for the interview but rather serve as overall talking points during the interview.

What do you think good information security behavior means?

- Do you consider information security in your daily work and you think it is something that is important in your daily work? (Ajzen, 1985: Bulgurcu et.al. 2010)

Do you think that management in your organization is committed to proper information security practices/ committed to the information security policy? (Von Solms, R and Von Solms, B 2004a; Hu et.al. 2012)

- Has the importance of following proper information security practices been discussed in your organization?
- How often are information security related matters discussed in a daily organizational communication?

As far as you know, does your company have any formal information security guide or policy in place?

- Are you familiar with the content of the guidelines/policies?
- Are they readily accessible if you need them?

Do you feel that you have followed your organization's information security policy to the best of your knowledge?

- Do you feel you have the necessary tools and knowledge to comply with the policies/guidelines?
- Do you think some rules in the policies/guidelines are unnecessary?
- Are there any aspects that you think complicate compliance with information security policies?

Do you feel that others in your organization act according to proper information security behavior?

- Do you think the behavior of others influence your information security behavior?

Have you ever knowingly/unknowingly acted in a way that was against the information security policies of your organization/ good information security behavior? (What are the reasons?)

- Have you ever shared your passwords with anyone?
- Have you used your own/unknown external storage devices on your organization's devices?
- Have you opened files or links on an unknown email?
- Have you consistently followed a clean desk- policy?

Are there any official sanctions in place if information security policies/guidelines are violated?

- Do you feel that the possibility or severity of punishment would have a significant effect on the information security behavior in your organization? (Williams and Hawkings, 1989)
- How likely do you think it is that improper information security behavior will be punished? (Williams and Hawkings, 1989)
- How severe do you think the consequences would be? (Williams and Hawkings, 1989)

How do you think information security behavior could be increased in your organization?

- Do you think some type of incentives would motivate proper behavior? (Chen et.al. 2012)
- What type of incentives?

Has your organization arranged any information security related training? (Thomson and von Solms, 1998; Puhakainen and Siponen, 2010)

- What type of training have you received?
- Did you feel the training was useful for you?
- Do you wish training should be arranged more often?
- What type of training do you think would be most beneficial to you?

Do you think that management in your organization is committed to proper information security practices/ committed to the information security policy? (Von Solms, R and Von Solms, B 2004a; Hu et.al. 2012)

- Has the importance of following proper information security practices been discussed in your organization?

How often are information security related matters discussed in a daily organizational communication in your organization?