The Strength of the Chain is in its Weakest Link

A qualitative study of how employee information security behavior can be enhanced

Julia Hergart

Jennifer Ren Liu

Bachelor Thesis
Stockholm School of Economics
May 2020

Abstract

Information is one of the most valuable assets for an organization. However, through the evolution of the internet, it has become increasingly difficult for organizations to protect their information assets. Although firewalls and other technological tools are necessary, it is increasingly acknowledged that humans are the weakest link in ensuring information security (IS). The aim of this thesis is therefore to explore how employee IS behavior can be enhanced. A cross-sectional study was conducted including three of the four largest banks in Sweden: SEB, Swedbank and Handelsbanken. In total, 16 in-depth interviews with IS managers and users were conducted, followed by an analysis based on the Theory of Planned Behavior. The findings from the study imply that employee IS behavior can be improved through a focus on threat awareness, management support and participation, communication, social learning, security culture and self-efficacy. These results enhance the knowledge about what aspects that can be considered valuable for organizations to mitigate the risk of the human element in IS. It can further give suggestions to practitioners as they design their information security programs.

Keywords: Information Security, Information Security Behavior, Banking Sector, Employee Behavior, Theory of Planned Behavior

Authors:
Julia Hergart (24251)
Jennifer Ren Liu (24057)

Supervisor:
Ingela Sölvell, Researcher, *Centre for Advanced Studies in Leadership*

Examiner:
Laurence Romani, Associate Professor, *Department of Management and Organization*

Bachelor Thesis
Bachelor Program in Management
Stockholm School of Economics

Acknowledgements

We would like to acknowledge and extend our sincere gratitude to everyone who have challenged, supported and helped us throughout the completion of this thesis.

To our supervisor Ingela Sölvell - for your attention to detail and always challenging us.

To our supervisor-group - for your support and valuable feedback.

To the respondents at Handelsbanken, SEB and Swedbank - for sharing your experiences.

To our families - for always being there for us.

Thank you!

TABLE OF CONTENTS

1. Introduction

1.1 Background

The 21st century has been characterized by a new competitive landscape driven by globalization, deregulation and a rapid development of technology and digitization. Although this digital era comes with many opportunities, it also brings a great deal of challenges (Salminen and Hossain, 2018). One of the main concerns for today's businesses is information security (IS)[1]. As the world is becoming increasingly connected, individuals and organizations are more vulnerable and exposed to cyber attacks than ever before. IS management has to be a top priority for organizations to protect the company's information against IS incidents, which often disrupt operations, damage organizational reputation and cause financial losses (McLaughlin and Gogan, 2018). Programs and systems companies use to protect themselves against viruses, malware, spam, phishing and spyware are all essential, but do not seem to be sufficient to ensure safety of information on their own (Safa and Sookhak et al. 2015). In fact, one of the main reasons why IS is a continuous plague organizations is because of the employees, which are considered the "weakest link" in ensuring IS (e.g. Vroom and von Solms, 2004; Warkentin and Willison, 2009; Spears and Barki, 2010). Employees often lack information security awareness and show negligence, passivity and resistance towards IS, making them a prime target for hackers (Safa et al., 2016). Hackers that are after company information do not primarily target their systems, but rather the people working in the organization (Safa et al., 2016). As a result, despite large investments in technological tools, incidents related to IS continue to rise due to ignorance of the security risk related to the employees in the organizations (Ifinedo, 2012).

As the issue has grown more serious, most organizations have started to implement preventive measures to avoid harmful IS incidents. Most significantly, many companies have established an IS policy (ISP). Although a step in the right direction, merely adhering to policies and legal frameworks is not sufficient to prevent attacks on their own (Warkentin and Willison, 2009). Thus, the greatest challenge for organizations is not compliance with ISP or development of technological systems, but rather to establish a change in behavior among the employees. Studies indicate that appropriate and constructive employee IS behavior, which is described as a general awareness, vigilance and a strong intention to protect the organization's information, will significantly enhance IS (Öğütçü et al., 2016; Stanton et al., 2004; Ng et al., 2009). It is essential for organizations to understand how this behavior can be achieved. Changing people's behavior is not easy, but there are several frameworks that can help explain and create an understanding of this process. A highly relevant behavioral change framework is the *Theory of Planned Behavior* (TPB) that was introduced by Ajzen (1985). According to Ajzen, behavioral intention, which is the antecedent of actual behavior, is influenced by three constructs: *attitude, subjective norms and perceived behavioral control* (Ajzen, 1991). TPB has been used by a variety of scholars in previous research on IS

[1] Information security is in this thesis defined as the protection of the confidentiality, integrity and availability of information (Finansinspektionen's Regulatory Code, 2014)

behavior in organizations and there is strong support for the model (Ifinedo, 2012; Pahnila et al., 2007; Peace et al., 2003; Bulgurcu et al. , 2010), making it a solid foundation for our theoretical framework. However, as previous studies have mainly taken a deductive and quantitative approach testing core construct relationships (Ifinedo, 2012; Herath and Rao, 2009; Anderson and Agarwal, 2010; Bulgurcu et al., 2010), there is a need for more qualitative studies to find out how these relate to what employees believe will enhance IS behavior (Lebek et al., 2014). Furthermore, since other empirical studies have concentrated on IS managers' perspective (Bauer et al., 2017), there is a growing need for the view of the general employees to provide more generalizable results (Finch et al., 2003). This qualitative study aims to contribute to existing IS behavioral research by exploring how employees believe IS behavior can be enhanced, including both the views of IS managers and general employees. We argue that the professional experience of the IS managers, along with the perspective of the employees who are the targets of IS efforts, can give additional insights to organizations as they design their IS practices.

1.2 Purpose of study and research question

The purpose of this study is to explore how employee IS behavior can be enhanced. This will be done through a combination of empirical data, including both the perspective of IS managers and general employees, and a theoretical framework developed based on the Theory of Planned Behavior. The research question is as following:

"How can employee IS behavior be enhanced?"

1.3 Delimitation

The study is limited to examining the banking sector. Because of their large cash flows, increased dependency on data and important societal function, banks are highly exposed to financial crimes and fraud (Norton and Walker, 2014). They have also been considered to be in the center of the battle against cyber attacks (EY, 2018), which makes it an interesting setting for exploring IS behavior. More specifically, the study will focus on the major commercial banks in Sweden (storbankerna). The reason for this delimitation is twofold. First of all, these banks are significantly larger than the other banks in the Swedish banking sector and their substantial assets and large cash flows make them particularly exposed and vulnerable to cyber attacks compared to other Swedish banks. Secondly, the limitation was made to appropriately match the scope of a bachelor thesis, and with access to interview subjects in mind. The study is further limited to examine individual perceptions and opinions of how IS behavior can be enhanced, with a focus on how the respondents themselves experience the banks' current IS efforts and what else they think should be done.

2. Theoretical background and framework

2.1 Previous research

Previous research on IS has mainly focused on technical issues that relate to the design and application of security systems (Choo, 2011; Zafar and Clark, 2009), such as how intrusion into organizational systems can be prevented with the help of advanced technological tools (Hansen et al., 2007) and how to create the most secure firewalls (Ayuso et al., 2012). Research that explores the human aspect of IS has on the other hand, until recently, been limited. However, as most researchers now agree that the employees constitute the weakest link in securing information assets (Vroom and von Solms, 2004; Warkentin and Willison, 2009; Spears and Barki, 2010), research on risks related to the human element has grown significantly.

To overcome this threat, and strengthen what is considered to be the weakest link in IS, many researchers have suggested using ISP's (Bulgurcu et al., 2010; Pahnila et al., 2007; Ifinedo, 2012). However, while it is necessary to have ISP's outlining specific security requirements, research have found that they do not work alone and that employees often do not comply with these documents (Warkentin and Willison, 2009; Sommerstad et al, 2014; Siponen and Vance, 2010). Scholars have pointed out that focus should not be on compliance, but rather to create a change of behavior (Ifinedo, 2012; Siponen, 2000; D'Arcy et al., 2009; Anderson and Agarwal, 2010). Thus, it is suitable to include and evaluate findings from behavioral theories and examine what implications they may have on IS behavior.

2.1.1 Use of behavioral theories in IS literature

Behavioral theories have been widely used in IS literature (Sommestad et. al, 2014; Lebek et. al, 2014). Three theories have been identified as most prominent within the field of employee's IS behavior and will be presented below.

Theory of Planned Behavior (Ajzen, 1991) builds on the notion that individuals' behavior is determined by their behavioral intentions, which in turn is influenced by *attitudes, subjective norms* and *perceived behavioral control*. The model has been widely used to explain employees' behavioral intention and there is strong support for the model in IS literature (e.g. Ifinedo, 2012; Pahnila et al., 2007; Safa et al., 2015). **Protection Motivation Theory** (Rogers, 1975) suggests that employees' attitude towards IS is based on their assessments of security threats and their abilities to cope with these threats, so called *threat appraisal* and *coping appraisal*. **General Deterrence Theory**, originating from criminal justice research, is based on rational decision-making and builds on the notion that one can discourage people from performing a certain behavior through the fear of formal and informal sanctions (Forcht, 1994). In the context of IS, researchers have found that the *perceived severity of sanctions* and the *perceived certainty of sanctions* impact users' security behavior through a balance between cost and benefits (Anderson and Agarwal, 2010; Herath and Rao, 2009).

The three mentioned theories all explain employees' behavioral intention or actual behavior by adapting different factors. However, the most prominent theory used to find antecedents of information security behavior is Theory of Planned Behavior, which is one of the most well-established theories in the behavioral sciences. As the theory has been considered highly valid by many researchers in the field (e.g. Cox, 2012; Ifinedo, 2014; Lee and Larsen, 2009; Sommestad et al., 2014), and based on an assessment of the empirical material as well as the purpose of our study, we argue that the Theory of Planned Behavior is suitable as a conceptual framework to capture the drivers of IS behavior.

2.1.2 Research gap

Past research on employees' IS behavior has primarily focused on testing the significance of different theories through quantitative methods (Ifinedo, 2012; Herath and Rao, 2009; Anderson and Agarwal, 2010; Bulgurcu et al., 2010). However, research that articulates employees' views about how organizations can enhance IS behavior, is limited. Furthermore, the few empirical studies that have been made are based on the perspective of top management or IS managers (Knapp et al., 2005; Straub and Collins, 1990; Dhillon and Torkzadeh, 2006), which raises the question of whether these findings can be seen as representative for the whole organization (Finch et al., 2003). With employee IS behavior still being a large issue in many organizations, we argue that there is a need to examine what general employees deem necessary to enhance IS behavior, along with the professional experience of IS management.

2.2 Background to TPB

TPB was first introduced by Ajzen (1985) and has been widely used by scholars to predict and explain information security behaviors (Cox, 2012; Ifinedo, 2014). In this section, we will give a short background to the theory, so that we can later discuss the implications of the theory on our specific research question.

TPB is an extension of the Theory of Reasoned Action (TRA) (Fishbein and Ajzen, 1975), but takes into account the effect on non-volitional factors on behavior. According to both theories, behavior is determined by the *intention* to perform the behavior, which is assumed to show the motivational aspects that impact individuals' behavior. Thus, intention serves as an indicator of an individual's readiness to perform a given behavior, and there is empirical evidence of a strong correspondence between the two (Ajzen, 1991; Ajzen, 2011). According to the model, intention is in turn determined by three constructs: attitudes towards the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991). In general, a person's intention to perform a certain behavior is stronger the more favorable the attitude and subjective norm, and the higher perceived behavioral control (Ajzen, 1991). These key constructs of behavior will be discussed further below.

2.3 Elements of TPB

2.3.1 Attitude

Attitudes are formed inevitably and spontaneously. In the case of a behavior, these beliefs are mainly concerned with the behaviors' likely consequences. The attitude towards a behavior is further defined as "*[...] the individual's positive or negative feelings toward engaging in a specified behavior.*" (Khosrow-Pour, 2015, p. 3333). To explore the role of attitude in employee IS behavior, three aspects highlighted as key determinants of attitude will be presented.

2.3.1.1 Awareness of threats

IS researchers have suggested threat awareness as an important factor in shaping individuals' attitude, stating that individuals are more likely to have a positive attitude towards taking action if they believe the threat is significant (Lee and Larsen 2009; Pahnila et al. 2007; Herath et al., 2014; Anderson and Agarwal, 2010). In other words, if the employees have a clear perception of the damage the organization might sustain in the event of an information security compromise, it will result in an improvement of their attitudes (Bélanger et al., 2017). Consequently, behavioral intentions will be stronger (Rogers, 1975) and the likelihood of individuals engaging in appropriate security behavior will increase (Workman et al., 2008).

However, it has been found that individuals generally underestimate security threats and experience a form of personal invulnerability (Hochhauser, 2004). Even though they might recognize that the threat exists, they are not worried about the consequences. This has further been described as a mindset of *"it won't happen to me"* (Roe-Berning and Straker, 1997), which comes from an illusion of invulnerability that is created from a need to perceive the world as stable and orderly (Hochhauser, 2004; Roe-Berning & Straker, 1997). Thus, it is of great importance that an organization makes sure that their employees understand their own or the organization's vulnerability to security threats, as well as the potential damages they could result in (Anderson and Agarwal, 2010; Herath et al., 2014; Herath and Rao, 2009).

2.3.1.3 Management participation and support

Management participation and support have been highlighted by several researchers as crucial in creating positive IS attitudes among employees, and as a key aspect in enhancing IS behavior (Hu et al. 2012; Puhakainen and Siponen, 2010; Cuganesan et al., 2018). Puhakainen and Siponen (2010) found that visible top management support, in the form of promoting IS issues and acting as role models through their own IS behavior, had a significant effect on employee IS attitudes and was an important step in improving employees' behavior. The authors also found that the perception of management not being involved in IS efforts was one of the main reasons why employees demonstrated inappropriate IS behavior. However, as the management changed their attitude toward IS and

became more actively involved, employee attitude toward IS behavior improved significantly and employee participation in IS efforts increased (Puhakainen and Siponen, 2010).
By visibly showing their involvement in the issue, top management can signal to the rest of the organization that IS is an important topic (Schneider et al.,1966). Furthermore, since engaging in IS programs and training is often regarded by employees as "extra work", the legitimacy that comes from top management commitment and participation is argued to be essential (Hu et al., 2012). Apart from attitudes, top management support has been found to have an indirect effect on employee IS behavior via workplace norms (Cuganesan et al., 2018). This has also been emphasized by Hu et al. (2012), who also highlights the role of management participation in creating a "security culture".

2.3.2 Subjective norms

Subjective norms have been used to explain many different types of behavior, and several previous studies have confirmed the role of expectations from others on employees' security behavior. If managers, IT personnel or peers expect appropriate IS behavior, employees are more likely to engage in this type of behavior (Venkatesh et al., 2003; Herath and Rao, 2009).

2.3.2.1 Social learning

In addition to expectations deriving from subjective norms, researchers have emphasized the importance of including *descriptive norms* when discussing the role of social influence on behavior. IS behavior will be improved if it is demonstrated by people in the organization (Sheeran and Orbell, 1999; Rivis and Sheeran, 2003). Lee and Larsen (2009) found that this pressure to perform a certain behavior is even stronger when it is demonstrated by people that are considered to be important. This is referred to as *peer influence.* These findings align with the implications of *social learning theory* developed by Bandura (1977). Central in social learning theory is that learning can happen through observation of other people's behavior, which is a process referred to as *modeling* (Bandura, 1977).

According to Manz and Sims Jr. (1981), the setting in which the learning takes place has a significant impact on its effectiveness, arguing that modelling that occurs in informal, everyday situations is one of the most critical components to successful learning. Applying this perspective to IS suggests that employees are influenced by whether their managers and peers demonstrate appropriate IS behavior. Thus, if concern about IS is generally accepted among employees, the *normative beliefs* may be formed as a result of an organizational norm or culture, which increases the chances of appropriate employee IS behavior.

2.3.2.2 Security culture

Security culture refers to the set of shared values and beliefs people in an organization have about IS (Veiga and Martins, 2015). Schlienger and Teufel (2002) highlights four main focus areas for establishing a security culture: (1) artefacts and creations, (2) collective values, (3) norms and knowledge and (4) basic assumptions and beliefs. The authors further suggest that: *"Security culture should support all activities in such a way that information security*

becomes a natural aspect in daily activities of every employee." (Schlienger and Teufel, 2002, p.7). The importance of security culture has been acknowledged by several researchers (Schlienger and Teufel, 2002; Vroom and von Solms, 2004; Hu et al., 2012). For example, studies have shown that an organization's IS efforts are likely to be unsuccessful unless a security culture is embedded in the organizational culture (Chia et al., 2003). Many people underestimate their vulnerability to IS incidents since they might not have experienced it before. By establishing a security culture, a gradual change of employee behavior can be achieved, rather than forcing employees to comply with ISP, which is likely to cause resistance (Vroom and von Solms, 2004).

2.3.3 Perceived Behavioral Control

Fishbein and Ajzen (2010) assert that favorable attitudes and social norms are not always sufficient to increase the intention to perform a behavior. In addition to those constructs, intentions are further influenced by perceived behavioral control. This last construct of TPB relates to *"people's perception of the ease or difficulty of performing the behavior of interest"* (Ajzen, 1991, p. 183). The construct is described as the extent which people believe that they are capable of performing a given behavior, and is built on Bandura's (1997) concept of *self-efficacy*.

2.3.3.1 Self-efficacy

Bandura's (1997) social cognitive theory about self-efficacy, is the term used in IS literature to describe the extent to which users perform a specific action. In this study, this refers to the skills and knowledge that are required to protect the organization's information (Woon et al., 2005; Pahnila et al., 2007). Ifinedo (2012) found that if an individual believes in their own ability to protect the organization through preventive security measures and IS precautions, this will have a positive impact on their security behavior. Several other researchers have confirmed this view and agreed that there is a direct relationship between self-efficacy and individuals' security practices (Rhee et al., 2009; Vance et al. 2012)

In previous studies, a positive relationship between self-efficacy and an individual's level of knowledge has been established (Woon et al., 2005). Employees are more likely to engage in IS behavior if their knowledge of IS is high. The users must have a good understanding of the security risks (threats and vulnerabilities) to the company's information assets, and the level of security inside the organization (Von Solms, 1999; Van Niekerk and Von Solms, 2010). Similar to what has been suggested for improving attitudes to IS, research has concluded that managers should encourage employees to develop the necessary skills to protect the organization's IS assets. They also highlight the importance of making users understand the potential damage of IS attacks (Ifinedo, 2012; Herath and Rao, 2009) and the need for technical education on IS, as this would improve employees' competence and ability (Siponen, 2000).

3. Methodology

3.1 Choice of method and research approach

3.1.1 Research strategy

The study is based on an abductive approach where theory and empirical data were collected in parallel during the course of the research, which allowed us to ensure the empirical data and theoretical framework were closely connected (Bell et al. 2019). As the data collection began, we found that our data fitted well with the constructs in TPB, which was used to develop an initial theoretical framework. The initial framework was then modified as new empirical and theoretical insights were gained, extending our theoretical framework with additional theory that we identified through analysis of our empirical data. This process of going back and forth between the data, theory and analysis enabled us to ensure the fit between theory and reality (Tavory and Timmermans, 2014), which would not have been possible with a pure inductive or deductive research method. It also enabled collection of relevant empirical data, as our interview questions could be adapted on the basis of supplementary theory.

Because our aim with this study is to explore what perception and ideas employees in the three largest Swedish banks have on how IS behavior can be enhanced, we chose a qualitative research strategy. This allowed us to capture the respondents' subjective experiences of current IS efforts and their individual belief of what else that should be done. Thus, the study takes off in a constructivist ontology which reflects the social reality of each individual, as opposed to the natural reality (Bell et al., 2019). Our focus on understanding employees' views and interpretations of effective IS efforts, further motivates our interpretive epistemological position. Combining a qualitative and quantitative approach could potentially have strengthened the evidence around the factors that influence the employees' IS behavior in the Swedish banking sector, but given the magnitude of that research approach we consider the qualitative research strategy to be the most effective in the scope of a bachelor's thesis and to answer our research question.

3.1.2 Research design

The interviews performed for the purpose of this study have been of semi-structured character which allowed the respondents to prioritize which answers they consider most central (Bell et al. 2019). This was essential for our study as it enabled us to create the general understanding by which the study's paradigm is characterized. In line with the purpose of semi-structured interviews, the questions were flexible and open in their nature to allow room for the respondent to develop their thoughts. Unlike with structured interviews, this made it possible for the respondents to guide us to new themes related to IS behavior that we had not previously thought of. We are aware that this might impact the comparability between the respondents to some extent. However, we believe that the predetermined questions in our interview guide were sufficient to reduce this deficiency, while it at the same time allowed for the respondents to present their personal thoughts on IS behavior.

We have chosen to perform a cross-sectional study to explore what employees in the Swedish banking sector believe is needed to enhance IS behavior, where data is collected from more than one case and at a single point in time. As our focus is not to examine the cases in their unique context, but rather to provide a more general view on what employees deem necessary to improve IS behavior, the cross-sectional study approach is preferred over a multiple-case study (Bell et al., 2019).

3.2 Selection

3.2.1 Selection of cases

As mentioned, we have decided to look at the banking sector as it is one of the industries most vulnerable to IS attacks. Based on the banks' high exposure to these types of threats, we argue that an exploration of how their employees believe IS behavior can be enhanced will offer valuable contributions to our research question. Within the frame of this study, we contacted the four major banks in Sweden (Svenska bankföreningen, 2018). Of these, three chose to participate: Handelsbanken, SEB and Swedbank. Since these banks handle the accounts for the majority of Swedes (Finansinspektionen, 2019), they have access to large amounts of money and customer data, which makes them particularly vulnerable to potential cyber attacks. This, together with the fact that they are all working actively with IS efforts, makes them suitable for our thesis. Including more banks in the study could have been beneficial in order to achieve higher generalizability in the results. However, we believe that by focusing on the three of the four major players in the Swedish banking sector, covering the majority of the Swedish banking market, the study will provide insightful implications that may be transferable to other industries.

3.2.2 Selection of respondents

In the context of this study, we have performed 16 qualitative interviews with employees at the three different banks. At each bank we have interviewed at least one person working within the Information Security department (from now onwards *IS manager* and referred to as IMX in the empirical section), and two other employees working in the organization (also *user,* referred to as UX in the empirical section). The selection of respondents was strategically made to best answer the research question (Bell et al. 2019). First, we chose to interview people at the IS department to learn about the banks' current efforts to enhance IS behavior in the organization, and hear their expert view on what else that could be done. We then wanted to add the perspective from the general employee by interviewing employees from different units and roles to see what their perspective is on how IS behavior can be enhanced, providing a more representative view of the organization. By including both of these perspectives, we gain a more general understanding and can place possible different experiences in relation to each other. In doing so, it provides a more in-depth and comprehensive analysis of what the employees in the organization believe is needed to enhance IS behavior, which helps us in answering our research question.

We used different methods to contact the respondents. The IS managers were mainly contacted through LinkedIn, as this enabled us to see what company role they had. The other employees, on the other hand, came both from LinkedIn, but also our personal network as this made it possible for us to reach more people interested in participating in our study. Considering the relatively small number of respondents in our study, we cannot present a generalizable view about how all employees in the different banks perceive the IS efforts. However, we tried to minimize this deficiency by interviewing employees from different departments and organizational levels of the banks. Moreover, we further argue that 16 interviews were still sufficient to provide valuable insight to our research question. A table of respondents, companies and divisions can be found in *appendix 1*.

3.3 Gathering of empirical data

3.3.1 Pilot study

To gain knowledge about the Swedish banking sector and IS, two pilot interviews were conducted with a Cyber Security Manager at Ernst & Young and with a Senior Risk Expert at Finansinspektionen. This gave us an insight into the current IS landscape in the banking sector and what challenges it is facing. Through these interviews, we gained a deeper interest in the human element in IS and how this risk related to employee misbehavior can be mitigated. To deepen our knowledge, we performed a wide literature review on IS behavior, which helped us identify potential theories for our theoretical framework. The pilot study also helped us discover interesting themes and knowledge gaps, which supported us in shaping our research question. More specifically, the pilot study showed that employees are the weakest link in ensuring safety of information and that organizations must achieve a change in behavior, which is what we decided to explore further. Using the material from our interviews and secondary data, an initial interview guide was formed (see *appendix 2*).

3.3.2 Interview process

All interviews were conducted by both of us with the purpose to reduce any misunderstandings, as this method allowed us to compare our interpretations of the respondents responses and reflections. During the interviews, one of us asked the questions, while the other one took notes of interesting comments and ambiguities, which could then be followed up on. By having one person leading the interview, the other one could focus on making sure that all planned themes were covered, whilst still respecting what the respondent considered most central and allowing for new themes to emerge. Most of the interviews were conducted in Swedish except for one which was made in English, based on the interviewee's preference. The interviews lasted on average for 40 minutes and took place at a location of the respondents choice, usually at their office. In order for us to record and transcribe the interview afterwards, places with minimal background noise were necessary. We wanted to avoid interviews over the phone as this could make it harder to connect with the respondents, which could affect the detail of their responses (Bell et al. 2019). However, due to unforeseen

circumstances[2], the second half of our interviews had to be made over the phone. We do not believe it had a significant impact on the results of our study as we still managed to receive broad and detailed responses. After conducting 12 interviews, we considered empirical saturation to be fulfilled as we identified repetitions of similar concepts, patterns, deviations and similarities within the empirical data. After an additional four interviews, we concluded that further interviews would not have increased the understanding of the subject.

3.4 Analysis of data

The data processing began with a transcription of the empirical material. This was done directly after the interview to ensure it was as close to the data as possible. As a result of the abductive approach of the study, the analysis of data was made based on a continuous interplay between existing theory and the empirical material, where categories were derived both from theory and data (Bell et al., 2019). As previously mentioned, the main themes were identified using the constructs of TPB, which are: (1) *attitude* (2) *subjective norms* and (3) *perceived behavioral control*. These identified themes served as the basis for our continued analysis. A further analysis of data then allowed for a number of sub-themes to emerge based on patterns in the empirical material. When coding the empirical material, we continuously and separately categorized the data to find common keywords and concepts, remaining as close as possible to the actual quotes. We then discussed the results to distinguish the sub-themes that together with the main themes would create the basis for the empirical section. Through this process we have covered all possible areas for analysis, and established a high reliability of our results. Finally, Swedish quotes were translated to English and minor alterations of the sentencing were made for ease of reading.

3.5 Discussion of methodology

3.5.1 Trustworthiness

To ensure the reliability and validity of a qualitative study, Guba and Lincoln (1985) have proposed four criterias: credibility, transferability, dependability and confirmability, all of which we have considered during our research process. To establish credibility, we made efforts to reduce any misinterpretations of what the respondent had said by always conducting the interviews together, which enabled us to discuss our interpretation afterwards. This also helped increase the study's confirmability as it reduced any personal values and made the analysis more objective. If any ambiguities arose during the interviews, we asked the respondent to clarify what they meant. Finally, to further increase the credibility, all interviews were recorded and transcribed. Overall, we argue that the credibility aspect of our thesis is strong.

The transferability aspect, on the other hand, can be hard to achieve in a qualitative research study of this size. To handle this deficiency, we have focused on creating so-called "thick

[2] In the first quarter of 2020, when this thesis was conducted, the whole world was hit by a novel Coronavirus (Covid-19) that was classified as a pandemic. To minimize contagion, people were encouraged to "social distancing", and most people were working from home.

descriptions", where quotes from the respondents are central in the presentation of the empirical material. This way, the readers can form their own judgement of whether the findings are transferable or not (Guba and Lincoln, 1985). As for dependability, we have continuously taken notes of our process, from the initial problem formulation, interview selection, interview transcripts, coding and categorization of the data.. This way we can look back at our process and make sure that proper procedures were followed.

3.5.2 Ethical implications

Each interview began with us asking the respondent for permission to record the interview. We then clarified that the recordings will only be used for the purpose of this study and not in any other context. The interviews were thereafter conducted in the language the respondent felt most comfortable with. Furthermore, considering the confidential and sensitive nature of the subject, the interviewees' have been clearly instructed before the interview that they can choose not to answer a certain question and that they at any time can discontinue the interview. The respondents names have also been anonymized, along with their specific role and what bank they work at.

4. Empirics

The empirical section will be presented with the respondents' reflections and responses in focus. By concentrating on what the interviewees said and what they chose to talk about, an understanding of what the respondents believe is important to enhance IS behavior can be created. To facilitate the reader's comprehension, we have structured the empirics based on our theoretical framework. Apart from the headings in the theoretical framework, one additional theme, *communication,* has been identified based on the empirical material.

4.1 Attitude

4.1.1 Awareness of threats

4.1.1.1 Focusing on the *why*

During the interviews, the IS managers highlighted the importance of explaining *why* employees should engage in appropriate security behavior, and what risks they take if they do not. IM4 explains: *"It is about explaining the "why" - because when they [the users] understand why they need to do it, and what kind of risks they take if they act differently, they are much more willing to do the things in a secure way."* Many of the respondents further state that it is necessary to create a sense of fright by emphasizing the organization's vulnerability to these threats: *"They are not aware that this is going on here and now, they still think it's some science fiction, so to explain it in a way that actually makes you a bit scared, but also understands that there are antidotes to it, I think that is necessary."* (IM2).

4.1.1.2 Use trainings to increase awareness

Moreover, it was a common view among the interviewees that trainings and education is needed to increase user awareness and understanding of IS, which was also something that all three banks said they engaged in: *"We have also developed a number of e-learnings, which is meant to create awareness and also 'demystify' the concept of security, because for many, it is still very much 'hocus pocus'"* (IM2). This training is mandatory and something that everyone must complete when they start working at the bank. IM5 explains: *"[We have] mandatory e-learnings and that is something that all employees must do"*.

The respondents further emphasized the need to show the implication of IS for employees and their families, and not only in their job role. This will help increase employees' understanding of why and how to protect their information, which is something they will later bring back to work: *"It is a very important aspect, I think, to start talking about the "I" - what can I do to protect myself and my family? If people get that understanding, then they can bring it with them to the workplace as well. So I think that's the winning concept."* (IM5). Furthermore it was emphasized that the interest among the employees could be improved by showing how it was applicable to an employee's everyday life and their role within the company. IM7 compares it to watching a movie: *"[...] if you watch a movie and think: this I can relate to, then in some way it will be incredibly more interesting."*

4.1.2 Communication

4.1.2.1 Make it fun

Although the respondents saw the need for training to increase employee awareness and understanding, many of the users argued that the mandatory trainings failed to create an interest among the employees. U2 argues: "*[you should] make it a little more interesting, if you can make it interesting. Maybe that's the problem."* U3 further comments: "*It is basically just something you click through, because they are very boring."* Furthermore, when reflecting back on the training they have done, the employees also had a hard time remembering what they were about, which made them believe that it was not the most effective way to learn about IS. U3 continues: *"I can't remember what was said [in the training], so it might not be the most effective way to learn. You need to get the information continuously, you have to remember it."*

4.1.2.2 Interactive training methods

Hence, the users saw the need for other types of training that would be better at creating an interest. Some of the respondents argued that the mandatory trainings should be replaced by other types of training, because people will not process the information if it is something they are forced to do, U3 suggests: *"I think you should replace them [the mandatory trainings] because I think nobody likes to do them, because everyone just does them because you have to - and then you don't learn it very well."* To improve the interest around IS awareness and behavior, the respondents saw the need for incident simulations and interactive discussions: *"[A little more] hands-on, maybe a simulation or something, I think that would make it easier to attract interest. Alternatively, you could run a workshop or something like that, which creates some more discussion."* (U1). The respondents further described that an important aspect of enhancing IS behavior is by making it more 'alive' by combining the digital trainings with in-person education: *"It should be a combination of physical and digital, we have digital material, and then we would like to do it in meetings, workshops or discussions because it always becomes more alive then."* U3 agrees and gives additional suggestions on how to make IS training more fun: *"You could have full training days where you go through everything about IT security and where everyone who works at the bank can join in. Something like that where there is more discussion and participation, which is more fun than just sitting and listening or watching a movie.*"

4.1.2.3 Tailored training

During the interviews, the IS managers emphasized the importance of making IS activities role-based and to address the different levels of the organization in different ways. IM5 explains that *"to achieve an impact on this [the company's IS efforts] you have to take the whole pyramid and you don't do that in the same way, you have to address the different parts [in the company] with different activities for it to be relevant."* IM4 agrees that the activities need to be tailored to the different roles in the company: *"[...] different kinds of activities are done for different people based on what their job roles are"*. To have role-based education was also highlighted by the users as something that can increase the interest among the

employees and make trainings less "boring". U1 explains: *"Because it is such a broad subject [it will] make people bored if they must go through each section, even what may not be relevant to you. So making them specific to your role, at least your area, will make it easier to attract interest, I think."*

4.1.3 Management support and participation

Several of the respondents emphasized that management has an important role in increasing the company's security: *"I think, if you want to increase the security, it must come from further up in the organization."* (U2). The interviewees further argued that it is important that management participate in IS efforts to show that it is important for the bank: *"The fact that the managers do not care about information security would create huge credibility problems for the programs, so everyone must take part [...] the leaders really need to underline that this is an important issue and absorb the information that is given. So it plays a huge role - the attitude that the managers have - and what they communicate down to the staff [...] you have to communicate that this is of great importance, and that it is the new big threat."* (IM1). This was further emphasized by U8 who underlined that manager engagement is essential to make employees understand the importance of IS: *"Obviously it's very important that every leader in every part of the organization takes it seriously. Because otherwise, it's hard to get employees to think it's important"*.

Some respondents explained that the CEO has made appearances in the company's mandatory e-learning, which they believe helps to show the importance of the topic: *"We have involved [the company's CEO] in our mandatory e-learning to show that this is something that is important at the bank"*. (IM5). Many of the respondents particularly emphasized the value of having local managers that are engaged in the topic and that can help carry out information about IS in their teams, as this will increase the employees' knowledge of the topic: *"[...] to create awareness around information security has a lot to do with the local manager's engagement in the issue"*. (IM3).

4.2 Subjective norms

4.2.1 Social learning

Moreover, many of the respondents remarked that managers have an important role in encouraging appropriate IS behavior because they are seen as role models to their subordinates: *"People will follow, they look at their leaders, they look at their peers as well, but if the leader, if their manager doesn't care, then why should they? It is leading by example, and it's very important."* (IM4). U5 agrees that employees' and managers' actions impact IS behavior: *"[...] unless employees or managers take it seriously then I will not put energy on it either"*. In addition, several of the respondents state that they are positively affected by their peers' and managers' behavior: *"Fortunately, I believe that most of my employees and managers follow the guidelines we have, so I am positively influenced to do the same"*. (U1). U2 continues: *"You notice that people are extremely strict about this which*

also affects my own behavior". The importance of other employees' behavior stems from what is described by respondents as a need to blend in: *"I mean we are herd animals. You want to do what everyone else does, because you don't want to stand out. So if everyone is on board, then you have no issues, but if people don't take it seriously, that's when you start to have problems."* (IM1). This further relates to what some of the interviewees refer to as building a security culture.

4.2.2 Security culture

Many of the respondents explained that IS should be something that is ingrained in the organization and an obvious part of daily work. This is further explained by the interviewees as creating a "security culture" and the respondents gave examples of how it can be achieved: *"We're talking about security culture, because that's actually what needs to change, [and] how do you change the culture? Well, it is very important that everyone has to take responsibility, as soon as we have to take a new tool, a new process, or whatever it is, then security must be a natural part of it."* (IM5). IM5 continues explaining that they have created so called security champions to help change the culture: *"We look for people that think it's interesting and are curious about security, and maybe also a good 'speaker person' out in their organisation. It does not have to be a manager, but people like this person, you listen to him or her. Then we make them 'security champions', giving them a little more education, and letting them spread the knowledge where they are in the organisation."* The interviewees also describe that the creation of a culture is something the whole corporation must engage in, and that needs to fit into the existing culture: *"It's not a one man's show, it's really the corporation that have to build this culture and it has to fit into the organizational culture."* (IM4).

A common statement in the interviews was that the IS department is there to help people do right, rather than punishing them for doing wrong. As expressed by IM1: *"There will never be a whip if you happen to make mistakes, everyone can make mistakes. After all, information security is there to help people do the right thing, not to punish people."* The importance of making IS something that engages employees, rather than something they do solely to avoid potential sanctions, was highlighted by many other of the respondents. IM4 adds: *"[...] you have to find a positive way of engaging people, rather than punishing them"*. A similar view is offered by IM7 who also goes back to the importance of making it a natural part in everyday life: *"After all, we can't point fingers and say: 'You can't do this or that, it should just sit there.' It is much better to come to something where we start talking about this more naturally in everyday life, than that security - it is a group over here that is handling that."*

4.3 Perceived behavioral control

4.3.1 Self-efficacy

4.3.1.1 Knowledge

When asked about what is needed to enhance IS behavior in their organization, some respondents emphasized the importance of making employees feel confident and comfortable in being responsible for their own and the company's IS. IM5 states: *"It's about me being an employee and feeling: I have so much knowledge that I feel that I can do my job in the most, trustworthy way, so to speak."* At the same time, the responses further indicated that most users believe they already have adequate IS knowledge and that much of how to protect yourself against security incidents is common sense. Many also explained that it is necessary to be aware of IS as it has become a part of everyday life and something that everyone must have knowledge of. U2 explains: *"[...] you will come a long way with common sense, and I believe that most people know those things [refers to IS guidelines/behavior]"*.

4.3.1.2 Trust in technical interventions

There is a common perception among the users that their organizations have good infrastructure to protect their employees from outside threats, and some users mention that they themselves rely on these systems: *"Man is perhaps the weakest link, so there must be, like, systems [...] At least I hope they exist somewhere in the background so you don't have to focus on it all the time."* (U6). Several of the IS managers point to a risk with this assumption and argue that it might have a negative impact on employees' IS behavior, as it reduces their sense of responsibility over IS. IM5 states: *"[I believe many users think] 'IT security takes care of that protection, my workplace is secure, and my mobile phone is safe because they take care of it.' But yes, we take care of the shell protection, but it is still you as an individual who receives the garbage by clicking on a link, so to speak. And it is this mindset that we have to get away from"*.

5 Analysis

In this section, the presented empirics will be analyzed in guidance of our theoretical framework, as well as the additional theme identified in the empirical section, to answer the research question of how employee IS behavior can be enhanced.

5.1 Attitude

5.1.1 Threat awareness

As reflected in the empirical material, there is a need to make employees understand *why* appropriate IS behavior is important, and what can happen if they do not exhibit this behavior. Some IS managers argued that it is necessary to create a level of fright among the employees, which could be interpreted as developing an awareness of the threats' potential consequences. In turn, this is likely to lead to more positive attitudes toward engaging in appropriate IS behavior (Bélanger et al., 2017; Lee and Larsen 2009; Pahnila et al. 2007). This emphasis on potential damages that could affect the organization aligns with what Rogers (1975) referred to as perceived threat vulnerability and severity. If employees believe security incidents might happen, and understand the devastating effects they could have, they are more likely to engage in appropriate security behavior (Lee and Larsen 2009; Pahnila et al. 2007; Herath et al.,2014). Thus, the empirical findings showed that it is important that the organizations focus on this aspect in their IS training programs, as employees otherwise tend to underestimate their own and the organization's vulnerability to these threats (Hochhauser, 2004). In addition to the theoretical basis, empirical findings emphasized the importance of making employees understand that IS relates to them on a personal level, as this would make them more inclined to change their behavior. These results are understandable as it is reasonable to assume that individuals are more inclined to ensure the security of themselves and their family, than an organization.

5.1.2 Communication

The empirical results showed that the methods used to communicate IS play an important role in creating a positive attitude around IS among the employees, and thereby in enhancing their IS behavior. In the interviews with the users, there was a mutual agreement that the current IS mandatory trainings are not effective in creating an interest among the employees and it was clear that it had a negative impact on their attitude toward IS. Many could not remember what the trainings were about, which could be assumed to have negative effects on the companies' efforts to increase threat awareness. Instead of the mandatory trainings, the interviewees suggested a more interactive two-way communication approach, highlighting the need for discussions and workshops. Additional suggestions came from the IS managers, who had also identified some issues with the mandatory trainings. However, rather than replacing the current training methods, they highlighted the need to make them role-based.

5.1.3 Management support and participation

As existing literature highlights, the empirical findings confirm that management support and participation are central elements in how employee IS behavior can be enhanced (Hu et al. 2012; Puhakainen and Siponen, 2010; Cuganesan et al., 2018**)**. The empirical data shows the importance of establishing a sense among the users that IS is highly prioritized by management, to provide a reason as to why it should be important to them (Hu et al., 2012). Furthermore, the general attitude among the respondents that *"if my manager doesn't care, why should I?"* is in line with previous literature stating that employees' opinions are strongly affected by the beliefs and practices of management (Schneider et al., 1966; Puhakainen and Siponen, 2010). As stated by Schneider et al. (1966), employees are more likely to engage in appropriate IS behavior if management publicly supports the IS initiative, which can be seen in the empirical findings where some of the banks' CEOs are involved in IS training programs. Additionally, empirical findings highlight how managers are seen as role models and that their behavior forms the behavior of others' in the organization. This could be linked to research showing that management has a significant impact on the ability to establish workplace norms and build a security culture (Hu et al., 2012).

5.2 Subjective norms

5.2.1 Social learning

There is an agreement among the respondents that other people's IS behavior, in particular that of managers, play an important role in shaping employee IS behavior. This is in line with previous literature, suggesting that individuals often experience a pressure to perform a behavior if it is demonstrated by people who are important to them, referred to as *peer influence* (Lee and Larsen 2009). This peer influence can further be seen as an expression of social learning and modeling, as mentioned by Bandura (1977), where individuals develop a certain behavior by observing the behavior of others. As existing literature highlights, modelling that occurs in informal, everyday situations, is one of the most critical components to successful learning (Manz and Sims Jr, 1981). Interviewees emphasized this as well, for instance suggesting the use of so-called 'security champions' to create informal role-models that could help develop a security culture.

5.2.2 Security culture

When interviewees were asked to describe efforts they believed are necessary to enhance IS behavior, many highlighted the importance of creating a *security culture*. To make people engage in IS practices, it has to be integrated into the daily activities of every employee (Schlienger and Teufel, 2002). If information security is not an integral part of the organizational culture, trainings and other IS efforts are unlikely to be successful (Chia et al., 2003). However, the respondents highlighted two key challenges in establishing this security culture. Firstly, you need to change people's habits. People are used to doing things a certain way and are resistant to change, since they do not believe any harm will happen to them (Roe-Berning and Straker, 1997). It is therefore essential for management to show the

organization's vulnerability to these types of threats, which relates to our previous analysis in 5.1.1. Secondly, the respondents indicated that a sense of responsibility over IS is lacking among the employees, and that the users rely on the IS department or systems and firewalls to protect the organization against possible security incidents or attacks. This could in turn affect users self-efficacy, which will be discussed next.

5.3 Perceived behavioral control

5.3.1 Self-efficacy

As mentioned, there is an agreement among the respondents that training is needed to increase employees' awareness and knowledge of IS. Employees will feel more confident in engaging with security practices if they believe that they possess the necessary skills. This relates to the concept of self-efficacy (Bandura, 1977; Pahnila et al., 2007; Ifinedo, 2012). At the same time, many of the users stated that they already have sufficient knowledge about IS, and that much of what is said in the trainings is "common sense". However, as mentioned previously, it was still evident that they rely on organizational infrastructure and management, which indicates a belief that their own actions do not have a large impact on the security of the organization. According to Rhee et al., (2009), it is therefore essential that IS professionals design training programs that are more effective in creating a sense of efficacy belief among the employees, as this will increase user's sense of responsibility over IS, and thereby enhance their IS behavior. This could further be linked to the respondents' suggestion on role-based security training, which apart from making IS more interesting, could make individual employees' role in ensuring safety of information more clearly established.

6. Discussion

6.1. Elaboration of findings

Important aspects of enhancing IS behavior were identified as threat awareness, management participation and support, social learning, security culture and self-efficacy, all of which were presented in the literature review. Apart from these, a new key aspect of improving IS behavior, communication, was identified. Potential reasons for why this particular aspect was not discovered during the literature review could be that it is not included in the research field or that it was overlooked. Another explanation could be that since previous literature has mainly taken a deductive and quantitative approach, the subjective opinions of employees on how IS behavior can be enhanced, in particular those of general employees, have not been sufficiently highlighted.

This study showed that it is essential to make employees comprehend the organization's vulnerability to potential IS incidents and raise awareness of the implications of security threats, which is supported by the findings of other researchers in the field (Lee and Larsen 2009; Pahnila et al., 2007; Herath et al., 2014). In addition, our findings suggested that when employees understand the relevance IS has for them on a personal level, they become more involved and are more likely to demonstrate appropriate IS behavior. This adds to the findings of LaRose et al., (2008), who reached similar conclusions. One of the most significant and unanticipated findings of this study is the importance of effective communication methods. Although not emphasized in IS literature, the role of communication has been considered by researchers in other fields as both necessary and effective in generating any form of organizational change (Greenberg, 1975; Greenwood and Levin, 1998). Our findings suggest that there is a need for more interactive and tailored IS efforts, as this would be more interesting than the current mandatory trainings. This is reasonable since participation-based training is likely to lead to increased motivation among employees (Greenberg, 1975), and thus an improved attitude toward IS behavior. Another important finding of this study is the role of management in influencing employee's attitude toward IS, and indirectly affecting employee IS behavior through workplace norms.

Furthermore, subjective norms have been found to have a significant influence on IS behavior by a number of previous researchers (Venkatesh et al., 2003; Herath and Rao, 2009; Lee and Larsen, 2009), and have been found as an important aspect also in this study. Our findings suggest that both managers, as well as other influential people within the organization, have an essential role in shaping IS behavior and in creating a security culture. Lastly, although our findings offered some support for the importance of perceived behavioral control and self-efficacy, it was not as emphasized as in many other IS studies (Rhee et al., 2009; Woon et al., 2005; Herath and Rao, 2009). According to the analysis, there was a gap between users' believed knowledge, and the degree to which they felt that they could protect the organization against security threats. This gap can be related to Rotter's (1966) concept of *locus of control*, suggesting that people attribute outcomes to *internal* or *external* factors

(Ajzen, 2002). The employee's perceived knowledge speaks for an internal locus of control, while the delegation of responsibility to the IS department speaks for an external. Thus, it is desirable for the organizations to have employees with an internal locus of control as those are more likely to adopt a proactive approach towards IS. The roots of the employees' external locus of control can be further explained by Seligman's (1975) theory of *learned helplessness*. The incentives for people to initiate a behavior will depend on their (learned) expectation that their actions can result in some improvement. In this case, employees might have developed the expectation that there is little they can do to positively affect the outcomes of security incidents.

An unexpected finding was that sanctions or punishments for inappropriate IS behavior should be avoided, which is in contrast to what is proposed by many other researchers such as Peace et al. (2003) and Straub (1990). Rather than sanctions, respondents highlighted the importance of explaining to employees how appropriate IS behavior may benefit them, which can be seen as a type of reward-strategy. This finding is consistent with those of Hu et al. (2011), suggesting that the perceived benefits of engaging in IS behavior dominate the perceived risks of misconduct.

These findings, which support the role of *attitude, subjective norms* and *perceived behavioral control* in encouraging a certain behavior, confirms those of previous research (Ifinedo, 2012; Pahnila et al., 2007; Peace et al., 2003; Bulgurcu et al., 2010). It also suggests a strong generalizability and robustness of the TPB theoretical framework.

7. Conclusion

7.1 Addressing the research question

Through a qualitative study, we have explored what IS managers and general employees believe is necessary to enhance employee IS behavior in the Swedish banking sector. The empirical data has been analyzed through our theoretical framework based on the *Theory of Planned Behavior* (Ajzen, 1985) with the purpose of answering the following research question:

"How can employee IS behavior be enhanced?"

Based on the empirical and theoretical findings that were analyzed in this thesis, the research question is considered to have been answered. Aspects that influence IS behavior have been identified through theory and confirmed and modified through in-depth interviews with employees at the banks. Through our cross-sectional study, it was shown that *threat awareness, communication, management participation and support, social learning, security culture* and *self-efficacy,* which all impact the constructs of TPB, are important aspects in enhancing employee IS behavior. These are considered key findings as they give suggestions on how the human risk in IS can be mitigated, which is an important issue for today's organizations (Ifinedo, 2012; Stanton et al., 2004). The presented aspects, as well as how they influence the constructs of TPB, are visualized in the following figure.

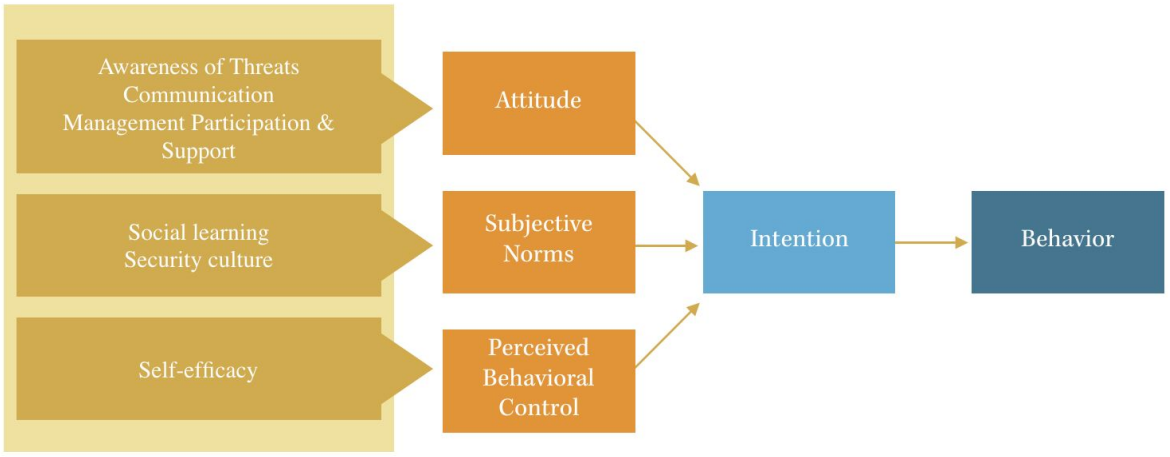

Figure 1: Aspects that positively impact employees' IS behavior

7.2 Theoretical implications

Our findings provide several theoretical implications. First, it adds to the credibility of TPB in explaining employee IS behavior, as it shows the significance of attitude, subjective norms and perceived behavioral control in enhancing security behavior among employees. Second, similarly to theories and literature applied in this research, our findings indicate that IS behavior is affected by threat awareness, management support and participation, social learning, security culture and self-efficacy, which in turn has been proved to impact the constructs in TPB. Third, the research emphasizes the importance of effective communication methods in enhancing IS behavior in organizations, which could be of interest for future studies to explore further. Lastly, by including the views of both IS managers and users, this study gives a representative view on how employees believe appropriate IS behavior can be encouraged. This has been argued by previous research to be necessary to enhance insight (Herath and Rao, 2009; Lee and Kozar, 2005).

7.3 Managerial implications

From a practical standpoint, our findings offer suggestions for how to design effective information security interventions, which may also be of value for organizations in other industries than the banking sector. Furthermore, as mentioned in our expected contribution, we have also given the perspective of the general employee, which so far has been lacking in IS literature. This is of great interest for IS managers and departments as they can see whether their efforts match employee preference. Finally, by showing how the risk related to the human aspect of information security can be mitigated, our findings might help organizations *strengthen* what is currently considered to be the *weakest* link in ensuring safety of information.

7.4 Limitations

One limitation to our thesis is that it is based on a qualitative study of the largest Swedish banks, making the empirical data highly specific. A second limitation to the study is that it is made within the interpretivist paradigm with the respondents subjective view in focus. Thus, the interpretation of an answer can only be directed towards that particular respondent. Another important limitation of this thesis is that the study is dependent on the context, situation and time, especially since IS is a relatively new area that is growing quickly. Many organizations have recently started working with these efforts, and what is considered to be most effective to improve IS behavior will likely change over time as the threat landscape evolves.

7.5 Future research

Our findings provide a wide range of possibilities for future research in the field of IS behavior. Since this thesis only highlights how to enhance IS behavior among general employees, future research might focus on certain user perspectives such as different

personality types. In addition, to increase knowledge in this area, future studies could also examine the views of contractors and other staff that different organizations might employ. Furthermore, due to the relatively limited scope of this study, both in terms of selection of respondents and number of companies, we also suggest that our findings are further tested and applied to larger studies, maybe also in other industries and countries. This would further increase the transferability and generalizability of the study and increase the trustworthiness of its results.

8. References
8.1 Literature

Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior*. J Kuhl, J Beckmann (Eds.), Action-control: From cognition to behavior, Springer, Heidelberg (1985), pp. 11-39

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50, pp. 179-211

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology. 32. 665 - 683. 10.1111/j.1559-1816.2002.tb00236.x.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections' *Psychology & Health*, 26, 1113-1127.

Alnatheer M., Chan T. and Nelson K. (2012). Understanding And Measuring Information Security Culture. *InPACIS 2012* (p. 144).

Anderson, C. L. and Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions, *MIS Quarterly*, 34(3), pp. 613-A15. doi: 10.2307/25750694.

Ayuso, P. N., Gasca, R. M. and Lefevre, L. (2012). FT-FW: A cluster-based fault-tolerant architecture for stateful firewalls, *Computers & Security*, 31(4), pp. 524–539. doi: 10.1016/j.cose.2012.01.011.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215.

Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. W.H. Freeman and Company, New York.

Bauer, S., Bernroider, E. W. N. and Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, *Computers & Security*, 68, pp. 145–159. doi: 10.1016/j.cose.2017.04.009.

Bélanger, F., Collignon, S., Enget, K. and Negangard, E. (2017). Determinants of early conformance with information security policies, *Information & Management*, 54(7), pp. 887–901. doi: 10.1016/j.im.2017.01.003.

Bell, E., Bryman, A. and Harley, B. (2019). *Business research methods*. Oxford: Oxford University Press. (pp. 3-589).

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34(3), pp. 523-A7. doi: 10.2307/25750690.

Chia, P., Maynard, S.B. and Ruighaver, A.B., (2003). Understanding Organizational Security Culture. In: M.G. HUNTER and K.K. DHANDA, eds, *Information Systems: The Challenges of Theory and Practice. Las Vegas, USA: Information Institute, .*

Choo, K-KR. (2011). The cyber threat landscape: challenges and future research directions. *Computers & Security* 30(8), pp. 719-731

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, 28, 1849-1858

Cuganesan, S., Steele, C. and Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy, *Behaviour & Information Technology*, 37(1), pp. 50–65. doi: 10.1080/0144929X.2017.1397193.

D'Arcy. J., Hovav, A. and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, 20(1), pp. 79–98. doi: 10.1287/isre.1070.0160.

Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal* 16(3), 293–314.

Finch, J. & Furnell, S. & Haskell-Dowland, P. (2003). Assessing IT Security Culture: System Administrator and End-User Perspectives.

Fishbein, M. & Ajzen, Icek. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fishbein, M., Ajzen, I. (2010). Predicting and Changing Behavior. *New York: Psychology Press*, doi.org/10.4324/9780203838020

Forcht, K.A. (1994). *Computer Security Management*, Boyd & Fraser, Danvers, MA.

Greenberg, E. (1975). The consequences of worker participation: a clarification of the theoretical literature. *Social Science Quarterly*, 56(2), 191-209.

Greenwood, Davydd J. and Levin, Morton. (1998). *Introduction to Action Research: Social Research for Social Change*. London: Sage Publications.

Hansen, JV., Lowry, PB., Meservy, R. and McDonald, D. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems 43(4):1362-74.

Herath, T. and Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations, *European Journal of Information Systems*, 18(2), pp. 106–125. doi: 10.1057/ejis.2009.6.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. & Rao, H.R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service, *Information Systems Journal,* 24(1), pp. 61–84. doi: 10.1111/j.1365-2575.2012.00420.x.

Hochhauser, M. (2004). Smart Executives, Dumb Decisions, *Risk Management* (00355593), 51(9), p. 64.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture* Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture, *Decision Sciences*, 43(4), pp. 615–660. doi: 10.1111/j.1540-5915.2012.00361.x.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011) Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?, *Communications of the ACM*, 54(6), pp. 54–60. doi: 10.1145/1953122.1953142.

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

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition, *Information & Management*, 51(1), pp. 69–79. doi: 10.1016/j.im.2013.10.001.

Khosrow-Pour, M., (2015). *Encyclopedia of Information Science and Technology*, Third edn. IGI Global. (p. 3333)

Knapp, KJ., Marshall, T., Rainer, RK and Ford, FN. (2005) Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness (ISC)2 Inc., Palm Harbor, Florida and Auburn University, Auburn, Alabama.

LaRose, R., Rifon, N. J. and Enbody, R. (2008). Promoting personal responsibility for internet safety, *Communications of the ACM*, 51(3), pp. 71–76. doi: 10.1145/1325555.1325569

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014). Information security awareness and behavior: a theory-based literature review, *Management Research Review*, 37(12), pp. 1049–1092. doi: 10.1108/MRR-04-2013-0085.

Lee, Y. and Kozar, K. A. (2005). Investigating Factors Affecting the Adoption of Anti-Spyware Systems, *Communications of the ACM*, 48(8), pp. 72–77. doi: 10.1145/1076211.1076243.

Lee, Y. and Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software, *European Journal of Information Systems*, 18 (2), pp. 177-187

Lincoln, Y.S. & Guba, E. (1985). Naturalistic inquiry. Beverly Hills, CA: Sage.

Manz, C. C. and Sims Jr., H. P. (1981). Vicarious Learning: The Influence of Modeling on Organizational Behavior, *Academy of Management Review*, 6(1), pp. 105–113. doi: 10.5465/AMR.1981.4288021.

Mclaughlin, Mark-David & Gogan, Janis. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*. 17. 237-262.

Ng, B. & Kankanhalli, A. & Xu, Y.. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*. 46. 815-825.

Norton, J. and Walker, G. (2014). *Banks: Fraud and Crime*. Second Edition edn. Informa Law from Routledge.

Pahnila, S. & Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. 156b - 156b. 10.1109/HICSS.2007.206.

Peace, A. G., Galletta, D. F. and Thong, J. Y. L. (2003). Software Piracy in the Workplace: A Model and Empirical Test, *Journal of Management Information Systems*, 20(1), pp. 153–177. doi: 10.1080/07421222.2003.11045759.

Puhakainen, P. and Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, *MIS Quarterly*, 34(4), pp. 767-A4.

Rhee, H.-S., Kim, C. and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior, *Computers & Security*, 28(8), pp. 816–826. doi: 10.1016/j.cose.2009.05.008.

Rivis, A. and Sheeran, P. (2003). Descriptive Norms as an Additional Predictor in the Theory of Planned Behaviour: A Meta-Analysis, *Current Psychology*, 22(3), pp. 218–233. doi: 10.1007/s12144-003-1018-2.

Roe-Berning, S. and Straker, G. (1997). The Association Between Illusions of Invulnerability and Exposure to Trauma. *J Trauma Stress* 10, 319–327.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change, *Journal of Psychology*, 91(1), p. 93. doi: 10.1080/00223980.1975.9915803.

Rotter, J.B. (1966). Generalized expectancies of internal versus external control of reinforcements, *Psychological Monographs:General and Applied,* 80(1):1-28.

Safa, N.S., Soohak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, pp. 65-78.

Safa, N.S., Von Solms, R. and Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, pp. 1-13.

Salminen, M. and Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North. *Polar Record*, 54(2), pp. 108-118.

Schlienger, Thomas & Teufel, Stephanie. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security Management. 191-202.

Schneider, B., Brief, A. P. and Guzzo, R. A. (1996). Creating a Climate and Culture for Sustainable Organizational Change, *Organizational Dynamics*, 24(4), pp. 6–19. doi: 10.1016/S0090-2616(96)90010-8.

Seligman, M.E.P. (1975). *Learned Helplessness.* San Francisco, CA: W.H. Freeman.

Sheeran, Paschal & Orbell, Sheina. (1999). Implementation intentions and repeated behaviour: Augmenting the predictive validity of the theory of planned behavior. *European Journal of Social Psychology - EUR J SOC PSYCHOL*. 29. 349-369. 10.1002/(SICI)1099-0992(199903/05)29:2/33.0.CO;2-Y.

Siponen, Mikko. (2000). Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*. 8. 31-41.

Siponen, M. & Vance, A. O. (2010). Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487-502.

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*. 22. 10.1108/IMCS-08-2012-0045.

Spears, J. L. and Barki, H. (2010). User Participation in Information Systems Security Risk Management, *MIS Quarterly*, 34(3), pp. 503-A5. doi: 10.2307/25750689.

Stanton, J. & Mastrangelo, P. & Stam, K. & Jolton, J. (2004). Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. Proceedings of the 10th Americas Conference on Information Systems. 175.

Straub Jr., D. W. (1990). Effective IS Security: An Empirical Study, *Information Systems Research*, 1(3), pp. 255–276. doi: 10.1287/isre.1.3.255.

Straub, D.W. and Collins, R.W. (1990). Key information issues facing managers: software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly* 14(2), 143–156

Tavory, I., & Timmermans, S. (2014). *Abductive analysis: Theorizing qualitative research*. University of Chicago Press.

Vance, A., Siponen, M. and Pahnila, S. (2012) 'Motivating IS security compliance: Insights from Habit and Protection Motivation Theory', *Information & Management*, 49(3/4), pp. 190–198. doi: 10.1016/j.im.2012.04.002.

Van Niekerk, J. F. and Von Solms, R. (2010). Information security culture: A management perspective, *Computers & Security*, 29(4), pp. 476–486. doi: 10.1016/j.cose.2009.10.005.

Veiga, A. and Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study, *Computers & Security*, Volume 49, March 2015, Pages 162-176,

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View, *MIS Quarterly*, 27(3), pp. 425–478. doi: 10.2307/30036540.

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security* 7/1 [1999] 50-57.

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

Warkentin, M. and Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), pp. 101-105.

Woon, Irene & Tan, Gek & Low, R.T.. (2005). A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of the Twenty-Sixth International Conference on Information Systems.

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

Zafar, H. & Clark, J.G.. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*. 24. 557-596.

Öğütçü, G., Testik, ÖM. and Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, pp. 83-93.

8.2 Electronic sources and reports

EY (2018). *Is Cybersecurity About More Than Protection?* EY Global Information Security Survey 2018–19. Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf (Accessed 26 March 2020)

Finansinspektionen (2014). Finansinspektionen's Regulatory Code FFFS 2014:5, 17 April 2014. Available at: https://www.fi.se/contentassets/a8d558e3a0074cc796c4c23f6e6b3f53/fs1405_eng.pdf (Accessed: 27 March 2020)

Finansinspektionen (2019). *Bankbarometer*, 11 October 2019. Available at: https://www.fi.se/contentassets/fe3afcf530f9413ebe0c13a6423d51cd/bankbarometern-oktober-2019.pdf (Accessed: 16 April 2020)

Svensk Bankmarknad (2019). *Bankerna i Sverige.* Svenska Bankföreningen. Available at: https://www.swedishbankers.se/fakta-och-rapporter/svensk-bankmarknad/bankerna-i-sverige/ (Accessed: 31 March 2020)

9. Appendix

Appendix 1 - List of respondents

Name	**Bank**	**Sex**	**Division**	**Setting**	**Date**
IM1	Bank C	Male	IS division	In person	05-03-20
IM2	Bank C	Male	IS division	In person	09-03-20
IM3	Bank B	Male	IS division	Telephone	30-03-20
IM4	Bank A	Female	IS division	Telephone	06-03-20
IM5	Bank C	Female	IS division	Telephone	03-04-20
IM6	Bank A	Male	IS division	In person	28-02-20
IM7	Bank C	Male	IS division	In person	04-03-20
IM8	Bank A	Male	IS division	Telephone	18-03-20
U1	Bank A	Male	Sales	Telephone	19-03-20
U2	Bank C	Male	Structured Finance	Telephone	19-03-20
U3	Bank B	Female	Customer Advising	Telephone	27-03-20
U4	Bank A	Male	Customer Advising	Telephone	27-03-20

U5	Bank B	Male	Corporate Banking	Telephone	20-03-20
U6	Bank B	Male	Private Banking	In person	10-03-20
U7	Bank C	Male	Customer Advising	Telephone	17-03-20
U8	Bank A	Male	Private Banking	In person	04-03-20

Appendix 2 - Initial Interview Guide

Part 1: Background/Introduction

- ➢ Could you give a short presentation of yourself and your role?
- ➢ What does a normal day look like for you?

Part 2: The bank's IS efforts

Environment:

- ➢ How would you describe the current IS environment/level of cyber threats in the industry you work in?

Activities, trainings and activities:

- ➢ What does the company's efforts around the human aspect of information security look like?
- ➢ Which of these efforts do you see as most important?
- ➢ Is there anything you think the company could do more?
- ➢ Has the bank's information security efforts changed over time? How?
- ➢ How does the way of working with IS at your current workplace compare to previous jobs you have had?

Policys:

- ➢ What does the bank's information security policy look like?
- ➢ What do you think determines whether an employee complies with information security policy or not?

Employee awareness and attitude:

- ➢ To what degree would you say that you are aware of the company's work and policies regarding information security?
- ➢ Do you think that information security efforts are important? Why/why not?

- ➢ What is the company doing to increase the awareness of information security among the employees?
- ➢ Who is responsible for the company's information security?

Part 3: Top management and leaders' impact on information security

Top management:

- ➢ How important do you think the management believes information security is?
- ➢ What role do you think top management has in enhancing information security behavior?
- ➢ Can you give an example of how management has handled previous incidents?
- ➢ Is there anything regarding information security that you think management should improve?

Communication:

- ➢ What does the communication of information security incidents look like at the company?
- ➢ How do you think they should be communicated?

Role of managers/leaders:

- ➢ What is the role of managers or other leaders in enhancing information security behavior among employees?
- ➢ How does manager/leader behavior affect employees' information security behavior?
- ➢ What leadership do you think is needed to create awareness of information security among employees?
- ➢ Are there any aspects that are more important than others?

Part 4: Conclusion

- ➢ In one sentence, what would you suggest to improve the company's information security?
- ➢ Is there something you would like to add?/Something we have missed?
- ➢ Do you have any questions for us?
- ➢ Is it okay if we contact you again if we have any further questions?