LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Securing the Front Line: The Role of Employee Training in Mitigating Cyber Threats in Financial Institutions

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik.

Författare: Kamal Mansour
Tea Benic

Handledare: Niki Chatzipanagiotou, PhD - Senior Lecturer

Rättande lärare: Välj ett objekt.
Välj ett objekt.

Securing the Front Line: The Role of Employee Training in Mitigating Cyber Threats in Financial Institutions

ENGELSK TITEL: Securing the Front Line: The Role of Employee Training in Mitigating Cyber Threats in Financial Institutions – SVENSK TITLE: Säkra frontlinjen: Anställdas utbildnings roll för att mildra cyberhot i finansiella institutioner.

FÖRFATTARE: Kamal Mansour, Tea Benic

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: Maj, 2024

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 48

NYCKELORD: Information Systems (IS) Security, Cybersecurity, IS Security Training Programs, Banking Sector, Employees Training, Qualitative Research

ABSTRACT:
This bachelor’s thesis explores the effectiveness of cybersecurity training programs within a Swedish financial institution, utilizing the Theory of Planned Behavior (TPB) as the guiding theoretical framework. The research employed a qualitative approach, conducting an online survey with 28 bank employees to gain in-depth insights into their experiences and perceptions.
The findings reveal several key insights: strong organizational support for the training programs, enhanced employee understanding of cybersecurity risks, a preference for diverse training approaches, and a high level of employee engagement. The findings further show the alignment of the training initiatives with the TPB, highlighting the positive influence on employees' attitudes, subjective norms, and perceived behavioral control. The bachelor’s thesis study makes significant contributions to the existing research on cybersecurity training

effectiveness in the financial sector. The insights gained can help organizations design and implement more impactful training programs that resonate with employees and foster a security-conscious environment. The research also presents possibilities for future research, such as longitudinal studies. Overall, the bachelor's thesis offers a comprehensive understanding of the factors that contribute to the success of cybersecurity training programs.

Sammanfattning:
Denna kandidatuppsats utforskar effektiviteten av cybersäkerhet utbildningsprogram inom en svensk finansinstitution, med användning av teorin om planerat beteende (TPB) som det vägledande teoretiska ramverket. Forskningen använde en kvalitativ metodik och genomförde en online-enkät med 28 bankanställda för att få djupgående insikter om deras upplevelser och uppfattningar. Resultaten avslöjar flera nyckelinsikter: starkt organisationsstöd för utbildningsprogrammen, förbättrad anställdas förståelse för cyber säkerhetsrisker, ett önskemål om mångfald i utbildningsinsatser och en hög nivå av anställdas engagemang. Resultaten visar även på en överensstämmelse med utbildnings initiativen och TPB, vilket framhäver det positiva inflytandet på anställdas attityder, subjektiva normer och upplevd beteendekontroll. Kandidat Uppsatsens studie bidrar avsevärt till den befintliga forskningen om effektiviteten av cybersäkerhet utbildning i finanssektorn. Insikterna som vunnits kan hjälpa organisationer att utforma och implementera mer inverkansrika utbildningsprogram som resonerar med anställda och främjar en säkerhetsmedveten miljö. Forskningen presenterar även möjligheter för framtida forskning, såsom longitudinella studier. Sammantaget erbjuder kandidatuppsatsen en omfattande förståelse för de faktorer som bidrar till framgången för cybersäkerhet utbildningsprogram.

Acknowledgments

We would like to express our gratitude to our supervisor, Niki Chatzipanagiotou, for guiding us through the research process. We are deeply appreciative of your major contribution, knowledge, and support of our work. Additionally, we would like to thank the respondents who generously gave their time and willingly participated in this study. Your valuable insights and willingness to contribute have been instrumental for the success of this research. Thank you for being an integral part of this bachelor's thesis.

May, 2024

Tea Benic & Kamal Mansour

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

In today's banking and financial world, information systems play a crucial role in facilitating transactions between banks and customers. The increased reliance on digital platforms, such as online banking, which makes up 84% of transactions in Sweden are conducted online (Statista, 2020), makes clear that information systems are essential to everyday processes. With these numbers the digital age presents unprecedented challenges for financial security, emphasizing the need for strong cybersecurity measures.

Cybersecurity has emerged as a pressing concern for financial institutions, given the increasing frequency of cyber threats. These threats not only threaten sensitive financial information but also undermine the trust and confidence of customers in the financial system. Therefore, mitigating cyber threats has become a top priority for financial institutions globally (IMF, 2024).

The intersection of the financial sector with cybersecurity presents unique challenges that require careful consideration and strategic planning. While technological advancements have strengthened the capabilities of financial systems, they have also introduced new vulnerabilities and risks. Addressing these challenges requires a multifaceted approach that includes both technological solutions and the human element (BIS, 2020).

The human element in cybersecurity, particularly the role of employee training, has emerged as a vital factor in mitigating cyber threats in financial institutions. According to the 2024 Thales Global Data Threat Report, for the second year in a row, human error remains the leading cause of data breaches, with 31% of enterprises identifying it as the main underlying factor. Therefore, equipping employees with the necessary knowledge and skills to identify and respond to cyber threats is essential for enhancing the overall security posture of financial institutions.

1.2 Problem identification and Previous research

Despite the increasing emphasis on cybersecurity within the financial sector, organizations continue to face significant challenges in effectively mitigating cyber risks (American Bankers Association, 2024). Among these challenges, the role of employee training in bolstering cybersecurity defenses remains a key point of discussion. While financial institutions invest resources in training programs aimed at enhancing employees' awareness and skills in cybersecurity, questions continue regarding the effectiveness of these initiatives in reducing cybersecurity risks.

Daengsi et al. (2021) highlight that technology-based employees in an organization showed significant improvement in cybersecurity awareness after undergoing phishing attack simulations, indicating the potential effectiveness of practical, scenario-based training in enhancing cybersecurity awareness. Additionally, research has explored the relationship between organizational culture and cybersecurity practices, emphasizing the importance of fostering a security-first culture within organizations. While technical measures are crucial, neglecting the role of organizational culture can hinder effective cybersecurity (Willie, 2023). One of the key areas of concern is the influence of organizational culture on the outcomes of employee training programs. Organizational culture encompasses the shared values, beliefs, and norms that shape employees' attitudes and behaviors within an organization. However, the extent to which organizational culture supports or hinders the effectiveness of cybersecurity training remains unclear. Understanding the interplay between organizational culture and employee training is crucial for designing tailored training strategies that resonate with employees and foster a culture of cyber resilience.

Wu He et al. (2020) stress the importance of integrating self-relevant information in cybersecurity training, suggesting that training materials closely aligned with employees' personal and professional contexts are more effective in motivating secure behaviors. Furthermore, there is a need to assess the efficacy of existing training sessions in minimizing cybersecurity risks within financial institutions. While training programs aim to equip employees with the knowledge and skills necessary to identify and mitigate cyber threats, it is essential to evaluate their impact on employees' behaviors and organizational security posture. Without a comprehensive understanding of the effectiveness of training sessions, financial institutions may struggle to develop targeted and impactful cybersecurity strategies. Wu He. (2020) suggest that cybersecurity awareness programs that are engaging and include self-relevant information significantly improve employees' risk perception and cybersecurity behaviors, thereby enhancing the organization's overall security posture.

While there is a substantial body of research on cybersecurity practices and technologies, the existing literature lacks a comprehensive understanding of how organizational culture can impact the effectiveness of cybersecurity measures within organizations. This represents an important gap, as studies have highlighted the crucial role that human factors and cultural dynamics play in shaping an organization's overall cybersecurity posture. The financial sector, in particular, is an industry that faces significant cyber threats and would benefit from further research in this area.

1.3 Research Purpose and Research Questions

In light of the crucial role that human factors and organizational culture play in the cybersecurity defenses of the financial sector, our bachelor’s thesis purpose is to examine how these elements interact to influence the effectiveness of cybersecurity training programs. Consequently, the aim of the bachelor’s thesis is to reduce cyber risks and enhance the overall cybersecurity posture within the financial sector. To reply to the aforementioned purpose and aim, the following research question is formulated:

What role does organizational culture play in the effectiveness of employee training to reduce cyber risks and improve the overall cybersecurity posture within the financial sector?

1.4 Delimitations

The limitations of our bachelor's thesis mainly come from who we talked to and where we did our research. We carried out this study in the Swedish context, focusing specifically on people working at financial institutions. More specifically, we used as our example of the financial sector a local Swedish bank. Because of this, what we found out might not apply to other places or countries.

2 Literature Review

In this chapter, we outline the process of our literature review search, and present the outcomes of the literature review as main concepts of our bachelor's thesis. We also present the theory of Planned Behavior which is used in later chapters to interpret and discuss our findings. We complete this chapter with our conclusions drawn from the literature review findings.

2.1 Search procedure

To conduct our research on the effectiveness of cybersecurity training within the financial sector, specifically focusing on a case study of a local bank in Sweden, we embarked on a systematic literature review. We accessed various scholarly databases in the field of information systems and cybersecurity through Lund University Library's website, supplemented by searches on Google Scholar. Our search was centered around keywords such as "cybersecurity training effectiveness," "organizational culture in cybersecurity," "employee behavior towards cyber threats," and "cyber risk reduction in financial institutions." These keywords were utilized either individually or in conjunction with Boolean operators such as AND and OR.

We restricted our search to journal articles and conference papers, prioritizing content published in the English language. Recognizing the rapid evolution in the field of cybersecurity, we aimed to focus on literature published within the last decade to ensure the relevance and timeliness of our sources. However, we remained open to including seminal works and crucial studies predating this period if they offered foundational insights or addressed gaps in recent research. Our literature review search concluded the following articles as shown below in table 1.

Table 1. Literature Review Overview

Article	Source	Motivation
Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P. and Utakrit, N. (2021). *A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization.*	IEEE	Helped our understanding of phishing related risks, as well as development of strategies to increase cybersecurity awareness.
Wu He, Ivan Ash, Mohd Anwar, Ling Li, Xiaohong Yuan, Li Xu, Xin Tian. (2020) *Improving Employees' Intellectual Capacity for Cybersecurity Through Evidence-Based Malware Training*	Emeral Insight	Provided insights for enhancing employees' cybersecurity knowledge.
Kim, P. (2010). *Measuring the effectiveness of information security training: A*	Directory of Open Access Journals	By incorporating the findings and recommendations from this tudy, we have been

comparative analysis of computer -based training and instructor -based training		able to provide a more comprehensive analysis of the factors that contribute to the effectiveness of the cybersecurity training programs.
Zuopeng (Justin) Zhang, Wu He, Wenzhuo Li, and M'Hammed Abdous. (2021) *Cybersecurity awareness training programs: a cost–benefit analysis framework*	Emeral Insight	This source offered beneficial perspectives regarding the impact of limited resources, organizational culture, and challenges of measurement.
Kweon, E., Lee, H., Chai, S. & Yoo, K. 2021. "The utility of information security training and education on cybersecurity incidents: An empirical evidence"	Springer Nature Journals	This source offered beneficial perspectives regarding the critical role of employee awareness and understanding in enhancing organizational resilience against cybersecurity incidents.
Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. and Stulz, R.M. (2018). *What is the Impact of Successful Cyberattacks on Target Firms?*	NBER - National Bureau of Economic Research Working Papers	This source emphasizes the understanding of the severe financial and reputational consequences that can arise from security breaches.
Chowdhury, N. and Gkioulos, V., 2021. *Cyber security training for critical infrastructure protection: A literature review.*	ScienceDirect	This study's findings that highlight the importance of customizing cybersecurity training to the specific needs and characteristics of the target sector, has helped us strengthen the recommendations and implications of this research.
Khaw, K.W., Alnoor, A., Abrrow, H.A. -, Tiberius, V., Ganesan, Y. and Atshan, N.A. (2022). *Reactions towards organizational change: A systematic literature review.*	Springer Link	Provided an insight on the role of social influence in the context of organizational change. This report strengthens the understanding of factors that can impact the success of cybersecurity training programs.

2.2 The Theory of Planned Behavior

For our analysis on the important role of employee training in enhancing cybersecurity within financial institutions, we utilize the Theory of Planned Behavior (TPB). The TPB, developed by Icek Ajzen in 1985, is a widely recognized theory for understanding human behavior in various contexts, including the adoption and implementation of security practices. It posits that an individual's behavior is directly influenced by their intention to perform that behavior, which in turn is affected by three key components: attitudes towards the behavior, subjective norms, and perceived behavioral control (Ajzen, 1991).

Attitudes towards the behavior refer to the individual's positive or negative evaluation of performing the behavior. In the context of cybersecurity training, this could include employees' perceptions of the usefulness and necessity of undergoing training programs. Subjective norms involve the perceived social pressure to engage or not engage in the behavior, which could include the influence of colleagues, organizational culture, and industry standards on an employee's decision to participate actively in cybersecurity training. Perceived behavioral control reflects the individual's perception of the ease or difficulty of performing the behavior, influenced by factors such as the availability of training resources, time constraints, and personal capability to comprehend and implement the learned practices.

Applying the TPB to our research allows us to examine the motivational factors that drive employees' engagement in cybersecurity training within financial institutions. By understanding the interplay between attitudes, subjective norms, and perceived behavioral control, we can identify leverage points for enhancing the effectiveness of training programs. This approach acknowledges that the successful implementation of cybersecurity measures is not solely contingent on the availability of technological solutions but also critically depends on the human elements within the organization.

Given that the TPB is a behavior-focused theory, it is particularly suitable for our study as it emphasizes the role of individual employees in the broader cybersecurity framework of financial institutions. This theoretical perspective provides a comprehensive lens through which to explore how various factors contribute to the adoption of cybersecurity behaviors and the overall resilience of financial institutions against cyber threats. Through the TPB, our research aims to unravel the complexities of human behavior in the context of cybersecurity, offering insights into how training programs can be designed and implemented more effectively to foster a secure digital environment within the financial sector.

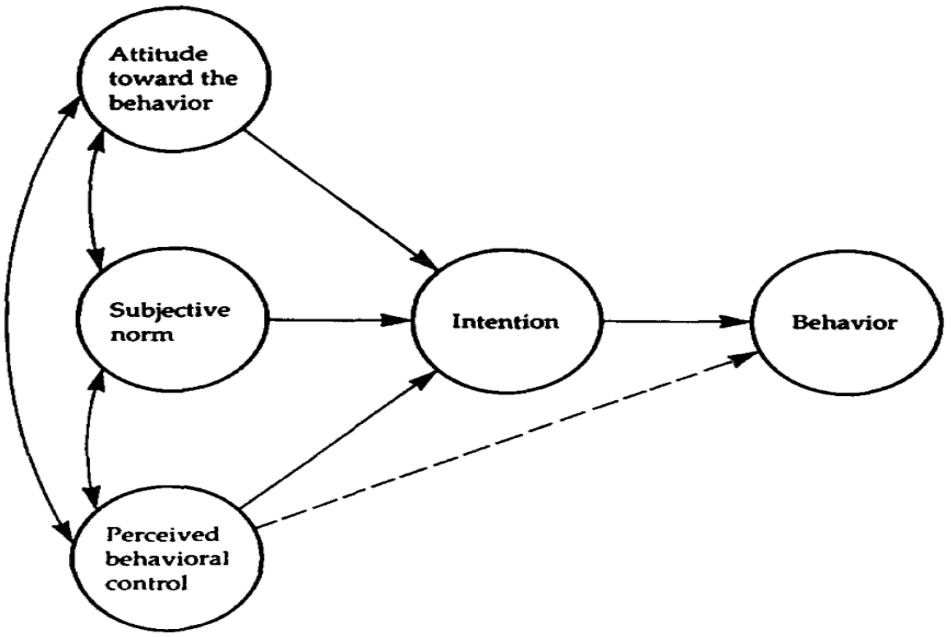

Figure 1. The Theory of Planned Behavior (Adapted from Ajzen 1991, p. 182)

2.3 Introduction to Cybersecurity in Financial Institutions

2.3.1 Overview of Cybersecurity Challenges

In Verizon's "2023 Data Breach Investigations Report," the Financial and Insurance sector's summary reveals that Basic Web Application Attacks are the leading pattern of breaches, indicating that adversaries are gaining unauthorized access with relative ease. This situation, alongside prevalent misdelivery errors, suggests a substantial opportunity for the

implementation of robust controls that could effectively mitigate a significant proportion of the cyber threats facing this industry (Verizon, 2024).

Meaning, the cyber breaches are an easy way to be used against financial institutions for personal reasons or even politically influenced where targeting institutions of this importance in the society have as little as zero cost for the issuer. Consequently, the defense of these bodies is key to preserving safety on an international scale.

However, developing robust cybersecurity defense is not a trivial task. As people are the weakest link in an organization's cybersecurity chain, every employee has the obligation to do their part in protecting the organization and thus they need to be equipped with sufficient security training and resources (Chatterjee, 2019)

2.3.2 Importance of Cybersecurity for Financial Institutions

In the banking and finance sector, the work environment is fundamentally anchored in sophisticated information systems and the essential requirement for persistent online connectivity. This infrastructure supports both employees and operational systems in their pivotal role of delivering accurate and real-time information to customers.

This leads to two principal conclusions. Firstly, addressing both software perspectives and hardware challenges specifically through robust coding practices and safeguarding against environmental breaches is crucial for system security. Secondly, the role of employees who interact with these systems, is equally significant, underscoring the importance of comprehensive security measures that encompass both technological defenses and user awareness.

When a breach of customer personal data occurs, the impacted firm typically faces significant repercussions, including a 1.1 percent loss in market value. Furthermore, there is a 3.2 percentage point decline in the year-on-year sales growth rate, highlighting the severe financial and reputational damage that can result from such security incidents (Kamiya. et al, 2018).

2.4 The Human Factor in Cybersecurity

2.4.1 Role of Employee Behavior in Cybersecurity Vulnerabilities

Any information systems need a human to operate, meaning that organizations who have any kind of information systems also have employees that handle, navigate and perform tasks on the variety of these systems. When the Employee is used as a temple to gain control over these information systems, Employees behavior then be of the most important aspects in cybersecurity.

There are independent ways to use Employees to gain control or to influence the information systems, usually the goal of these activities is according to Verizon's 2023 Data Breach

Investigations Report, the primary motivations for hacking are predominantly financial, with a staggering 97% of threat actors driven by monetary gains. These motivations are generally to acquire money, gain a competitive advantage, or disrupt an organization (Verizon, 2023). Where banks is the center of the finance in the world, with the fact that have been mentioned in the background where 84% of Sweden's banking is online (Statista, 2020), make Employees behaviors in these institutions very sensitive and have a large impact on everyday people's lives.

Incidents enabling unauthorized individuals to gain control over information systems, where they could access sensitive data including passwords, emails, transaction histories, addresses, phone numbers, previous cases, and any other information a financial institution is permitted to store, can occur through various means. One significant method is spear phishing. This is a more sophisticated and targeted variation of email phishing, utilizing personal information to compose messages that appear more authentic and credible (Charles Griffiths, 2024).

Despite appearing superficially straightforward to avoid, phishing attacks present intricate challenges in identification and detection in practice. Such attacks typically involve the distribution of emails containing deceptive messages, links, or simulated websites operated by the attacker (see Fig. 2), all designed to appear legitimate to the unsuspecting recipient (Daengsi et al., 2021). Particularly nefarious is the tactic known as spear phishing, where personal details about the target are leveraged to craft emails that convincingly mimic genuine communications, thereby increasing the likelihood of the recipient disclosing sensitive information.

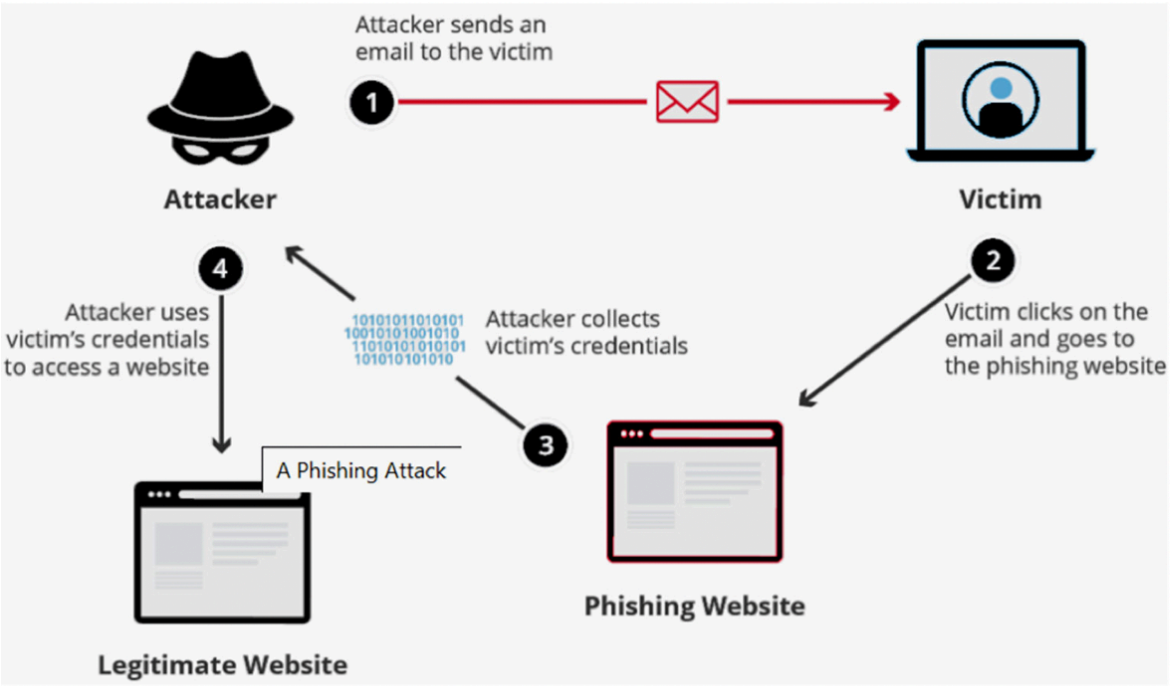

Figure. 2: Overview on phishing processes (Adapted from Chatchalermpun and Daengsi, 2021, p. 2)

2.4.2 Impact of Human Error on Security Breaches

Information security regulations, methods, and necessary safeguards must be individually understood and retained by the employee. If an employee is unaware of the policies and procedures, successful policy compliance cannot be ensured, even with the best policies and procedures in place (Kweon et al., 2021).

Phishing is similar to fishing in terms of meaning, it is an act of deception whereby impersonation is utilized by phishers to take sensitive information (e.g., user ID, email password, social networking application password and bank account number) in order to steal money from victims' bank account or credit card, or to install malware on the victims' computers or mobile devices (Daengsi et al., 2021).

Meaning by small mistakes the information system is used, manipulated and used by criminals. Which is of the highest security breach a financial institution can face, impacting the institutions so harmfully resulting in bankruptcy in worst case scenarios.

Recognizing the critical importance of cybersecurity in the realm of online banking is essential, in 2018, 35% of Chief Cyber Security Officers reported employee security education and training as the highest priority to ensure cyber security, outweighing infrastructure upgrades, breach defense, and network defense (Financial Services Information Sharing and Analysis Center, 2018).

Furthermore, cybersecurity is a crucial aspect of people in this digital age. It becomes a key defense in protection systems in organizations and users or employees that relates to the protection against cyber-attacks due to vulnerabilities and security risks (Daengsi et al., 2021).

2.5 Cybersecurity Training Programs

2.5.1 Methods of Cybersecurity Training for Employees

In this section we explore various methods employed in cybersecurity training programs within financial institutions. While there are numerous approaches, we will focus on presenting the most common methods used.

Classroom training is one of the most used teaching methods for cybersecurity awareness, and is an effective way to deliver awareness and education to users. Classroom-based instruction is often characterized as a more traditional, teacher-centered approach focused on lectures and demonstrations. One of the advantages of an instructor-led delivery method is that the instructor is able to provide real time feedback and clear communication.

Classroom training is one of the most used teaching methods for cybersecurity training awareness, and is an effective way to deliver awareness and education to users.

Classroom-based learning is often characterized as a more traditional, teacher centered approach focused on lectures and demonstrations. One of the advantages of an instructor-led delivery method is that it provides real-time feedback and clear communication (Abawajy, 2014).

Online training refers to learning on the internet rather than a physical classroom. It could include online courses, videos, training modules or discussion forums. These modules offer flexibility for the users to learn at their own pace (Means et al., 2010).

Phishing Exercises, phishing is a type of cyber-attack where cybercriminals attempt to trick individuals into revealing sensitive information, such as login credentials or financial information, by impersonating a legitimate organization or individual through deceptive emails, messages, or websites (Daengsi et al., 2021). Phishing exercises are an interactive form of cybersecurity training that allows organizations to test their employees' ability to identify and respond to phishing attempts (Chrisda, 2024).

2.5.2 Efficacy of Different Training Approaches

Studies show that certain aspects, such as the ability to share ideas, instructor rapport, and immediate feedback are valued in classroom learning. The interactive setting of classroom training allows for discussion, questions, and real-time feedback between the instructor and participants (Kumari, 2023).

Online learning also offers unique advantages for instance flexibility, allowing employees to learn at their own pace and on their own schedule, which can be particularly beneficial for those with busy schedules or geographic constraints (Means et al., 2010).

In contrast, phishing exercises provide a more practical and hands-on approach to cybersecurity training. These simulations test employees' ability to identify and respond to real phishing attempts, giving organizations valuable insights into the effectiveness of their training programs.

Research has found that phishing simulation exercises can significantly improve employees' ability to detect and report phishing emails, regardless of whether the training is delivered in a classroom or online setting (Kumaraguru et al., 2010). By exposing employees to realistic phishing scenarios, these exercises help them develop the necessary skills to protect against this common attack.

Kim (2010) discovered that while computer-based trainees had higher levels of information retention, instructor-based trainees had higher levels of learning transfer, suggesting that it would be beneficial to combine techniques. In conclusion, a combination of traditional classroom training, online learning, and phishing simulation exercises offers the most efficient approach to cybersecurity training. By combining these methods, organizations can create a

comprehensive cybersecurity training program that addresses various learning preferences and maximizes the effectiveness of training efforts.

A study conducted by Chowdhury and Gkioulos (2021) underscores the importance of tailoring cybersecurity measures to the specific needs of critical infrastructure sectors. The cybersecurity challenges and requirements vary significantly across different critical infrastructure sectors like energy, healthcare, finance, and government. This includes the necessity for sector-specific strategies, customized training programs, tailored regulatory frameworks, and collaboration among stakeholders. It emphasizes that a one-size-fits-all approach is ineffective, advocating instead for adaptive, interactive training and regulations that address the diverse cybersecurity challenges across sectors.

2.6 Factors Influencing Training Effectiveness

2.6.1 Attitudes Towards Cybersecurity Training

A person's attitude towards an object affects the overall pattern of his responses to the object, as demonstrated by the multiple studies that investigated the relation between strong attitude and subsequent behavior (Ajzen, 1991). Employees' attitudes towards cybersecurity training are a key factor in determining the effectiveness of such training programs. Positive attitudes, where employees see the value and importance of the training, are associated with better learning outcomes and increased application of the skills learned. Conversely, negative attitudes, such as viewing the training as irrelevant or burdensome, can undermine the effectiveness of the training. Various factors including organizational culture, rewards, recognition and peer pressure might impact the training participants motivation and attitudes. Therefore, understanding and addressing employees' attitudes towards cybersecurity training is essential for designing and implementing effective training within organizations (Khaw, Alnoor, AL-Abrrow, and Nguyen, 2023).

Some factors that contribute to a positive attitude are security and trust. When individuals feel secure and trust the new behavior, system, or act, they are more likely to exhibit positive attitudes towards its adoption. Furthermore, the complexity of the new behavior influences attitudes significantly. Lower perceived complexity is associated with a more positive attitude, suggesting that simplicity and ease of understanding are crucial factors in favorable attitudes towards adoption. Moreover, the perception that a new behavior offers advantages over the current approach is associated with a more positive attitude (Stieninger, 2022).

2.6.2 Subjective Norms and Social Influences

The effectiveness of cybersecurity training can also be influenced by the social setting in which it is conducted. Employees' desire to learn and implement the skills they receive during training can be influenced by social pressures from peers, supervisors, and organizational leadership. Employees are more likely to view cybersecurity training favorably and be driven to actively participate and use the skills they have gained in the workplace when they believe that their peers appreciate and support it. On the other hand, the efficiency of the training may be compromised by the social environment's lack of support or even opposition (Khaw, Alnoor, AL-Abrrow, and Nguyen, 2023).

Negative attitudes from any key stakeholders, including leaders, would impact the training's effectiveness. Resistance may discourage employees from actively engaging in training activities or prioritizing cybersecurity measures. By understanding the role of subjective norms and social influences in influencing employee behavior, organizations can implement strategies to foster a positive training environment (Khaw, Alnoor, AL-Abrrow, and Nguyen, 2023).

2.7 Challenges and Barriers to Effective Training

Limited budgets can significantly impact an organization's ability to implement comprehensive and effective cybersecurity awareness training programs, which are crucial for reducing cyber risks. Organizations must carefully allocate their resources to develop successful training programs, but budget constraints may prevent them from adopting the most optimal training approach (Zhang, 2021).

Organizational culture and peer pressure can impact the motivation and attitude of training participants. If the organization does not prioritize or support cybersecurity training, employees may be less inclined to participate actively. Secondly, the effectiveness of the training program itself can contribute to resistance (Khaw, Alnoor, AL-Abrrow, and Nguyen, 2023). Employee motivation and psychological ownership over cybersecurity practices can influence the effectiveness of security education, training, and awareness programs. If employees do not feel a sense of ownership or investment in the training, they may be more resistant to the program (Stieninger, 2022).

Additionally, a study by Wu He et al. (2023) found that employees who perceived the training as relevant and beneficial were more likely to actively engage and apply the knowledge gained. This suggests that tailoring cybersecurity training programs to address the specific needs of different employees can be an important factor in enhancing their effectiveness.

Measuring the effectiveness of cybersecurity training can also be a significant challenge. One of the primary challenges is the lack of standardization in the methods used to assess training effectiveness. The inconsistent approaches across studies make it diffiicult to compare results and draw reliable conclusions about the impact of cybersecurity training, Another significant

challenge is the difficulty in measuring behavioral change, which is a critical aspect of cybersecurity training. Awareness does not necessarily translate to behavior change, employees may demonstrate an understanding of the training content, but this knowledge may not always show in their day-to-day security practices. Addressing these challenges and aligning the training programs with organizational goals and strategies, is crucial for developing and implementing effective cybersecurity training programs that can enhance the overall security posture of the organization (Chaudhary, et al., 2022).

Limited resources for training programs can also hinder employees' understanding and implementation of cybersecurity practices. When organizations lack the means to develop and deliver comprehensive training, employees may struggle to grasp essential cybersecurity concepts and protocols. This can lead to gaps in their knowledge and skills, making them more receptive to security breaches and incidents. Furthermore, underfunded or inadequate training programs may convey a message to employees that their development is not valued, potentially leading to lower engagement and motivation levels (Zhang et al. 2021).

2.8 Summary of Key Findings from the Literature

The literature review has been conducted, focusing on the effectiveness of cybersecurity training within the financial sector. The key literature review findings show that financial institutions face significant challenges, such as breaches, resulting in both severe financial losses and reputational risks. It is crucial to include human factors, particularly the behavior of employees, as they play a pivotal role in vulnerability and breaches. Many of these subjective norms and attitudes of employees can be shaped through cybersecurity training programs, making them an effective tool in fostering better cybersecurity practices within organizations. Addressing this issue, organizations have implemented a variety of training methods including classroom sessions, online modules, and phishing exercises. It has been found that combining these methods provides a comprehensive approach to training, catering to diverse learning preferences and maximizing the effectiveness of these training initiatives. However, implementing such programs is not without its challenges. Budgetary constraints, time limitations, employee resistance, and insufficient resources can impede their integration and effectiveness.

Overall, the literature underscores the significance of comprehending human behavior, utilizing effective training strategies, and confronting organizational obstacles to bolster cybersecurity within financial institutions. It also recognizes the difficulties inherent in cultivating a workforce knowledgeable about security measures.

The aforementioned main literature review concepts form the theoretical basis of our bachelor’s thesis. Along with the theory of planned behavior (TPB) they create a theoretical

framework that is employed in later chapter 5 to interpret and discuss our research findings regarding employees' behavior in cybersecurity training. The theory suggests that behavior is influenced by intention, which is shaped by attitudes, subjective norms, and perceived behavioral control. This theoretical framework allows for understanding the motivational factors driving engagement in training programs. Meaning that employee attitudes towards training, subjective norms, and social influences impact their training effectiveness. By having positive attitudes, organizational support, and peer pressure can the organization contribute to better outcomes.

3 Methodology

In this chapter, we detail the methodology used in our bachelor's thesis. We outline the research approach adopted, alongside the method implemented for data collection. Furthermore, we delve into the criteria for participants' selection, and the method for analysis of the collected data. Concluding this chapter, we reflect on the integrity of our study and the ethical guidelines we observed throughout the research process.

3.1 Research approach

There are three main approaches in research: the quantitative, the qualitative, and the mixed methods approach. The quantitative approach involves testing theories and identifying patterns and includes the systematic collection and analysis of numerical data. In quantitative research, quantitative surveys, experiments are often employed techniques for collecting data. In order to evaluate data and make conclusions about relationships between variables, this approach depends on statistical techniques for analysis. (Creswell & Cresswell, 2017).

The qualitative approach involves the collection and analysis of non-numerical data, such as observations, interviews, and textual analysis. It seeks to deeply explore and comprehend complex phenomena. With an emphasis on context meaning and subjective experiences, this approach seeks to provide in-depth understanding of the research issue. Furthermore, it is characterized by its flexibility and adaptability, and researchers often need to adjust their research methods as they learn more throughout their study (Creswell & Creswell, 2017).

The mixed methods approach integrates components of both quantitative and qualitative research inside a single study. Through the collection and analysis of both numerical and non-numerical data, this research approach enables researchers to obtain a deeper understanding of complicated phenomena (Cresswell & Cresswell, 2017).

For our bachelor's thesis research, we have chosen the qualitative research approach to explore the effectiveness of employee training programs in mitigating cyber threats within financial institutions. Our decision to employ this approach is due to its ability to delve deeper into the participants' experiences, perspectives, and perceptions, rather than numerical data. A qualitative approach is also more suited to examine the factors that influence employees' responses and attitudes to cybersecurity training programs.

3.2 Method of Data Collection

3.2.1 Qualitative Online Survey

An online survey for data collection is a questionnaire via the internet to gather information from participants (Babbie, 2020). This method allows us to reach a large number of participants quickly and efficiently.

The surveys were distributed to employees across various departments of the bank, excluding the cybersecurity department. The survey consisted of 10 questions, encompassing a mix of question types such as scenarios, rankings, and open-ended questions (see appendix C). These diverse question formats were strategically chosen to capture different dimensions of participants' attitudes, perceptions, and behaviors related to cybersecurity training effectiveness and understanding of associated risks. By incorporating scenario-based questions, participants were prompted to envision real-life security threats, while ranking questions identified the prioritization of areas for improvement. Additionally, open-ended questions allowed participants to provide nuanced insights and elaborate explanations. By gathering qualitative data from a broader sample of employees, the surveys provided holistic understanding of the effectiveness and impact of cybersecurity training programs within the bank.

3.2.2 Research Setting

We chose to conduct our study at a bank because of the accessibility to its employees. This bank is a local Swedish institution with offices across Sweden. It operates primarily in retail banking and offers various account types for both organizations and private customers. The bank is also active in the loan and savings markets, catering to the everyday banking needs of its customers. It is estimated to have between 5,000 and 15,000 employees. The first researcher's connections at the bank facilitated our access and enabled us to conduct our bachelor's thesis research there.

3.2.3 Participants, Sample Technique, Criteria, and Sample Size

For our bachelor’s thesis research, the participants were required to be banking employees currently employed at the local Swedish bank where we conducted our study. This ensured that their firsthand experiences and perspectives were directly relevant to the research objectives. By only including current bank employees, we could be confident that the data we collected would provide meaningful, insider-level insights into the bank's daily operations and functioning.

Beyond the requirement of being employed at the bank, we did not impose any additional criteria for participant selection. The primary goal was to gather insights from individuals who were immersed in the bank's activities on a day-to-day basis. By keeping the eligibility criteria broad and inclusive, we were able to access a wider range of perspectives and experiences from across the bank.

We were able to obtain responses from a total of 28 participants working in different departments of the bank. This diversity of respondents, representing various roles and areas of the organization, helped to enrich the depth and breadth of the data we collected. By including participants from multiple departments, we could gain a more holistic understanding of the bank's operations. This diversity allowed us to identify common themes, as well as unique insights.

3.3 Method of Data Analysis

We employed thematic analysis as outlined by Oates, Griffiths & McLean (2022) to analyze the data collected from the online surveys. This method focuses on identifying recurring

themes and patterns, allowing us to derive meaningful insights from the extensive qualitative data collected.

We started by carefully going through every question and answer to make sure no detail was overlooked. This meticulous attention to detail was essential to maintain the accuracy and integrity of the data.

The next step involved generating initial codes from the transcripts. During this phase, we pinpointed key phrases, terms, and concepts that were especially relevant to our research question. These codes acted as the foundational elements for our analysis, helping us begin to piece together the larger picture.

Once we had our initial codes, we organized them into preliminary themes. These themes were designed to capture the recurring patterns we noticed in the data, each offering unique insights related to our research question. We took great care in reviewing and refining these themes, using color-coding and other visual markers to highlight connections and ensure each theme accurately reflected the data. As a result, we identified six themes that represent our findings. The themes are presented in later chapter 4, supported by quotations from the participants.

Concluding, thematic analysis as outlined by Oates, Griffiths & McLean (2022) was crucial in helping us draw out meaningful insights from the data. This structured approach not only facilitated the identification of key patterns in the data but also enabled us to develop a thorough understanding of the themes that surfaced during our research.

3.4 Reliability and Validity

The reliability of a study is determined by the consistency of its results when repeated under the same conditions. In order to ensure reliability, researchers should strive to minimize random errors and inconsistencies in their data collection according to Oates, Griffiths and McLean (2022). In our data collection we ensured reliability by maintaining a consistency in our survey by using standardized procedures and clear instructions for our participants.

Validity, however, is the extent to which a measurement or research instrument accurately represents what it is intended to measure (Oates, Griffiths & McLean, 2022). Oates, Griffiths and McLean (2022) state that validity is concerned with accuracy and meaningfulness of the deductions made from the research findings. In our study, we took several measures to enhance validity. We did this by incorporating a variety of question types, each question type served a specific purpose in capturing different dimensions of participants' attitudes, perceptions, and behaviors related to cybersecurity training. By incorporating a mix of scenarios, rankings, and open-ended questions, we aimed to ensure that our data collection accurately represented the intended research objectives.

3.5 Ethical Considerations

Oates, Griffiths and McLean (2022) emphasize that ethical considerations are an essential component of any research project. Researchers have a responsibility to protect the rights,

dignity, and well-being of their research participants, which includes obtaining informed consent, ensuring confidentiality and anonymity, and minimizing any potential harm or risks to participants. Firstly, the outline and purpose of our study was clearly stated, as well as the freedom for the participants to choose whether or not they want to take part in the study. Participants were assured confidentiality with their responses to prevent any identification. Additionally, the bank has requested not to disclose its identity and we have assured them of confidentiality.

4. Findings

The findings chapter presents the themes that emerged from the analysis of the collected data; that is, the online surveys. The themes represent the research findings and are explained and supported by quotations from the participants.

4.1 Theme 1: Organizational Support for Training

Based on the data collected from respondents about cybersecurity in general and cybersecurity training programs within the financial sector, especially within the Swedish bank, it is clear that there is substantial organizational support for such initiatives. The average ratings given by employees for various aspects of training provide a solid insight into the effectiveness and frequency of the training programs.

Also, the data was clear when it came to the effectiveness of training programs. Employees, when asked *"How effective do you think the current cybersecurity training at your workplace is in preparing you to handle potential threats?"*, rated the effectiveness of cybersecurity training at an average of 4 out of 5. This high rating indicates that the training is well-received and is perceived as adequately preparing employees to handle potential cybersecurity threats.

The responses also indicate that respondents are satisfied with their cybersecurity knowledge. When asked *"How satisfactory do you consider your current knowledge of cybersecurity to be in performing your job effectively?",* the average satisfaction level with their current cybersecurity knowledge, rated at 4, underscoring a workforce that feels competent and well-prepared. This confidence likely stems from the robust training programs provided by the organization, which not only educate but also empower employees to effectively apply their knowledge in their roles.

4.2 Theme 2: Impact of Training on Risk Perception

One of the themes that was clear within the collected data was how effective the training was on risk perception, which is the reflection we can see through the answers when we asked the employees *"You receive an email from an unknown sender asking you to click a link to update your work details. Do you click on it?"* Respondent 1 answered *"No, as there is a risk of fraud."* which gives the impact of a good understanding of the risks involved.

Respondent 9 emphasizes this by stating, *"No. Because we all should know better."* also highlighting the expectations of their colleagues and the clear culture expected. This response underscores a significant level of awareness and an established mindset about the appropriate behaviors expected when facing potential cybersecurity threats. It reflects a broad understanding within the organization that employees are expected to know better than to engage in suspicious communications.

Another important note when respondent 7 answers with *"No - do not engage with any communication from unknown senders."* The response directly points to a proactive and

secure behavior that has been encouraged and reinforced through cybersecurity training. The responses gathered under this theme vividly illustrate how cybersecurity training has effectively shaped employees' risk perception and prepared them to identify and react appropriately to potential threats. Like respondent 1 showed clear understanding of basic protraction within the cybersecurity when asked about clicking on a link in an email. Respondent 1's refusal, based on the risk of fraud, shows that the training effectively instilled a cautious approach to security, which is critical in preventing fraud and data breaches.

Respondent 6 also demonstrated a clear understanding of the type of cyber-attack that could be involved in such suspicious occasions, showing not only awareness but also the ability to correctly identify the threat. This indicates a solid grasp of the characteristics of phishing attacks, likely a result of specific training focused on recognizing different forms of cyber threats. Not only to the email attacks but also to the phone threats when attackers pose as trusted departments to get critical information. Respondent 6 expresses a critical procedural rule that prevents unauthorized access through social engineering attacks. The clarity in this protocol shows that the training was successful in delineating the correct steps employees should follow, enhancing their confidence and capability in maintaining security.

4.3 Theme 3: Attitudes Towards Training

Respondents 2, 26, and 28 provided specific feedback highlighting a desire for more dynamic and illustrative content within the training modules. They suggested including current videos that demonstrate how fraudsters and hackers operate, as well as different licensed training programs, as mentioned by Respondent 26 when asked, *"Do you have any suggestions on how the current training can be improved to better meet your needs and challenges?"*

The data clearly shows satisfaction by providing an average effectiveness rating of 4 out of 5 for current cybersecurity training programs when asked *"How effective do you think the current cybersecurity training at your workplace is in preparing you to handle potential threats?"*, indicating a strong positive reception among employees. This high rating suggests that the majority of the workforce finds the training sessions adequately informative and useful in preparing them to handle cybersecurity threats.

4.4 Theme 4: Reporting and Communication

This theme emerged from finding out that most employees were positive about going to ask the nearest boss or IT department about a question or a situation that occurred within the workplace. This indicates that employees feel very secure and supported in reporting security concerns or incidents to their superiors. When asked *"How comfortable do you feel reporting suspected cybersecurity incidents to your IT department?"* the majority gave it 5 out of 5, which can significantly enhance the overall security culture within the organization.

Also, when respondent 3 answered with only the sentence *"Report to the manager."*, which shows the responsiveness among employees. They are not only aware of the proper protocols but are also quick to act on them, which is crucial in mitigating potential damage from cybersecurity threats. It also points out the leadership support, the readiness to report directly

to a superior reflects confidence in leadership's handling of such reports. It indicates that the leadership is approachable and committed to maintaining a secure working environment.

The theme indicates that employees who reported higher levels of participation in the cybersecurity training programs, 4 or 5 on a scale to 5, tended to express higher satisfaction with their current cybersecurity knowledge. This suggests that the training programs have been successful in equipping employees with the necessary knowledge and skills to perform their duties effectively. Employees who reported high satisfaction with their cybersecurity knowledge were also more likely to feel comfortable reporting suspected cyber threats to the IT department. This correlation implies that the training programs have successfully provided the employees with the essential knowledge and abilities to identify and respond to potential security incidents. The data indicates a high correlation between the level of participation, the satisfaction with cybersecurity knowledge, and the comfort in reporting suspected cyber incidents. This suggests that the organization's efforts to provide comprehensive and effective training programs have been successful in creating a security-conscious workforce that is actively engaged to protect the organization against cyber threats.

4.5 Theme 5: Leadership Influence

Leadership influence was very apparent in our analyzed data. When Respondent 7 was asked about receiving a phone call from the IT department asking for credentials, the answer was a clear no, but the response also included the mention of consulting the nearest team leader. This reflects a collaborative approach to decision-making, emphasizing the role of both peers and superiors in guiding actions related to cybersecurity.

We also see that employees rely on the team leader or boss in their vicinity. When Respondent 6 was asked about a situation involving another employee using a USB, which is typical in the work environment, the response was clear about consulting the boss to determine if this action was allowed. This response highlights how leadership is central in setting boundaries and providing clear directives that inform employee actions. It shows that employees are not only aware of the hierarchical structure but also feel supported by it to make informed decisions, enhancing the overall governance of cybersecurity practices.

We can see the same pattern all over our data, such as when respondent 25 was asked “You discover that your work computer is acting strangely and showing signs of malicious software. How would you handle this?” the answer was short and clear “Contact IT security or nearest supervisor.” Emphasizing the close connection between leaders and employees.

4.6 Theme 6: Tailored Training and Continuous Enhancement

The feedback and suggestions from employees regarding the cybersecurity training program show strong engagement in the culture, when we left the question voluntarily 18 respondents gave different proposals of type of improvement to the education. Giving a clear case of an engaged workspace where employees feel comfortable giving feedback and suggestions without it being necessary.

Some were clear suggestions such as respondent 17 answering *"More practical tests and actual examples where companies have been affected."*. By simulating real incidents and discussing actual cases where companies face cybersecurity issues, training can become more engaging and relatable. Practical tests and scenarios can help employees better understand the implications of security breaches and the importance of their roles in preventing them.

Respondent 19 suggests incorporating discussions about cybersecurity protocols and response strategies into regular meetings. This recommendation points to the need for ongoing dialogue about cybersecurity, not just during formal training sessions but as part of the regular interaction within the team. Such discussions can reinforce learning, keep security top of mind, and ensure that all team members are prepared to act swiftly and appropriately in case of security incidents.

Additionally respondent 10 lifted the need for clarity and understanding of the training, by simply asking if anything is not clear. This approach can help ensure that uncertainties are addressed, leading to a deeper understanding and better application of the training content.

Respondents 2, 11 and 6 suggested different approaches to the education programs. By asking for more visually made tools to make the material more interesting and also relatable. This type of content can help make the training more engaging and realistic, providing employees with a clearer understanding of the nature of threats they are likely to encounter.

Respondents are asking for more practical elements in training, like hands-on exercises, simulations, and real-world problem-solving scenarios. This shows a need for experiential learning that lets employees practice their skills in settings that are safe yet realistic. Including practical exercises can strengthen learning, enhance problem-solving skills, and boost confidence in managing real threats.

Respondent 11 on the other hand is pushing for a more holistic approach to cybersecurity training that spans everything from basic concepts to practical implications. This comprehensive coverage ensures that employees across all levels and functions grasp the broader context of cybersecurity, how it affects their specific roles, and how to apply this knowledge in various operational scenarios. Such an approach helps develop a deep and practical understanding of cybersecurity.

5. Discussion

In this chapter, we discuss our empirical findings with the insights from the literature review and the theory of planned behavior (TPB) theory. The findings answer the posed research question: What role does organizational culture play in the effectiveness of employee training to reduce cyber risks and improve the overall cybersecurity posture within the financial sector? Through this discussion we aspire to provide a deeper understanding of the implications of our findings.

5.1 Organizational support for training

The high ratings given by employees on the effectiveness of cybersecurity training programs within the organization indicate strong organizational support for such initiatives. This aligns with the literature, which emphasizes the importance of organizational culture and leadership in fostering a security-conscious environment (Khaw et al., 2023). The open communication channels between employees and the IT department further reinforce the notion of a supportive organizational structure. This confidence likely stems from the robust training programs provided by the organization, which not only educate but also empower employees to effectively apply their knowledge in their roles

The study by Khaw et al. (2022) also highlights that organizational culture and peer pressure can significantly impact the motivation of training participants. If the organization does not prioritize or support cybersecurity training, employees may be less inclined to participate actively. The high ratings given by the Swedish bank employees on the effectiveness and frequency of the training programs suggest that the organization has successfully fostered a culture that values and supports these initiatives. Meaning these training programs tell that the training is relevant, up to date, comprehensive and covers the necessary skills and knowledge to navigate the evolving landscape of cybersecurity threats.

5.2 Impact of Training on Risk Perception

The literature review also highlights the critical role of employee behavior in cybersecurity vulnerabilities, with phishing attacks being a significant concern (Daengsi et al., 2021). The findings suggest that the training programs have been successful in enhancing the employees' risk perception and their ability to identify and respond to potential threats, such as phishing attempts. In the scenario questions, almost every single participant answered in a way that indicates they would handle the potential threats appropriately. However, the findings revealed that in the two scenario questions that included another colleague, a colleague asked you to download a file with no prior information, and a colleague using a personal USB to transfer files, a few participants would potentially fall for the threat despite the atypical nature of the situation. The TPB theory provides insights into why some employees may be more susceptible to such threats. Subjective norms, a key component of the TPB, suggest that individuals' perceptions of social pressure or expectation from their peers influence their behavior. In this context, the participants may have been motivated by a sense of social obligation or pressure to comply with their colleagues' requests, even if it posed a

cybersecurity risk. This reveals that even with comprehensive training, some employees may still be inclined to prioritize trust and social norms over security protocols in certain situations.

By understanding these human factors and the psychological biases that can influence employee behavior, the organization can further refine its training programs to address these vulnerabilities. Incorporating more practical exercises, case studies, and discussions around social engineering attacks can help employees develop a more robust and nuanced understanding of cybersecurity threats, ultimately enhancing the overall effectiveness of the training initiatives.

The findings from the employees illustrate how the training has successfully instilled a cautious and security-conscious approach. For example, Respondent 1's clear refusal to click on the suspicious link in the email, citing the risk of fraud, shows that the training has effectively translated into practical security behaviors This aligns with the study by Kweon et al. (2021) emphasis on the importance of employee awareness and personal understanding of security protocols for ensuring successful policy compliance and organizational resilience against cyber threats. Similarly, Respondent 9's statement, "No, because we all should know better," underscores a significant level of awareness and an established mindset about the appropriate behaviors expected when facing potential cybersecurity threats. This specific avoidance of engagement with unknown senders is a practical application of the training, indicating that the training sessions are effectively translating into everyday practices. It demonstrates that the training has successfully heightened employees' risk perception, enabling them to automatically identify and avoid potential threats.

These findings demonstrate the effectiveness of the training programs in shaping the employees' risk perception and preparedness to identify and respond to potential threats. The employees' clear understanding of the risks involved and their willingness to follow security protocols, such as avoiding engagement with suspicious communications, indicate that the training has successfully translated into practical security behaviors.

5.3 Attitudes Towards Training

As previously mentioned, our findings revealed a positive correlation between participation, participants satisfaction with their cybersecurity knowledge, and comfort in reporting potential cyber threats.

The findings from the previous studies align with and support the insights gained from the employee survey. The study by Khaw et al. (2023) emphasizes that positive attitudes towards cybersecurity training, where employees see the value and importance of the training, are associated with better learning outcomes and increased application of the skills learned. The findings indicate that the employees have developed positive attitudes towards the cybersecurity training programs, as evidenced by the high ratings on the effectiveness of the training.

5.4 Reporting and Communication

According to Kamiya et al. (2018) which highlights the severe financial and reputational damage resulting from security incidents, the importance of effective cybersecurity training becomes even more evident. By equipping employees with the necessary knowledge and skills to identify and respond to potential security incidents, organizations can mitigate the risk of data breaches and minimize the associated repercussions. By indicating a correlation between participation in training programs and increased comfort in reporting cyber threats, the survey suggests that well-trained employees are better equipped to identify and respond to potential security incidents. This enhances organizational security, but also mitigates the financial and reputational risks associated with cyber threats. Our findings reinforce the notion that investing in cybersecurity training is not only essential for enhancing organizational security but also for safeguarding financial stability and reputation.

Our findings indicate that the employees feel very secure and supported in reporting security concerns or incidents to their superiors. The participants expressed a high level of comfort (5 out of 5) in reporting suspected cybersecurity incidents to the IT department. This suggests that the organizational culture and leadership support have created a social environment that encourages and reinforces the reporting of security concerns, aligning with the TPB's concept of subjective norms. This level of comfort also suggests that there is a clear and open communication channel between staff and the IT department or cybersecurity team, which is essential for a proactive cybersecurity posture. By empowering employees to report security incidents and concerns, the organization has demonstrated its commitment to maintaining a secure working environment, which can further strengthen the subjective norms and social influences that shape employee behavior.

5.5 Leadership Influence

The study by Kwon et al. (2021) emphasizes that even with well-designed policies and procedures, successful implementation and compliance cannot be guaranteed if employees are not aware of these requirements. This aligns with our findings where the data suggests that leadership influence and support play a significant role in driving employee engagement and adherence to cybersecurity practices. Specifically, our findings indicate that the employees' willingness to report suspected cyber incidents directly to their supervisors or the IT department reflects a high level of trust and confidence in the organization's leadership.

This is also evident when Respondent 6 was faced with a situation involving another employee using a USB, which is atypical in the work environment, the response was to consult the boss to determine if the action was allowed. This response highlights how leadership is central in setting boundaries and providing clear directives that inform employee actions. It suggests that the employees feel supported by the hierarchical structure and are confident in the leadership's ability to provide guidance on appropriate cybersecurity practices.

If the organization does not prioritize or support cybersecurity training, employees may be less inclined to participate actively and rely on leadership for decision-making as argued by Khaw et al (2022). However, our findings indicate that the organization has successfully fostered a culture where employees feel empowered to consult with their superiors and

colleagues when faced with potential cybersecurity threats. This suggests that the leadership has been effective in creating an environment that encourages and reinforces the adoption of secure behaviors. By consulting with colleagues and a supervisor before proceeding, Respondent 7 demonstrates reliance on collective wisdom and leadership direction.

5.6 Tailored Training and Continuous Enhancement

The findings of both Wu He (2023) and Zhang (2021) highlighted that tailoring the training content to target the audience is crucial for enhancing the effectiveness of cybersecurity training programs. Our findings show that employees provided specific feedback on areas for improvement, such as incorporating more engaging and illustrative content, like videos for example. This suggests that the employees perceive the current training as lacking in these aspects. Ajzen (1991) further emphasizes that when the training is perceived as engaging and easy to understand, employees are more likely to exhibit positive attitudes towards it. This aligns with the employees' desire for practical and relatable training content. By tailoring the training programs to better meet the needs and preferences of the employees, the organization can improve the perceived relevance and efficacy of the training. This, in turn, is likely to foster more positive attitudes and increased engagement from the employees.

Furthermore, this aligns with the literature by Chowdhury and Gkioulos (2021) which highlights that effective cybersecurity training for critical infrastructure protection, such as the financial sector, requires a customized approach that considers the specific context, risks, and learning needs of the target audience. A one-size-fits-all training program is often insufficient. Our findings reflect this need for a tailored approach. The employees' suggestions for more dynamic and illustrative content suggest that the current training programs may not be fully addressing their specific learning preferences and the unique challenges they face in the financial sector. Organizations need to carefully analyze the specific requirements, learning styles, and preferences of their employees, and then design the training programs accordingly. When the training content and delivery are perceived as relevant, practical, and easy to understand, employees are more likely to find the programs effective and engage with them actively. This positive perception of relevance and efficacy is crucial for enhancing the overall impact and success of the organization's cybersecurity education efforts.

Our findings indicate that the participants have a strong preference for a combination of different training methods to enhance the effectiveness of the cybersecurity education programs. Specifically, the feedback provided by the respondents suggests that they would like to see a mix of traditional classroom-style training, online learning, and practical phishing simulation exercises. For example, Respondent 26 highlighted the desire for "different licensed training programs" to be incorporated into the current training modules. Another example is Respondent 2, who also provided constructive feedback on the training content. Respondent 2 suggested incorporating "Current videos that demonstrate how fraudsters and hackers operate" into the training modules. This suggests that the employees value a diverse range of training approaches. The literature review further supports this finding with Kim's (2010) study discovering that a combination of training methods can be the most efficient approach to cybersecurity education.

Our findings also suggest that the organization has been successful in creating an environment where employees feel empowered to provide constructive feedback and suggestions for

improving the cybersecurity training programs. This is shown by the 18 respondents voluntarily providing different proposals for improving the education, demonstrating strong engagement and a sense of ownership over the training initiatives. This aligns with Khaw et al. (2022) literature expressing the role that organizational culture and peer pressure has on employee engagement.

5.7 Discussion of Findings with the theory of Planned Behavior

By analyzing the findings through the lens of the Theory of Planned Behavior (TPB), we can see how the three key components: *attitudes*, *subjective norms*, and *perceived behavioral control* are reflected in the key findings as illustrated in the following figure 3.

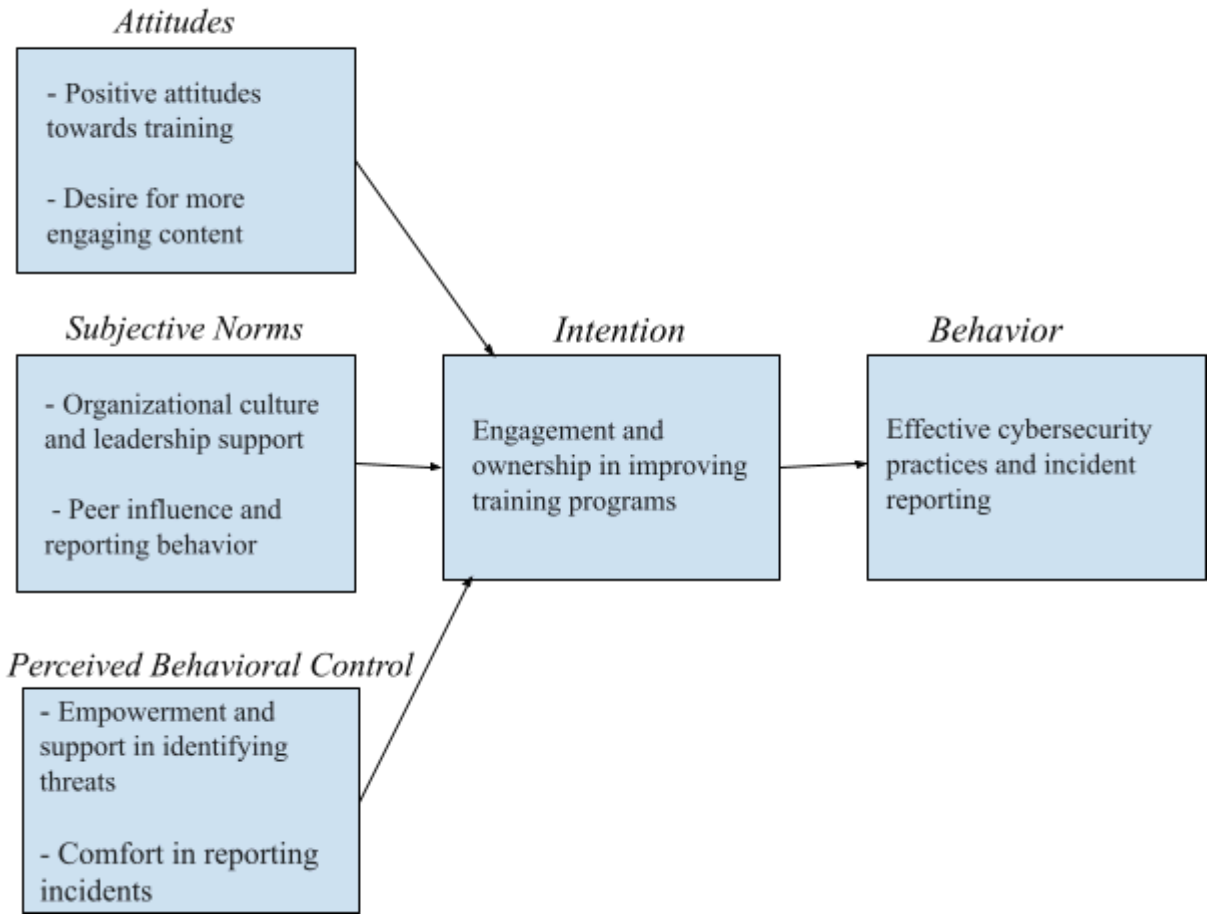

Figure. 3: TPB map of analyzed findings (Made by the authors, 2024)

Attitudes Towards Cybersecurity Training
The findings indicate that the employees have developed positive attitudes towards the cybersecurity training programs. This is evident from the high average effectiveness rating of 4 out of 5 when asked about the current training programs. The employees' desire for more dynamic and illustrative content, such as incorporating videos, further suggests that they

perceive the training as valuable and are interested in enhancing its relevance and engagement. However, the feedback from respondents suggests that there is room for improvement in the training content and delivery methods.

According to the TPB, attitudes towards a behavior are a key determinant of an individual's intention to engage in that behavior. If the employees do not perceive the training as sufficiently engaging or relevant, their attitudes may become less favorable, potentially undermining their motivation to actively participate and apply the learned skills.

To address this, the organization could leverage the TPB to better understand the factors shaping the employees' attitudes and design training programs that more closely align with their preferences and perceptions of usefulness. This may involve conducting surveys or focus groups to gather more detailed feedback on the specific aspects of the training that the employees find valuable or lacking.

Subjective Norms and Social Influences
The findings also highlight the importance of subjective norms and social influences in shaping employee behavior. The employees' willingness to report suspected cybersecurity incidents directly to their superiors or the IT department reflects the influence of the organizational culture and leadership support. Respondent 3's response of reporting potential threats or suspicious behavior to the boss, demonstrates the responsiveness and trust in the leadership's ability to handle such reports effectively. However, the TPB also highlights the potential for negative social influences to impact the effectiveness of the training programs. If the organization does not consistently prioritize and support cybersecurity education, or if there are pockets of resistance or indifference among the workforce, it could undermine the overall impact of the training initiatives.

Perceived Behavioral Control
The findings indicate that the employees feel empowered and supported in their ability to identify and respond to potential cyber threats. The majority of the employees expressed a high level of comfort (5 out of 5) in reporting suspected cybersecurity incidents to the IT department, suggesting a strong sense of perceived behavioral control. This is further reinforced by the employees' clear understanding of the appropriate protocols and their willingness to consult with supervisors or colleagues. Moreover, these results suggest that employees feel empowered and supported in their ability to take appropriate actions when faced with cyber security challenges.

By aligning the cybersecurity training programs with the principles of the TPB, the organization has been able to foster a security-conscious culture and enhance the overall effectiveness of their education initiatives. The positive correlation between participation, satisfaction, and reporting comfort reflects the successful integration of these theoretical considerations into the design and implementation of the training programs.

For example, the employees' feedback on the need for more dynamic and illustrative content 1 suggests that the organization should address the perceived complexity of the training, which can positively impact their attitudes and engagement. Similarly, the organization's efforts to encourage open communication and reporting channels align with the TPB's emphasis on subjective norms and their influence on individual behavior.

5.8 Concluding Remarks of the Discussion

The research question posed at the start of this bachelor's thesis is *What role does organizational culture play in the effectiveness of employee training to reduce cyber risks and improve the overall cybersecurity posture within the financial sector?* To answer this, a summary of the discussion and the key findings follows.

- **Positive employee attitudes**
  Employees have developed positive attitudes towards the cybersecurity training programs, evidenced by their high average effectiveness rating of 4 out of 5. To sustain these positive attitudes, continue to solicit feedback from employees to ensure training remains relevant and valuable to them.

- **Desire for dynamic training content**
  Employees desire more dynamic and illustrative training content, such as incorporating videos, to enhance the relevance and engagement of the programs. Moreover, employees want simulations and problem-solving scenarios to strengthen learning and enhance problem-solving. Incorporate more hands-on exercises and visually engaging content, such as current videos demonstrating real-world cyber threats. This will boost employee confidence in managing real cyber threats.

- **Influence of organizational culture and leadership**
  The organizational culture and leadership support have positively influenced employee behavior, as demonstrated by their willingness to report suspected cybersecurity incidents to superiors. Encourage ongoing discussions about cybersecurity protocols and response strategies during regular team meetings to reinforce learning and keep security top of mind.

- **Empowerment and support**
  Employees feel empowered and supported in their ability to identify and respond to potential cyber threats, as reflected in their high comfort level in reporting incidents to the IT department. Maintain this supportive environment by continuously reinforcing the importance of cybersecurity from the top-down.

- **Employee engagement and feedback**
  Employees provided constructive feedback and suggestions for improving the cybersecurity training programs, indicating a strong sense of engagement. Establish regular feedback to gather employee input and continuously enhance the training programs based on their needs and preferences.

6. Conclusion

In this chapter, we present the conclusions from our bachelor's thesis study, which constitute the research outcome. Further, we present our contributions. Finally, we provide some suggestions for future research.

6.1 Conclusions

The bachelor's thesis explored the effectiveness of cybersecurity training programs within a Swedish financial institution, utilizing the theory of planned behavior (TPB) as the guiding theoretical framework. The bachelor's thesis research employed a qualitative approach, conducting an online survey with 28 bank employees to gain in-depth insights into their experiences and perceptions. The collected data were analyzed thematically to conclude to six themes, which represent the research findings.

The findings show several key insights: strong organizational support for the training programs, enhanced employee understanding of cybersecurity risks, a preference for diverse training approaches, and a high level of employee engagement. The findings further show the alignment of the training initiatives with the TPB, highlighting the positive influence on employees' attitudes, subjective norms, and perceived behavioral control. More specifically, the findings indicate that in workplaces where there is a foundation of trust among employees, certain vulnerabilities can arise if cybercriminals exploit this trust. This suggests that employees who lack consistent education on what is permitted and what is not may show less concern about their colleagues' actions. Additionally, they become more narrowly focused on their individual responsibilities, potentially posing a significant threat if not managed effectively. The high ratings given by employees on the effectiveness and frequency of cybersecurity training programs indicate strong organizational support for such initiatives, emphasizing the crucial role of organizational culture and leadership in fostering a security-conscious environment. The training programs have successfully enhanced employees' understanding of cybersecurity risks and their role in mitigating these threats, as employees demonstrated a heightened awareness of potential security breaches and a willingness to report suspicious activities. Thus, a clear link between workplace culture and employees' behavior was found. The theory of planned behavior (TPB) provided further valuable insights into the study, particularly in understanding how employees respond to different situations based on the unspoken norms within the culture. Concluding, the findings reveal that the organization has effectively fostered positive attitudes towards cybersecurity training, leveraged the influence of subjective norms, and empowered employees with a sense of behavioral control.

6.2 Contributions

The bachelor's thesis has made several important contributions to the existing research on cybersecurity training effectiveness within the financial sector. By adopting a qualitative approach and incorporating the TPB framework, the study has provided a comprehensive understanding of the factors that influence the success of such training programs. The insights gained from this research can help organizations, particularly in the financial industry, to design and implement more effective cybersecurity training initiatives that resonate with employees.

The findings from this study have also directly benefited the participating Swedish bank, as the organization can use the feedback and recommendations to continuously enhance its cybersecurity training programs. The employees' engagement and willingness to provide constructive suggestions demonstrate a high level of investment in the organization's security posture, which can be leveraged to drive further improvements.

6.3 Suggestions for Future Research

The study has provided valuable insights, but there are several avenues for future research to build upon these findings. While numerous studies have explored cybersecurity in the financial sector across Asia and other regions where cash remains prevalent, there is a notable gap in research within Nordic countries. In these countries, where cash usage is minimal and online banking is predominant, understanding cybersecurity challenges and potential vulnerabilities is crucial. Future researchers are encouraged to address this gap by investigating cybersecurity issues specific to Nordic financial institutions, including the potential impact of insider threats gaining access to software systems.

Additionally, future research could delve into longitudinal studies in understanding the long-term impact of cybersecurity training programs and tracking the application of learned skills and behaviors over extended periods. By examining how employees' cybersecurity awareness, knowledge, and practices evolve over time following training programs.

References

Ajzen, I. (1991) *The theory of planned behavior, Organizational Behavior and Human Decision Processes.* Retrieved from: https://www.sciencedirect.com/science/article/pii/074959789190020T

American Bankers Association. (2024). Seven cybersecurity threats for banks in 2024—and some smart precautions. ABA Banking Journal. Retrieved from https://bankingjournal.aba.com/2024/03/seven-cybersecurity-threats-for-banks-in-2024-and-some-smart-precautions/ (ABA Banking Journal).

Babbie, E.R. (2020). *The Practice of Social Research*. [online] Google Books. Retrieved from: https://books.google.se/books?hl=en&lr=&id=lFvjDwAAQBAJ&oi=fnd&pg=PP1&dq=babbie+2016+the+practice+of+social+research&ots=I4xS3z8RVa&sig=GkrY5Tt9yfNjFLClv7BsoANX1hI&redir_esc=y#v=onepage&q=babbie%202016%20the%20practice%20of%20social%20research&f=false

Bank for International Settlements (BIS). (2020) *Enhancements to cross-border payments: building blocks of a global roadmap.* Retrieved from https://www.bis.org/cpmi/publ/d122.pdf

Chaudhary, S., Gkioulos, V. and Katsikas, S. (2022). *Developing metrics to assess the effectiveness of cybersecurity awareness program.* Journal of Cybersecurity. Retrieved from: https://academic-oup-com.ludwig.lub.lu.se/cybersecurity/article/8/1/tyac006/6590603

Chatchalermpun, S. and Daengsi, T. (2021) *Improving cybersecurity awareness using phishing attack simulation.* Retrieved from: https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015/pdf

Chatterjee, D. (2019), "Should executives go to jail over cybersecurity breaches?", Journal of Organizational Computing and Electronic Commerce, Vol. 29 No. 1, pp. 1-3.

Chrisda (2024). *Get started using Attack simulation training*. [online] learn.microsoft.com. Retrieved from: https://learn.microsoft.com/en-GB/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide

Chowdhury, N. and Gkioulos, V., 2021. *Cyber security training for critical infrastructure protection: A literature review.*

Creswell & Cresswel. (2017) *Research design: qualitative, quantitative, and mixed methods approaches.* [online] UCG. Retrieved from: https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P. and Utakrit, N. (2021). *A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization.*

Financial Services Information Sharing and Analysis Center. (2018). *FS-ISAC Unveils 2018 cybersecurity trends according to top financial.* CISOs. Retrieved from: https://www.fsisac.com/ article/fs-isac-unveils-2018-cybersecurity-trends-according-top-financial-cisos

Griffiths, C. (2024). The latest phishing statistics. Available at: https://aag-it.com/the-latest-phishing-statistics/

International Monetary Fund (IMF). (2024) *Global Financial Stability Report.* retrieved from: https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024

Jemal Abawajy, J. (2014). *User preference of cyber security awareness delivery methods.* Taylor & Francis. Retrieved from: https://www.academia.edu/20452374/User_preference_of_cyber_security_awareness_delivery_methods

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. and Stulz, R.M. (2018). *What is the Impact of Successful Cyberattacks on Target Firms?*

Khaw, K.W., Alnoor, A., Abrrow, H.A. -, Tiberius, V., Ganesan, Y. and Atshan, N.A. (2022). *Reactions towards organizational change: A systematic literature review.*

Kim, P. (2010). *Measuring the effectiveness of information security training: A comparative analysis of computer -based training and instructor -based training.* ProQuest. [online] Retrieved from: https://www.proquest.com/openview/715548571bf8798e77d60c70dcad6bba/1?pq-origsite=gscholar&cbl=18750

Kumari, P. (2023). *eLearning Or Traditional Classroom Learning? Exploring The Pros And Cons*. [online] eLearning Industry. Retrieved from: https://elearningindustry.com/elearning-or-traditional-classroom-learning-exploring-the-pros-and-cons.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). *Teaching Johnny not to fall for phish.* [online] ResearchGate. Retrieved from: https://www.researchgate.net/publication/220169843_Teaching_Johnny_not_to_fall_for_phish#fullTextFileContent

Kweon, E., Lee, H., Chai, S. and Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers, 23*, pp.361-373.

Means, B., Toyama, Y., Murphy, R., Bakia, M. and Jones, K. (2010). *Evidence-Based Practices in Online Learning: A Meta-Analysis and Review of Online Learning Studies*. [online] Retrieved from: https://www2.ed.gov/rschstat/eval/tech/evidence-based-practices/finalreport.pdf

Oates, B.J., Griffiths, M. & McLean, R. (2022). *Researching information systems and computing.* 2nd ed. [online] SAGE, Thousand Oaks. Available at:

https://books.google.com/books?hl=en&lr=&id=tN5XEAAAQBAJ&oi=fnd&pg=PP1&dq=Oates

Statista. (2022). Online banking penetration in leading European countries. Available at: https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/ (Accessed: 30 April 2024)

Stieninger, M. (2022) *Factors influencing the organizational adoption of cloud computing: a survey among cloud workers.* [online] SemanticScholar. Retrieved from: https://www.semanticscholar.org/paper/Factors-influencing-the-organizational-adoption-of-Stieninger/de2096b6b9e144909e8ed09a32b63bdf5788790f

Thales Group. (2024). *2024 Thales Data Threat Report ranks ransomware attacks as top threat.* Retrieved from: https://www.thalesgroup.com/en/countries-asia-pacific/india/news/2024-thales-data-threat-report-ranks-ransomware-attacks-top

Willie, M.M. (2023) *The role of Organizational Culture in cybersecurity: Building a security-first culture*, *SSRN*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4564291

Wu He, Ivan Ash, Mohd Anwar, Ling Li, Xiaohong Yuan, Li Xu, Xin Tian. (2020) *Improving Employees' Intellectual Capacity for Cybersecurity Through Evidence-Based Malware Training*

Zuopeng (Justin) Zhang, Wu He, Wenzhuo Li, and M'Hammed Abdous. (2021) *Cybersecurity awareness training programs: a cost–benefit analysis framework*

Appendices

Appendix A: Email to the bank employees

Hej allihopa! Vi är två klasskamrater som skriver vårt kandidatexamensarbete med ett särskilt fokus på cybersäkerhet inom banksektorn. Vår forskning syftar till att belysa och utforska betydelsen och effekten av de utbildningsprogrammen som vi genomför inom cybersäkerhet som bankbranschen genomgår kontinuerligt.

Med detta mejl hoppas vi att ni engagerar er i en kort undersökning som syftar till att fördjupa vår förståelse av ämnet. Vi är övertygade om att ert deltagande inte bara kommer att berika vår studie utan också bidra till en bredare förståelse av cybersäkerhetens roll och värde inom vårt verksamhetsområde.

Vi ber om lite av er värdefulla tid, ca 10 minuter, för att besvara några noggrant utvalda frågor. Vi har gjort vårt bästa för enkäten ska vara lätt att svara på och tar minimalt tid. Din medverkan skulle vara av stor betydelse för att öka förståelsen för dessa viktiga frågor och för att kunna dra relevanta slutsatser för arbetet.

Vi hoppas ni vill vara med och undersöka detta.

Appendix B: Informed Consent Form

Title of the Study: "Securing the Front Line: The Role of Employee Training in Mitigating Cyber Threats in Financial Institutions"

Researchers: Kamal Mansour, Bachelor Student, ka3688ma-s@student.lu.se, Tea Benic, Bachelor Student, te3373be-s@student.lu.se

Purpose of the Study: The purpose of this bachelor's thesis is to explore how human factors and organizational culture interact to influence the effectiveness of cybersecurity training programs in the financial sector. The aim of the thesis is to enhance the cybersecurity posture within financial institutions by identifying strategies to reduce cyber risks effectively. Your participation in this study will contribute valuable insights into the effectiveness of current training practices and the role of organizational culture in shaping cybersecurity defenses in the financial sector.

Procedures: You will be asked to participate in a semi-structured interview that will last approximately 30 minutes. The interview will be conducted by Kamal Mansour and Tea Benic. The interview will be recorded for transcription purposes, and the recording will be stored securely and confidentially.

Risks: There are no known risks associated with participating in this study.

Benefits: Your participation in this study will provide valuable insights into the critical success factors for the successful implementation of AI solutions in SMEs. The findings from this study may also help other SMEs considering AI implementation in the future.

Confidentiality: Your participation in this study is strictly voluntary and confidential. All information collected during the study will be kept strictly confidential and will only be used for research purposes. Your name and/or the name of your company will not be exposed

Voluntary Participation: Participation in this study is completely voluntary, and you may choose to withdraw your participation at any time. If you choose to withdraw, any information collected up to that point will be destroyed.

Contact Information: If you have any questions or concerns about this study, you may contact the Researchers at any of their given contact information.

Consent: By agreeing to participate in this study, you are indicating that you have read and understood the information provided above, and that you voluntarily agree to participate in this study.

Signature: _____ Date: _____

Appendix C: Online Survey

1. Om en kollega bad dig ladda ner en fil, som är viktigt för ert arbete, genom att använda ett USB-minne som du fick direkt från dem, utan att du hade fått någon tidigare information om det, skulle du då använda USB-minnet för att hämta filen så att du kunde fortsätta ditt arbete?

2. Du får ett e-postmeddelande från en okänd avsändare som ber dig klicka på en länk för att uppdatera dina arbetsuppgifter. Klickar du på det?

3. Du får ett samtal från någon som påstår sig vara från IT-supporten och ber om dina inloggningsuppgifter för att lösa ett problem med ditt konto. Ger du ut dina inloggningsuppgifter?

4. Hur ofta deltar du i cybersäkerhetsutbildningar på din arbetsplats?

5. Hur bekväm känner du dig med att rapportera misstänkta cyber säkerhetsincidenter till din IT-avdelning?

6. Hur tillfredsställande anser du att din nuvarande kunskap om cybersäkerhet är för att utföra ditt arbete effektivt?

7. Hur effektiva tycker du att de nuvarande cybersäkerhet utbildningarna på din arbetsplats är för att förbereda dig på att hantera potentiella hot?

8. Du upptäcker att din arbetsdator agerar konstigt och visar tecken på skadlig programvara. Hur skulle du hantera detta?

9. Du märker att din kollega använder sitt personliga USB-minne för att överföra filer till arbetsdatorn. Vad skulle du göra i denna situation?

10. Har du några förslag på hur den nuvarande utbildningen kan förbättras för att bättre möta era behov och utmaningar?

Appendix D: Online Survey Transcriptions

The collected empirical material, presented in this appendix, has been translated from Swedish to English for the purpose of consistency and clarity in the bachelor's thesis. That is, the survey was conducted in Swedish, but since the thesis is written in English, the quotations included in chapter 4 have been translated to maintain uniformity in language throughout the document. This translation ensures that all readers can understand and interpret the findings accurately.

Respondent ID	Om en kollega bad dig ladda ner en fil, som är viktigt för ert arbete, genom att använda ett USB-minne som du fick direkt från dem, utan att du hade fått någon tidigare information om det, skulle du då använda USB-minnet för att hämta filen så att du kunde fortsätta ditt arbete? Förklara gärna du svara Ja/Nej	Du får ett e-postmeddelande från en okänd avsändare som ber dig klicka på en länk för att uppdatera dina arbetsuppgifter. Klickar du på det? Förklara gärna du svara Ja/Nej	Du får ett samtal från någon som påstår sig vara från IT-supporten och ber om dina inloggningsuppgifter för att lösa ett problem med ditt konto. Ger du ut dina inloggningsuppgifter? Förklara gärna du svara Ja/Nej	Hur ofta deltar du i cybersäkerhet utbildningar på din arbetsplats?	Hur bekväm känner du dig med att rapportera misstänkta cybersäkerhetsincidenter till din IT-avdelning?	Hur tillfredsställande anser du att din nuvarande kunskap om cybersäkerhet är för att utföra ditt arbete effektivt?	Hur effektiva tycker du att de nuvarande cybersäkerhet utbildningarna på din arbetsplats är för att förbereda dig på att hantera potentiella hot?	Du upptäcker att din arbetsdator agerar konstigt och visar tecken på skadlig programvara. Hur skulle du hantera detta?	Du märker att din kollega använder sitt personliga USB-minne för att överföra filer till arbetsdatorn. Vad skulle du göra i denna situation?	Har du några förslag på hur den nuvarande utbildningen kan förbättras för att bättre möta era behov och utmaningar?

1	Nej, jag hade behövt mer information innan så att det inte blir några konsekvenser av nedladdningen.	Nej då det finns risk för bedrägeri.	Nej, jag hade behövt ställa följdfrågor som till exempel varför dom behöver mina inloggningsuppgifter och sagt att det inte känns bekvämt att lämna ut dom uppgifterna.	4	5	5	4	Går direkt till IT och ber dom kolla på det.	Skulle berätta att det finns konsekvenser till det men samtidigt är det varje persons ansvar att sköta det själv.	Tyvärr inga förslag.
2	Nej	Nej	Nej	5	5	4	4	Skicka den till soptunnan	Skicka usbn till soptunnan	Utbildningarna ska innehålla aktuella videos som visar hur bedragare/hackare jobbar för att komma åt information och pengar.
3	Nej	Nej	Nej	1	3	2	2	Ringa IT	Rapportera till chef	Fler utbildningar
4	nej	nej	nej	3	2	2	4	kontakta	be den att	mer

								en teamledare oh sedan felanmäla	sluta och kontakta teamledare.	utbildningar på arbetsplatsen
5	Nej	Nej	Nej	3	5	5	5	Börja med att starta om datorn, alternativt stänga ner och sedan anmäla felet.	Det beror lite på vilken kollega, (lite känsligt) och fråga rakt ut vad sysslar du med?!	
6	Nej, Jag har inte riktigt koll på vart USB:et kommer ifrån därför kommer jag både ställa mer frågor och eventuellt inte använda den	Nej, Det är ju phishing	Nej, IT ska inte ringa oss utan bara vi ringer dem	5	4	5	5	Jag rapporterar det till vår IT-system	Jag skulle fråga närmaste chef om detta är tillåtet eller ej	Mer praktiska moment
7	Nej - fråga mer om USB	Nej - rör inte någon kommunikation från okänd avsändare	Nej - kollar med kollegor och/eller chef innan jag går vidare	2	4	3	3	Kontaktar IT för en prognos om datorn om det är möjligt	Jag antar att kollegan är medveten om riskerna men påpekar det ändå, om de fortsätter så litar jag på att det är säkert och låter det vara.	Inga förslag

8	Nej vet inte om det finns virus på USB-stickan	Nej, detta sker via annat system	Nej, det gör jag aldrig	4	4	4	3	Kontakta IT supporten	Berätta för Hen att det inte är ok	Nej, det är det vi behöver lära oss
9	Nej. Inte för att jag direkt misstror kollegan men jag hade ifrågasatt det. Jag hade inte använt USB-minnet eftersom det inte är etiskt korrekt samt att det inte finns någon rimlighet varför någon skulle be någon annan att göra det.	Nej. För att vi alla borde veta bättre.	Nej. Jag hade bet att få ringa tillbaka när jag stämt av med lokal IT person.	3	5	4	5	Gå direkt till lokal IT support samt inte öppna mailen eller andra system.	Ifrågasätta syftet direkt till personen.	Inte i nuläget.
10	nej	nej	nej	2	5	4	5	Be en kunnig person om hjälp	Fråga personer varför hen gör detta	fråga om man är osäker på något
11	Nej	Nej	Nej	3	5	5	5	Okända popup, okända appar dyker upp. Jag kopplar ifrån internet, startar datorn i felsäkert läge. Installerar ett antivirus	Informera kollegan att detta kan leda till säkerhetsbrist och ber kollegan att ta loss USB-minnet.	Informera kollegan att detta kan leda till säkerhetsbrist och ber kollegan att ta loss USB-minnetUtbildningen ska

								program.		innehålla alla fundamentala delar för att stärka din kunskap om cybersäkerhet. Allt från begrepp till vad det innebär säkerhetsmässigt i slutändan. Detta för att förstå specifika hot och utmaningar och implementera dessa oavsett vilken verksamhet du jobbar inom.
12	nej, inte om jag inte får information om varför.	Nej	Nej	3	5	4	4	Stänger ned och rapporterar felet	Fråga varför, alt. meddela chef	Olika övningar så att alla är säkra på hur de ska agera
13	Nej	Nej	Nej	4	4	4	4	Stänger	Ta det	

								av datorn och kontaktar IT	med närmsta chef	
14	Nej	Nej	Nej	4	5	4	5	Gå till IT-ansvarig på min arbetsplats	Rapportera händelsen till närmsta chef	Tycker att vi har bra utbildningar som förbereder en vid en sådan situation.
15	Jag tror att jag skulle hämtat filen om det var en kollega som jag litade på. Om det däremot var en kollega som jag inte pratar så ofta med så hade jag ifrågasatt vad som fanns på USb minnet och varit mer kritisk.	Nej eftersom det kan vara ett bluffmail. Jag vet att man aldrig ska klicka på länkar från okända personer.	Nej det hade jag inte gjort då det finns personer som påstår sig vara till exempel IT-supporten för ett företag men som sedan visar sig vara en bluff. Detta kan ge stora konsekvenser som att pengar försvinner från sparkontona osv.	3	3	3	3	Jag tror att man ska stänga av datorn på direkten och kontakta någon på arbetsplatsen om vad som har hänt. För om min dator har blivit utsatt behöver detta åtgärdas så fort som möjligt.	Jag skulle sagt till chefen om detta då kollegan döljer någon typ av information som inte ska finnas i arbetsdatorn	Att arbetet ska skicka ut fler tester om bluffmail och bluffar på teams så vi får lära oss hur typiska bluffmail ser ut och lära oss hur vi ska hantera dem.

16	Nej	Nej	Nej	3	5	4	4	Stänga av datorn och sedan ringa IT.	Prata med kollegan	Nej
17	Nej, vi ska inte behöva externt USB för att utföra arbetsuppgifter.	Nej, anmäler mailet och raderar det.	Nej. Ger aldrig ut inloggningsuppgifter, IT-supporten kommer in på min dator utan mina uppgifter om de behöver.	2	4	5	3	Dra ut nätverkskabeln, stänga ner datorn och kontakta IT.	Ifrågasätta vad kollegan gör, och sedan anmäla till chef/IT.	Mer praktiska tester och faktiska exempel där företag blivit drabbade.
18	Nej	Nej	Nej	4	5	5	4	Anmäla det	Stoppa kollegan	nej
19	Nej, utan någon slags information om vad USB-minnet innehåller eller att jag kan se det själv först skulle jag inte ta emot det.	Nej, raderar det istället.	Nej, om jag är medveten nog att veta att det inte finns något problem med mitt konto kan jag lägga på samtalet eller också välja att inte svara om det är ett okänd nummer som	3	4	5	2	Försöka ta bort programvaran, alternativt be om hjälp om jag inte kan hantera det själv.	Egentligen inte min ensak, men av rent intresse skulle jag fråga varför den används och vad den används till.	Prata mer om det under möten kanske? Hur vi ska agera och vad vi ska göra om något sådant händer.

			ringer.							
20	Jag vill säga nej direkt men jag hade absolut ifrågasatt varför det kommer på en USB och inte skickas eller läggs på våra gemensamma ytor.	Nej	Nej	4	5	5	4	Beror på hur den agerar, ofta agerar den konstigt utan att ha skadlig programvara :) Troligtvis hade jag startat om den till att börja med. Beroende på hur den agerar hade jag troligtvis kontaktat servicedesk eller lokala IT (***)	Ifrågasätta vad som sker och om misstanke finns att USB-minnet är personligt skulle jag kontakta chefen.	Flera obligatoriska moment under utbildningens gång, ex. tester som man måste klara av.
21	Nej	Nej	Nej	5	5	5	5	ringer it-support	Förklarar för honom att det inte funkar så	Kanske mer "praktiska" moment, tester osv.
22	Nej	Nej	Nej	5	5	4	5	Stänga av och ge till närmaste IT	Kontakta närmaste chef och anmäla till ledningen	Det finns alltid förbättringsarbeten och utbildningar för

										djupare kunskap
23	Nej, då vanligtvis har vi inga USB som används på jobbet	Tar bort mejlet och anmäler som bluff	Lägger på samtalet	5	4	5	4	Ringer vår support nummer	Talat med närmaste chef om det ska vara ok	
24	Nej. jag vet inte vad minnet kan innehålla för skadligt.	Nej	Nej. Ger aldrig ut sådana uppgifter.	5	5	4	4	Stänga ner datorn och kontakta IT	Om jag inte pratar själv med kollegan så ber jag chefen prata. Meddelar Chefen oavsett.	Att den hålls så aktuell det går, bedragarna ligger ändå alltid steget före.
25	Nej, velat ha med info om vad det gäller och innehåller isf. Annars utgår jag ifrån att min kollega klarat det själv.	Nej	Nej, inte utan att säkerställa att det verkligen är så.	5	5	4	5	Kontaktar IT säkerhet eller närmsta chef.	Kontakta min chef situationen.	Det är faktisk redan bra, lärorikt och tänkvärt. Mycket bra dessutom att det sker regelbundet.
26	Nej	Nej. Rapporterar nätfiske.	Nej. Går inte att identifiera personen.	5	5	4	3	Koppla av nät och meddelar IT-avdelning	Berätta att det är fel och meddelar IT-avdelning/chef	mer interaktiva och licensierade utbildningar.
27	nej har inte koll på vad finns i den USB	Nej	Lägger på samtalet	4	3	2	4	Talar med chefen	Talar med chefen	
28	ja, beror lite	Nej, Vi	Vet inte	5	5	4	4	Kolla	Frågat vad	Oftare

	på vilken kollega, men jag hade litat på at min kollega inte ger mig något skumt.	har fått utbildning. Phishing. Vi anmäler det som bluffmail.	vad jag hade gjort i den situationen då det aldrig hänt. Men om man ska vara korrekt så hade man väl bett o lägga på och ringa upp den interna IT desken.					med IT-avdelningen.	hen håller på med.	och uppdaterat efter samhället. Bedragarna hittar på nya sätt hela tiden.

Appendix E. AI statement

Through the process of writing our bachelor's thesis, we have leveraged the capabilities of artificial intelligence as a tool to enhance various aspects of the writing. The core ideas, analysis, and overall content of the thesis are entirely our own work. AI has been used as a supportive mechanism to improve the quality, structure, and language of the final bachelor's thesis report. One of the key ways we have utilized AI is in refining the academic language and grammar of the text. AI has helped us identify and correct grammatical errors, inconsistencies, and elevate the academic language.

Additionally, we have relied on AI to assist in the structuring of our bachelor's thesis. This includes using AI to generate potential section headings that effectively capture the essence of the content and ensuring logical coherence and flow from section to section.