JÖNKÖPING UNIVERSITY
Jönköping International Business School

Guardians at the Gate: The Influence of Senior Management on Cybersecurity Culture and Awareness Training

A Qualitative Multiple Case Study

BACHELOR'S DEGREE PROJECT
THESIS WITHIN: Business Administration
AUTHORS: Adam Karim & Alexandra Törnqvist
TUTOR: Emma Stendahl
JÖNKÖPING December 2023

Bachelor Thesis in Business Administration

Title: Guardians at the Gate: The Influence of Senior Management on Cybersecurity Culture and Awareness Training

Authors: Adam Karim & Alexandra Törnqvist

Tutor: Emma Stendahl

Date: December 2023

Key Terms: Cybersecurity, Cybersecurity Culture, Senior Management, Awareness Training

Abstract

Background: Organisations are left vulnerable and susceptible to cyber-attacks due to the digitisation of information and dependency on information and communication technologies. As a result, the critical need for organisations to hinder, protect and preserve their cyberspace from multiple threats is emphasised. Due to human error being accountable for most electronic data breaches, a resilient cybersecurity culture is desired. To minimise cybersecurity threats, a human-inclusive strategy must be implemented in the culture and the inclusion and engagement of strong leadership within senior management.

Purpose: The purpose of this study is to explore senior management's role in cybersecurity culture and particularly, its influence on awareness training.

Method: The research is based on an interpretivist paradigm and adheres to abductive reasoning. Through the usage of semi-structured interviews and the utilisation of non-probability sampling, qualitative data was produced, and a multiple case study was conducted.

Conclusion: Senior management influences the practical implications in the organisation, such as training, as well as the assumptions and beliefs of its employees. Senior management influences the engagement, involvement, and responsibility of protecting and safeguarding the organisation's assets, and how this is reciprocated to the whole organisation. Furthermore, senior management addresses and manages the priority of cybersecurity in the organisation. Thus, employee behaviour and attitude are greatly impacted by senior management engagement and presence, showcasing a positive correlation between senior management influence and employee behaviour and beliefs.

Acknowledgement

Throughout this thesis process, we have had the great honour of receiving invaluable support from various people and want to express our gratitude.

First and foremost, we would like to thank Emma Stendahl, our supervisor, whose support, guidance, and feedback have been of great significance. This thesis would not have become what it is without you.

Secondly, we want to convey our appreciation to all participants who shared their valuable insights and experiences for our data collection, without their contributions, this thesis would not have been possible.

Lastly, we want to thank Catharina Tornqvist for her engagement in this thesis. Your valuable network and time have helped us gain access to significant interviewees. Your participation has contributed immensely, and for that, we are ever thankful.

Adam Karim

Alexandra Törnqvist

Table of Contents

1. Introduction

This chapter introduces cybersecurity, cybersecurity culture and leadership, and the potential influence on awareness training. The reader will be provided with an overview of the research background, problem discussion and purpose, key concepts and be presented with the research question.

1.1 Background

Cybersecurity attacks have profoundly increased over the last few years as organisations have become more reliant on information, information technology and communication technology (Alshaik, 2020). The National Institute of Standards and Technology (n.d) describes a cyber-attack as an attempt to disrupt, disable, damage, or maliciously manipulate a computing environment through cyberspace to compromise or tamper with data integrity. In 2021, an average of 771 cyberattacks a week were executed on Swedish organisations, an increase of 153% from 2020 (Check-Point, 2021). According to Check-Points Cyber Security Report (2021), the manufacturing industry, which is the most targeted, stood for 1086 cyber-attacks per week, with a 30% increase from 2020, whilst the government and military were subjected to 944 attacks a week, a 148% increase.

Organisations are left vulnerable and susceptible to cyber-attacks due to the digitisation of information and dependency on information and communication technologies, ICT (Von Solms & Van Nierkerk, 2013). Although ICT has commenced as an easier and more accessible technological instrument to share information, gather knowledge, and communicate in organisations (Von Solms & Van Nierkerk, 2013), the critical need for organisations to hinder, protect and preserve their cyberspace from multiple threats is emphasised. Additionally, cybersecurity threats can include, but are not limited to, software failure, spam, phishing attacks, and human error. Nonetheless, according to Reid & Van Niekerk (2014), humans are the weakest component of any cybersecurity programme.

To minimise cybersecurity threats created by the human factor and to implement policies, training and knowledge, a resilient cybersecurity culture is necessary (Bada et al., 2021). According to DaVeiga et al. (p.92, 2020), Cybersecurity culture is "*contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and an understanding of how to implement* *requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives."* Additionally, Mwim & Mtsweni (2022) state that to effectively combat cybersecurity threats, a more human-inclusive strategy in the culture must be implemented. Similarly, the UK Information Commissioner's Office, ICO (2019) stated that human error was to be held accountable for 90% of electronic data breaches. Modern technology has demonstrated that it is unable to ensure the protection of people, organisations, nations, nor can it regulate human behaviour (El-Bably, 2021).

To manage human error and aid in forming cybersecurity culture, the most fundamental step is proactive leadership (Huang & Pearlson, 2019). Huang & Pearlson (2019) state that organisational leadership, also referred to here as senior management, has become an essential factor in an organisation's capacity to successfully decrease cybersecurity risks and promote a culture of cybersecurity awareness. Similarly, to address one of cybersecurity cultures weakest links, poor leadership, senior management must promote leadership (Banks, 2016). Indeed, for organisations to develop a cybersecurity culture, an excellent leadership team within senior management, to oversee awareness training and direct employees in a secure cybersecurity manner, that aligns with the organisation's objective, is required (Humaidi & Balakrishnan, 2015). Moreover, to further implement cybersecurity culture and manage human error, awareness training is crucial. Security awareness training is a performance instrument used to alter human perception associated with knowledge, attitudes, and behaviour to prevent intended and unintended cyber harm (Mwim & Mtsweni, 2022). Security awareness training aims to reduce user related faults, theoretically eliminate human error, and increase the effectiveness of security systems and processes from the user's perspective (Siponen, 2000).

The significance of a cybersecurity culture is also shown in organisational performance. Organisational performance refers to three overall meters of performance, financial, market and shareholder value (Mejia, 2019). It is widely and commonly believed by researchers, that cybersecurity preparedness can provide organisations with growth and competitive advantages (Li & Liu, 2021). Similarly, organisations with a strengthened cybersecurity readiness can manage and mitigate cyber-attacks far more efficiently, which positively impacts the organisation's overall performance, including financial outcomes (Mejia, 2019).

Thus, through examination of the relationship between cybersecurity culture and senior management and the concerning increase in cyber-attacks, the urgent need for organisations to implement a cybersecurity culture is prevalent. It is evident that cybersecurity threats must be managed and minimised, since if the issue is left unaddressed, it will confront and impact an organisation's culture, leadership, and performance.

1.2 Problem Discussion

The concept of cybersecurity culture is relatively underexplored, with research primarily conducted in the last decade (Park & Chai, 2018). Prior research has concentrated on four main factors: technological solutions to cyber harm (Holstein et al., 2015), the human factor of cybersecurity risk (Knowles et al., 2015), security awareness training, and the effect of cybersecurity culture on organisations (Hasan et al., 2021). Indeed, the most significant previous research provides literature on technological solutions, focusing on technology-advanced measures and procedures to limit cyber-attacks. Secondly, previous research extensively provides literature on the human factor, stating that employees are the first line of defence and simultaneously the weakest link (Ani et al., 2019), noting the need for security awareness training amongst employees. Lastly, the literature delivers an extensive array of the effects of cybersecurity culture on organisations, specifically on organisational performance. Hasan et al. (2021) state that implementing a cybersecurity culture positively impacts organisational overall performance and, therefore, is in the interest of senior management and shareholders. However, the literature on cybersecurity culture has concentrated on technological-level solutions and therefore, the literature lacks a clear theoretical standpoint and concrete human-related measures organisations can implement to improve their cybersecurity culture (Carpenter, 2019; Park & Chai, 2018). Additionally, a recent study from Gcaza & Von Solms (2017) explains that the absence of these concepts suggests that senior management’s influence on cybersecurity culture is poorly comprehended and understudied. As a result, measures organisations can take to enhance their cybersecurity culture and standards to verify these measures are unclear (Gcaza & Von Solms, 2017).

Even though, in recent years, the literature on cybersecurity culture has increased, current cybersecurity culture theories cannot be fully applied to organisations and, more importantly, senior management as they are substantially lacking in providing measures for managers to manage employees and human error (Gcaza & Von Solms, 2017). Indeed, human-inclusive methods are needed to protect organisations from cyber harm, specifically human error. As a result, it is necessary to research how senior management can implement these methods to create a resilient cybersecurity culture. Still, current theories lack incorporation of senior managers' influence on cybersecurity culture, which has proven to significantly contribute to increased cybersecurity awareness in organisations (Mwim et al., 2023). As aforementioned, current literature showcases how organisations' cybersecurity strategies are driven by technology, which are not designed to suit individual organisation's unique security needs (Van't Wout, 2018). Current theories focus on technological solutions by increasing organisational security measures and regulations limiting employees' ability to cause cyber harm unintentionally (Renaud & Zimmermann, 2019). The current approach essentially names employees as the villains, and measures are taken to limit employees from "unsafe" behaviour rather than external threats. Nonetheless, Renaud & Zimmermann (2019) suggest that employees' place in cybersecurity culture needs to be re-examined, as treating employees as the problem has proven ineffective.

Additionally, Shultz (2005) states that theories have neglected senior management's influence on human behaviour and its importance in cybersecurity. The critical role of senior management in cybersecurity is overlooked in previous research, and even though leadership practices are vital to managing human error (Letho & Limnéll, 2021), current research does not implement or cater to the effects and influence of senior management. Accordingly, research by Mwim & Mtsweni (2022) states that an efficient strategy combines assistance and policies from senior management leaders with security awareness training to accomplish a cybersecurity culture. Nevertheless, previous literature lacks an understanding of the influence of senior management, strategies for managing the influence and how to leverage it to enhance cybersecurity culture. This calls for further investigation into the relevance of senior management in cybersecurity and whether the role of senior management can additionally modify the behaviour of employees. Indeed, Triplett (2022) states that the promotion of cybersecurity awareness and training falls under the responsibilities of senior management.

The lack of adequate research on cybersecurity solutions for managing human error has consequently neglected research on implementing these solutions in organisations, thereby overlooking senior management's role and influence on cybersecurity culture. Indeed, senior management's influence ranks as a significant subject matter (Mwim et al., 2023). Thus, the need for research on senior management's influence on cybersecurity culture and awareness training is necessary for organisations to protect and safeguard organisational assets and to address the literature gap. Developing an understanding of the theoretical impact senior management has on cybersecurity culture, can aid the implementation and comprehension of cybersecurity strategies. As a result, the research seeks insight into the intricate interrelationships between senior management, cybersecurity culture and the efficacy of awareness initiatives.

1.2 Purpose

The purpose of this study is to explore senior management's role and their influence on cybersecurity culture within organisations. The research aims to examine the process through which senior management engages and integrates awareness through engagement and training to combat cyber threats and establish a resilient cybersecurity culture.

1.3 Research Question

To attain the research purpose of this study, the following research question was developed:

RQ1: How does the role of senior management influence the cybersecurity culture, and how does it influence the implementation of awareness training?

1.4 Delimitations

The scope of the research includes limitations. The study is restricted to Swedish organisations, requiring additional elements to be taken into consideration while employing various settings. Furthermore, the study is based on Swedish organisations, in contrasting sectors, limiting comparability.

2. FRAME OF REFERENCE

This chapter's purpose is to provide the reader a theoretical framework of the current literature on cybersecurity culture, senior management in cybersecurity and awareness training. This chapter aims to describe the method of identifying relevant literature as well as increase knowledge through a literature review.

2.1 Method for Literature Review

The research purpose requires information and data to be investigated and analysed from secondary sources. The sources used are essential to verify the reliability and accuracy of the research and conceptual framework (Collis & Hussey, 2014). The frame of reference was developed by characterising keywords and key terms within cybersecurity, cybersecurity in organisations and cybersecurity culture. Keywords used were "cybersecurity," "cybersecurity culture," "senior management," "senior management and cybersecurity culture," "awareness training," and "awareness training and cybersecurity culture." These keywords were used for literature searches in three databases: Google Scholar, Primo and Science Direct.

The literature search was limited to the publication year range 1985-2023. The wide range was used to explain the expanding field of cybersecurity literature and the substantial improvement of research done in the area, as well as to consider frequently cited work. Collis & Hussey (2014) state that frequently cited arguments become more credible. The wide range also confirmed the limited research conducted on senior management and cybersecurity culture. However, the research was focused on studies conducted in 2019-2023, to accurately describe the current research on cybersecurity.

An emphasis on the impact score of each journal was maintained to ensure the accuracy and applicability of publications. The Academic Journal Guide (AJG) was used to evaluate the ranking of journals and guide the authors in implementing and maintaining high-scoring journals with relevant research. Scores exceeding 3.0 were highly regarded journals. High-scoring journals further guarantee the research's relevancy.

The literature was selected based on its correspondence to the quality requirements and relevance to senior management's influence on cybersecurity culture. The evaluation focused on identifying discussions relevant to various aspects of the research topic, including cybersecurity culture, the role of senior management, and awareness training. The initial assessment of the literature analysed and identified fundamental relationships between senior management and cybersecurity culture.

2.2 Literature Review

2.2.1 Cybersecurity in Organisations

The increase in cyber-attacks in the last decade has negatively affected global organisations' overall performance (Hasan et al., 2021). Organisational cyberattack costs exceeded 4.45 billion dollars in 2022 and are projected to surpass 8 trillion by 2023 (Freeze, 2023; IBM, 2023). Moreover, Hasan et al. (2021) state that 49% of businesses experienced financial losses because of cyber-attacks in 2021 and the FBI (2022) projects these statistics to worsen as cyber-attacks increase in size and sophistication. Hasan et al. (2021) continue that organisations must strengthen their cybersecurity to mitigate cyber harm as organisational security performance, which improves organisational revenue, is favourably impacted by organisational cybersecurity preparation. Accordingly, researchers hold a common belief that cybersecurity solutions and readiness may cater a substantial growth advantage for organisations (Li & Liu, 2021). However, prior research on factors that affect organisations knowledge and awareness of cybersecurity are scarce (Hasan et al., 2021).

Recent research states that cybersecurity readiness, defined as an organisation's ability to manage and mitigate cyber-attacks, can benefit an organisation's competencies and performance (Hasan et al., 2021). Similarly, Smith et al. (2010) and Tsou & Hsu (2015) state that organisations may enhance their reputation and financial performance by establishing cybersecurity practices, such as awareness training. Additionally, Park & Chai (2018) gives insight that organisations with established cybersecurity readiness create stronger security control systems, system management and emergency preparation, which considerably influences organisational core competencies and attains higher performance. Subsequently, if an organisation's cybersecurity knowledge is poor or inconsistent, and its members are unwilling to adopt cybersecurity practices, creating an adequate degree of cybersecurity to safeguard its assets will be challenging. Consequently, the organisation's financial performance may decline (Hasan et al., 2021).

Additionally, cyberattacks have significant financial consequences and detrimental impacts on organisations (Nicholson, 2019). That is loss of sales, damage to organisational reputation, and leakages of sensitive material and information (Nicholson 2019). Indeed, companies may choose not to report cyber-attack occurrences to protect organisational reputation or prevent humiliation, signifying that the actual costs of cyberattacks may be higher than initially reported (Pearson, 2014). Furthermore, Berlilana et al. (2021) conclude that due to the rising regularity of cyberattacks and the extensive repercussions an organisation may bear from it, it is essential for organisations to implement appropriate and suitable cybersecurity practices to protect firm assets. However, despite the importance of cybersecurity readiness on organisational performance, Hasan et al. (2021) present that an examination of the research reveals that organisations' preparedness for cybersecurity attacks and harm is insufficient and not properly thorough, nor has the impact on organisational performance been empirically validated. Notably, this warrants further research into the applicability of cybersecurity and whether cybersecurity practices can enhance organisational performance. Indeed, organisations must secure a degree of cybersecurity readiness to protect assets and limit cybersecurity attacks to strengthen their performance and reputation (Smith et al., 2015; Tsou & Hsu, 2015; Park et al., 2017).

2.2.2 Cybersecurity Culture

Cybersecurity culture refers to a culture with security policies and procedures directed by management to alter human perception associated with security knowledge, attitudes, and behaviour to prevent intended and unintended cyber harm (Mwim & Mtsweni, 2022). Al Hogail (2015) presents that cybersecurity culture's aim is to support all the operations in an organisation to protect organisational assets to the extent that cybersecurity becomes a routine part of every employee's daily tasks. Indeed, organisations' overall cybersecurity readiness is enhanced by cybersecurity culture (Gcaza & Von Solms, 2017). Da Veiga (2016) concludes that despite the importance of creating a cybersecurity culture being acknowledged, research that focuses specifically on establishing and measuring cybersecurity culture is still in its initial stages, and there are no established standards to verify the solutions (Gcaza & Von Solms, 2017), demonstrating a literature gap.

Prior cybersecurity research has focused on technological solutions (Holstein et al., 2015) and studies aimed at creating effective cybersecurity regulations within organisations. Still, cybersecurity risk persistently increases (Van’t Wout, 2018). According to Van’t Wout (2018), the primary cause of the rise is the continuous effort concentrated on technological solutions, which cannot eliminate cybersecurity concerns due to human vulnerability. Indeed, an organisation’s cybersecurity readiness and implementation of strategies may be reduced or inconsistent if they only adhere to the technological aspect. Organisations may face cybersecurity concerns that are singular to their specific information assets and may find it challenging to protect and preserve their organisations with standard technological solutions (Pollini et al., 2021). As a result, cybersecurity culture requires technological solutions to incorporate human elements, as human-independent technology has proven ineffective at protecting and preserving organisational assets (Pollini et al., 2021). Accordingly, organisations without a fundamental grasp of cybersecurity and suitable implementation measures led by senior management may have an increase in employee errors and limit the capacity to safeguard the firm against cyber harm (Van’t Wout, 2018). Similarly, research conducted by Jeong et al. (2019) states that human factors necessitate using novel methods owing to their subjectivity and complexity to fully appreciate how they influence cybersecurity. Additionally, whether deliberate or not, employee negligence and potential cybersecurity ignorance have emerged as a primary risk of cybersecurity threats (Ramsluckan et al., 2020). As a result, organisations that do not incorporate human-related measures cannot fulfil the requirements of an overall cybersecurity culture, minimising their cybersecurity readiness (Gcaza & von Solms, 2017), which in turn can affect organisational overall performance. Therefore, Mwim et al. (2023) suggest that for a cybersecurity culture to be fostered, a more human-inclusive strategy must be implemented (Mwim & Mtsweni, 2022).

An effective strategy that can encourage a cybersecurity culture, according to Mwim & Mtsweni (2022), is through three crucial elements: security education, training, and awareness with support from senior management. These three factors are regarded as the most significant due to their immense relevance in developing, applying, and maintaining cybersecurity culture (Mwim & Mtsweni, 2022). Additionally, literature by Banks (2016) argues that the influence of senior management on organisational cybersecurity practices is the solution to fostering a cybersecurity culture amongst employees. Therefore, inadequate leadership in organisations is seen as the “weakest link” in cybersecurity culture, which compels senior management to establish management via security guidelines and educational awareness campaigns (Banks, 2016). Thus, the implementation of cybersecurity culture in organisations is used to prevent intended and unintended cyber harm, create support from senior management and mitigate human error.

2.2.3 Summary of Literature Review

The literature review introduces the critical role of cybersecurity in organisations by highlighting the negative performance effects caused by the increase in cyberattacks. Freeze (2023) continues to showcase the escalation of cyberattacks by forecasting the costs of cyberattacks to surpass 8 trillion dollars by 2023. A recurring concept across the literature is cybersecurity readiness and the ability of organisations to effectively manage cyberattacks. Implementing a strong cybersecurity culture within the organisation to effectively mitigate cyberattacks can enhance not only the overall organisational performance but also the company's reputation and financial stability (Smith et al., 2010; Tsou & Hsu, 2015; Park et al., 2017). However, Hasan et al. (2021) point out the lack of research confirming the impact of cybersecurity on organisational performance. The research of Mwim & Mtsweni (2022) and Al Hogail (2015) identifies developing a cybersecurity culture as crucial in improving an organisation's readiness against cyberattacks. A developed cybersecurity culture, directed by management, helps alter attitudes and behaviours toward cybersecurity throughout the organisation. However, researchers point out a significant gap in understanding what measures an organisation can take to improve its culture (Carpenter, 2019; Park & Chai, 2018; Da Veiga, 2016; Gcaza & Von Solms, 2017).

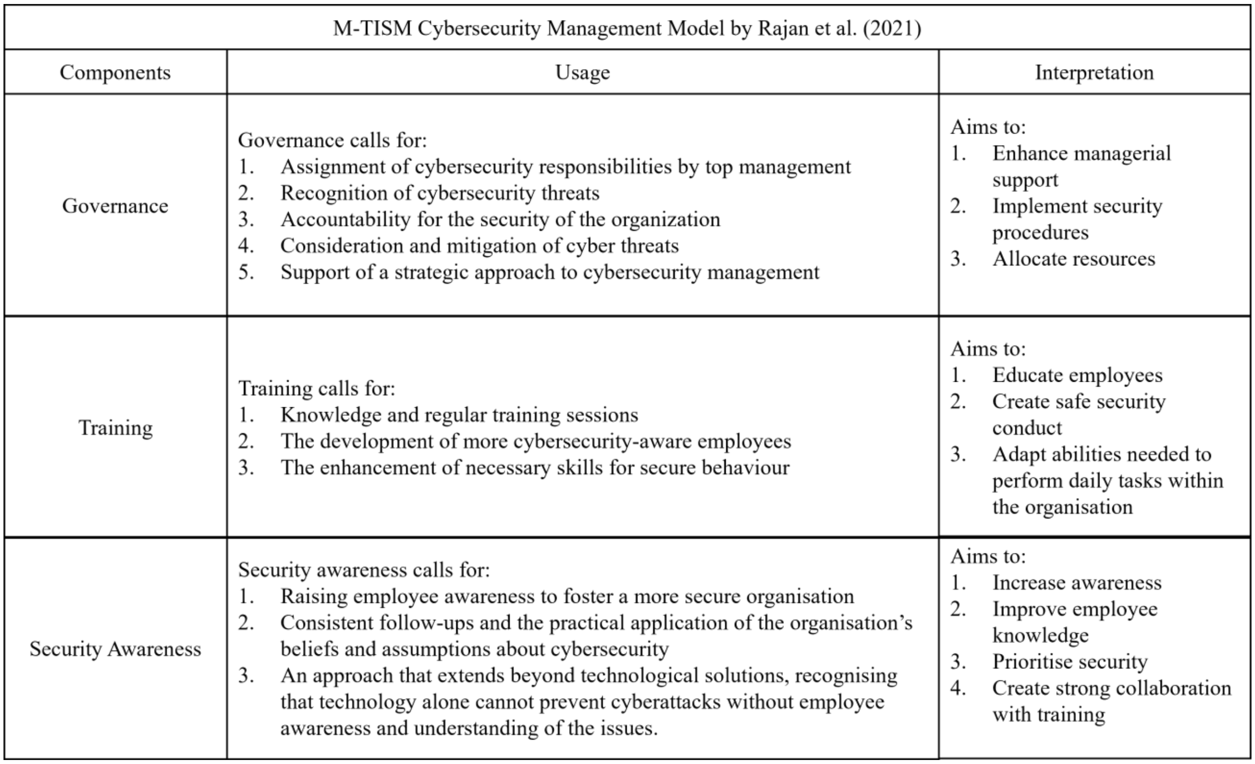
Finally, the literature review underscores the importance of managing the human element in cybersecurity, highlighting that human vulnerability and employee negligence are primary targets of cyber threats (Ramsluckan et al. 2020; Van't Wout 2017). Thus, the cybersecurity landscape is evolving from focusing on technological solutions to incorporating human-inclusive strategies (Mwim et al., 2023).

2.3 Theoretical lens

2.3.1 Cybersecurity Management

Strategic cybersecurity management is referred to as the capacity of an organisation to strategically safeguard its information resources, digital processes, and IT systems in a cyber environment that is ever-evolving (Ferdinand, 2015). Cybersecurity management's aim is to assist organisations in protecting their integrity of the data, through managerial controls (Ferdinand, 2015). Indeed, organisations that seek to manage cyber risks and informational threats, must understand the usage of cybersecurity management to operationalise more efficient strategies (Lee, 2020). Thus, examining strategic aspects of cybersecurity management in organisations is crucial (Rajan et al., 2021).

Prior literature has examined the individual effects of security awareness, technology, and leadership. However, few studies have been published on how these factors interact and how their relationship affects cybersecurity management, cybersecurity strategy, and its combined effect on cybersecurity culture (Rajan et al., 2021). The relevance of these factors calls for using the Modified Total Interpretive Structural Model, M-TISM, Strategic Cybersecurity Management model constructed by Rajan et al. (2021). The model aids in the process of identifying significant components in organisational cybersecurity, the links between them and making a hierarchical order of those factors (Rajan et al., 2021). The model presents seven components that impact cybersecurity management: Resources and Capabilities, Information Flow, Training, Alliance and Collaboration, Governance, Security Awareness and Technological Infrastructure. However, in this thesis, the components used will be limited to Governance, Training and Security Awareness due to their relevance to the research question. The conducted model demonstrates how information security theory can be enhanced by managing cybersecurity within organisations. The factors will help outline a theoretical framework for analysis, allowing for further interpretation of the empirical findings. Through the model, it has become prominent that the most critical factor affecting cybersecurity and information security within organisations is governance by senior management (Rajan et al., 2021). The model provides management insides and argues that organisations may improve their cybersecurity management by focusing on the variables and their interrelationships. Indeed, this model guides the influence of senior management and its influence on cybersecurity culture.



M-TISM Cybersecurity Management Model by Rajan et al. (2021)		
Components	Usage	Interpretation
Governance	Governance calls for: 1. Assignment of cybersecurity responsibilities by top management 2. Recognition of cybersecurity threats 3. Accountability for the security of the organization 4. Consideration and mitigation of cyber threats 5. Support of a strategic approach to cybersecurity management	Aims to: 1. Enhance managerial support 2. Implement security procedures 3. Allocate resources
Training	Training calls for: 1. Knowledge and regular training sessions 2. The development of more cybersecurity-aware employees 3. The enhancement of necessary skills for secure behaviour	Aims to: 1. Educate employees 2. Create safe security conduct 3. Adapt abilities needed to perform daily tasks within the organisation
Security Awareness	Security awareness calls for: 1. Raising employee awareness to foster a more secure organisation 2. Consistent follow-ups and the practical application of the organisation's beliefs and assumptions about cybersecurity 3. An approach that extends beyond technological solutions, recognising that technology alone cannot prevent cyberattacks without employee awareness and understanding of the issues.	Aims to: 1. Increase awareness 2. Improve employee knowledge 3. Prioritise security 4. Create strong collaboration with training

Table 1: M-TISM Cybersecurity Management

The interrelationship between Governance, Training and Security Awareness is significant in the M-TISM model and is valuable for managing cybersecurity in organisations. The model demonstrates that governance improves cybersecurity in organisations via allocating resources, producing, and implementing cybersecurity protocol, fostering a cybersecurity culture, participating in the engagement of cybersecurity initiatives, and assisting in the development and revision of cybersecurity policy (Wiley et al., 2020). Senior management should also promote training programs and security awareness. Firstly, by promoting training, senior management can enhance knowledge, support sensitive information exchange between employees, protect the organisation against cyber threats, support the development of cybersecurity culture (Li et al., 2019), and create aware and engaged employees. Employee's knowledge and abilities may be developed through training, which can increase their understanding of cybersecurity. Secondly, through governance and training, senior management can generate an aware employee. Training generates a more understanding and aware employee, which aids in maintaining information confidentiality, protecting organisational vulnerabilities, and detecting emerging threats quickly (Rajan et al., 2021). Thus, senior management needs to govern its organisation to make correct cybersecurity decisions, where the importance of training is communicated and acted upon, creating a secure and aware employee. Without one or the other, an organisation may find itself vulnerable and susceptible to cyber threats.

2.3.2 The Responsibility of Senior Management

Iovan and Iovan (2016) explain that senior managers play a critical role in cybersecurity management. Findings by Iovan and Iovan (2016) and Knowles et al. (2015) highlight the several important roles of senior management. The responsibilities of the senior management team include developing holistic strategies that cover all aspects of cybersecurity, prioritising investments, allocating resources, and establishing the standards and protocol needed to guide cybersecurity efforts in the organisation (Knowles et al., 2015). Von Solms and Von Solms (2004) explain that for security policies to be effective, they need to be integrated into the organisational culture. Indeed, for the integration to be successful, the policies and assumptions defined by senior management must align with the personal beliefs and assumptions of the staff (Von Solms & Von Solms, 2004). Von Solms and Von Solms (2004a) emphasise that the integration of the policies is a process that falls under the responsibility of senior management. Influencing employees of the organisation through specific policies and procedures to serve the interests of the organisation is a critical part of their role. By clearly defining and implementing these policies, senior management can guide employee actions in a way that aligns with the organisational goals and values (Von Solms & Von Solms, 2004). Furthermore, the attitude and participation of senior management toward cybersecurity have a positive impact on employee compliance with established policies (Puhakainen and Siponen, 2010). Additionally, Puhakainen and Siponen (2010) note that well-designed training programs endorsed by senior management can further improve compliance with organisational security policies. The commitment of senior management to cybersecurity initiatives is essential to communicate the legitimacy of these efforts (Tyler et al., 2007). James (1999) states that senior management participation and commitment lead to employee trust and compliance with organisational objectives. Additionally, it is essential to provide the tools necessary to measure and enforce compliance with security policies, as there is no use in establishing comprehensive organisational objectives without the ability to monitor their adherence (Von Solms & Von Solms, 2004). Not monitoring compliance can result in a false sense of security, as the policies are only effective if implemented by the members of the organisation.

2.3.3 Security Awareness

Senior management is responsible for acknowledging and addressing the threat of cyber-attacks through awareness (Zwilling et al., 2020). Zwilling et al. (2020) state that security awareness is an essential component of an organisation’s cybersecurity culture. If members of the organisation are not properly informed of cybersecurity issues, it is unlikely that technological systems safeguard the organisation alone (Dahbur et al., 2017; Wiley et al., 2020). Senior management plays a vital role in cybersecurity by providing necessary resources, support, and training programs while monitoring and participating in decision-making processes (Berry & Berry, 2018). Chen et al. (2006) suggest that improving cybersecurity awareness involves educating employees about company security guidelines, procedures, and practices. Efforts to improve cybersecurity awareness can involve training programs, workshops, and follow-ups. It is argued that with adequate security awareness, employees can become the best defence against security threats (Parsons et al., 2014). Uchendu et al. (2021) argue that the essence of security training is to prepare the employees with the necessary abilities and competencies to perform their tasks without creating cybersecurity vulnerabilities. However, Chapman (2020) underscores that just having knowledge about cyber threats is not enough. The emphasis is instead on the employees' adherence to established security guidelines.

While Uchendu et al. (2021) claim that communication between senior management and employees is critical for employees to become informed about security policies and protocols, they also highlight that training sessions to communicate security practices are not always as effective as they seem. A significant amount of the information from the training quickly fades. Hassandoust et al. (2022) clarify that employees may not be properly informed about cybersecurity because of several factors. For example, the lack of involvement in the policy-making process or no clear communication of individual responsibilities can lead to employees having insufficient information. Additionally, Ander (2022) emphasised that it is vital for employees to understand the reason behind the development to be inspired to participate in it.

3. METHODOLOGY & METHOD

The selected methodology and method will be presented in this chapter. The methodology outlines the research philosophy, approach, and design. The method is firstly described by introducing data collection secondly through the procedure used to acquire primary data and lastly, interview format and setting. To conclude, the chapter ends with ethical considerations.

3.1 Methodology

3.1.1 Research Philosophy

Research philosophy is described as the nature, scope, and development of research assumptions (Andriukaitené et al., 2018), which examines the partnership between the researchers and the research subject (Collis & Hussey, 2021). The researcher's background, philosophical knowledge and personal values may impact the chosen approach, and a research paradigm captures a researcher's viewpoint of the world consisting of ontological, epistemological, and methodological assumptions (Collis & Hussey, 2021). Ontology forms the foundation of all research, and the researcher's epistemological and methodological stance naturally follow (Grix, 2002). The methodological choices made in this thesis are closely tied to specific ontological and epistemological beliefs aligned with the interpretivist paradigm, such as subjective nature, contextual understanding, and multiple realities perspective. The research will be based on qualitative data. Firstly, the thesis aligns with a subjective nature, as it is recognised that each individual carries their views and experiences. Secondly, the role that senior management plays in cybersecurity is context-dependent and differs depending on each organisation, which indicates that every organisation carries its own understanding of the issue. Lastly, the authors have interviewed a range of positions, generating various perspectives and a range of realities. This thesis interlinks with the interpretive viewpoint due to interviewees having subjective opinions and perceptions about the role of senior management in cybersecurity culture, as well as how the organisation has formed these thoughts and experiences in their employees, constructing an overall organisational view of cybersecurity.

3.1.2 Research Approach

To add to the existing body of knowledge and to further theory development in the field, an abductive approach was aligned with the interpretivist paradigm. According to Saunders et al. (2019), an inductive, deductive, or abductive approach can be applied to theory development.

Considering the lack of relevant frameworks, it was concluded that the abductive approach fit the research aim of exploring senior management’s leadership practices and their influence on the cybersecurity culture within organisations. The abductive approach necessitates the use of a theoretical lens while simultaneously encouraging the identification and examination of novel concepts that differ from current theoretical frameworks (Hurley et al., 2021). Thus, the authors chose the abductive approach as it allowed for integrating prior knowledge and literature through a theoretical lens, including cybersecurity management, senior management, and awareness, that offered guidance (Hurley et al., 2021). However, considering the complexity of humans that arose throughout the thesis, the use of current literature to understand the research question was not sufficient. Indeed, the abductive approach allows for a novel perspective, which the authors champion for this thesis. Thus, the abductive approach was found to guide the authors in overseeing preconceived perspectives of senior management and constructing new narratives of the role of senior management in cybersecurity culture, leading to the development of new theories based on relevant findings (Tavory & Timmermans, 2014).

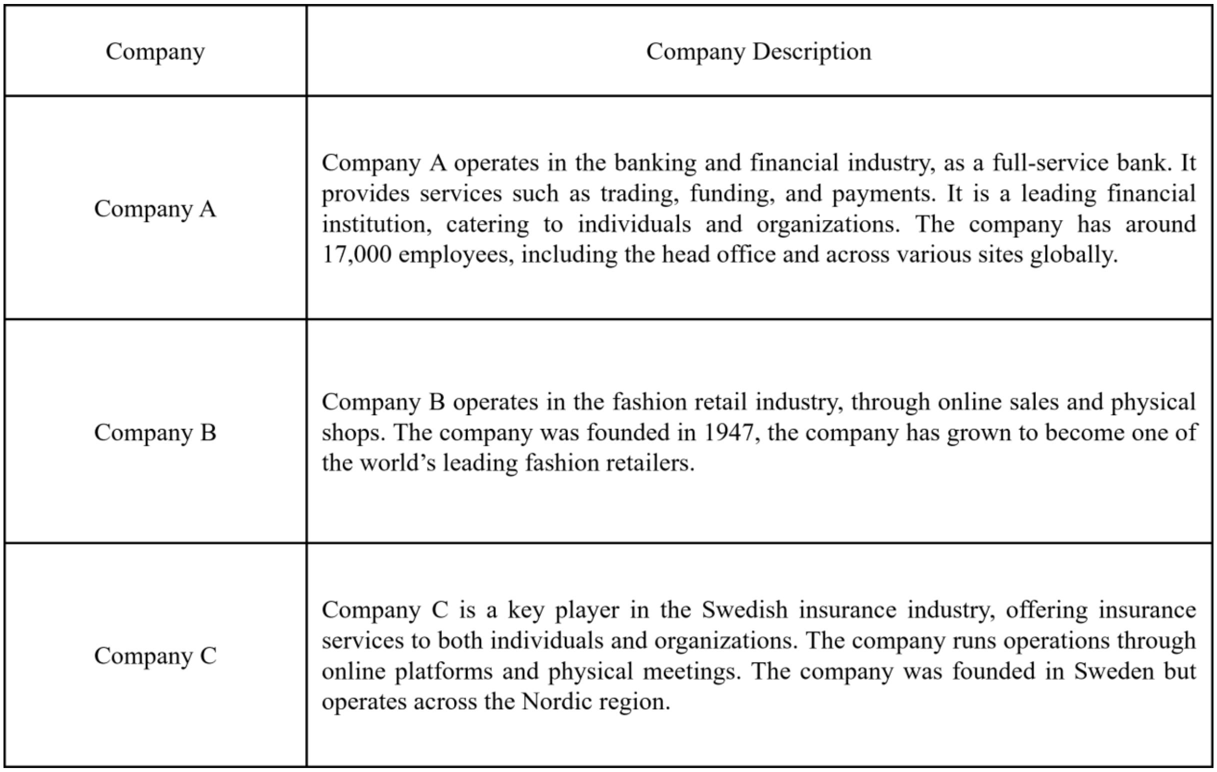
3.1.3 Research Design

To investigate the research question, the study will implement a research design described as an exploratory case study. The study aims to explore how senior management’s leadership practices influence the establishment of a cybersecurity culture. According to Collis & Hussey (2014), a case study is a methodology to gain in-depth insight into a phenomenon within its real-life context, making the importance of context essential. Furthermore, an exploratory case study might be used when the body of knowledge is insufficient and there are limited theories (Collis & Hussey, 2014). Given the study’s exploratory nature, it was fitting to characterise it as a case study with the inclusion of qualitative research interviews.

There are three types of approaches to research design to consider when carrying out a study. The three different approaches are called descriptive, explanatory, and exploratory design (Saunders et al., 2007). The exploratory approach is specifically compatible when exploring the research field of senior management because of the lack of existing theories and the current gap in the literature (Saunders et al., 2019). A multiple case study design will be utilised to understand the intricate relationship between senior management practices, awareness training, and the established company’s cybersecurity culture. The multiple case study design is aligned with the exploratory nature of the research question being investigated, making it an exploratory multiple case study. As highlighted by Eisenhardt & Graebner (2007), the strength of a multiple case study is its ability to help researchers trace out similarities and differences between the multiple cases being interviewed. Employing a multiple case study design is nonetheless grounded in alignment with the interpretivism paradigm, as it demands comprehensive investigation and a deep contextual understanding (Collis & Hussey, 2021).

3.1.4 Case Description

The primary data collection revolves around the three selected case companies: Company A, Company B, and Company C. In selecting these companies, three key criteria were considered to make the chosen companies relevant to the research. The first criteria considered were size and market presence. All three case companies are large-sized enterprises characterised by their significant market presence in each sector. The size not only refers to their significant employee counts and annual revenue but also the complexity of their decision-making processes. The second criterion considered was the handling of sensitive personal data. The selected companies handle large amounts of sensitive personal data, both customer and employee-related, which increases the importance of routine cybersecurity measures. It is important to note that the selected case companies operate across different industries. Therefore, cybersecurity compliance measures and regulations they must adhere to may vary depending on the nature of the data the companies handle. For example, compliance in the financial sector can be influenced by the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions ensure the protection of sensitive data (Gramm-Leach-Bliley Act, 2023). The final criteria considered was the companies' digital footprints. All three companies have a large part of their operations online. The online digital footprints arguably make organisations increasingly susceptible to cyber threats, elevating the need for an established cybersecurity culture.



Company	Company Description
Company A	Company A operates in the banking and financial industry, as a full-service bank. It provides services such as trading, funding, and payments. It is a leading financial institution, catering to individuals and organizations. The company has around 17,000 employees, including the head office and across various sites globally.
Company B	Company B operates in the fashion retail industry, through online sales and physical shops. The company was founded in 1947, the company has grown to become one of the world's leading fashion retailers.
Company C	Company C is a key player in the Swedish insurance industry, offering insurance services to both individuals and organizations. The company runs operations through online platforms and physical meetings. The company was founded in Sweden but operates across the Nordic region.

Table 2: Case Description

3.2 Method

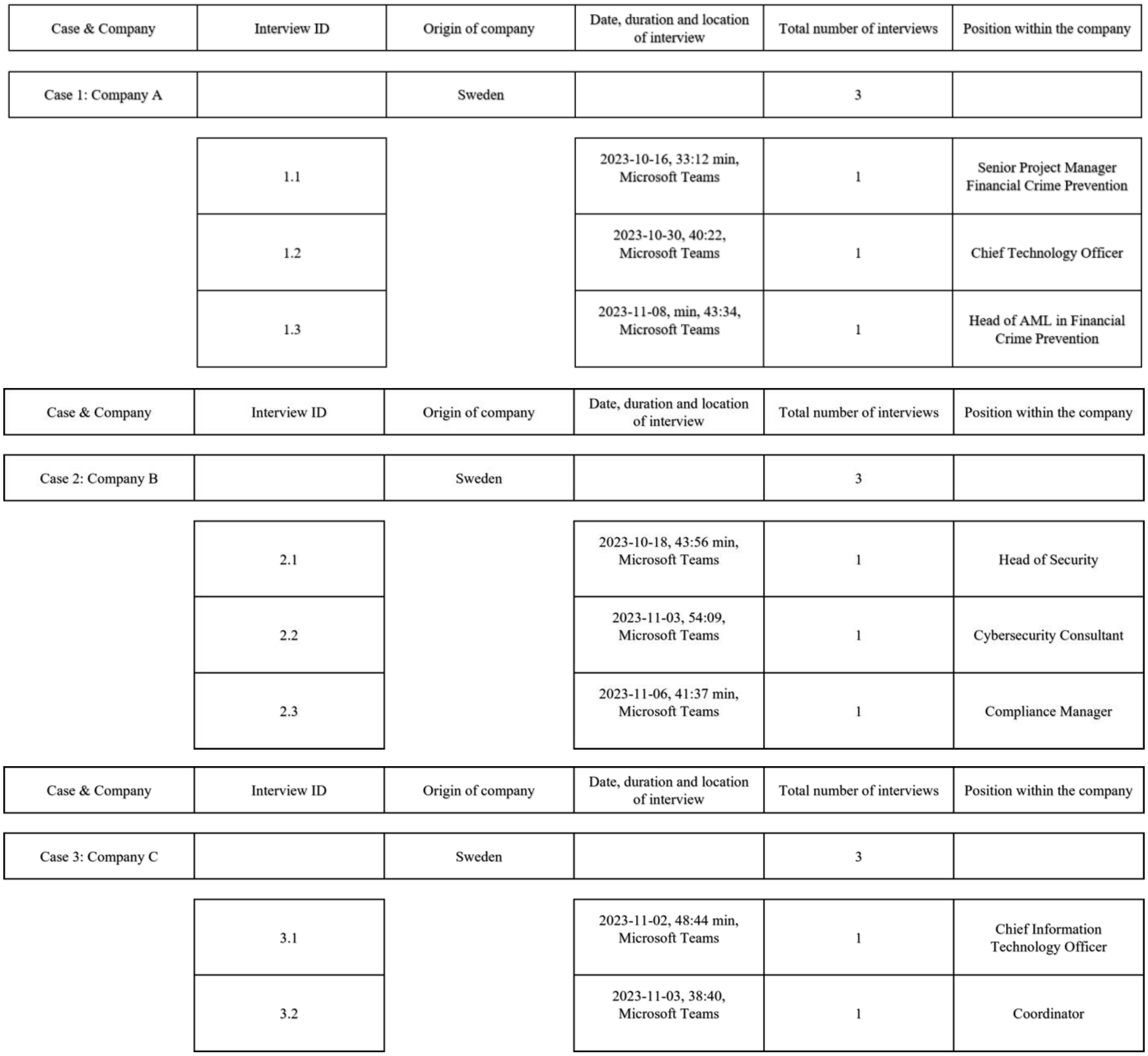
3.2.1 Data Collection

In this qualitative study, the data collection procedure used a multiple case study, where extensive and diverse data was gathered from various sources, including semi-structured interviews and documents. According to Creswell (2013), relying on a single source of data is insufficient to nurture an in-depth comprehension of the research. It, therefore, requires several types of qualitative data to be gathered. Indeed, primary data collection was applied through in-depth semi-structured interviews, which served as a critical source of information, allowing for new conclusions to be drawn from the data and providing a comprehensive overview of the respondents' perspectives and experiences. Further, secondary data was collected through reports and documents. Integrating the two data collection techniques enables the usage of triangulation in the research and provides the possibility to improve the quality of the data in the study further (Saunders et al., 2019).

3.2.2 Primary Data

In this research, qualitative methods were used to gather primary data and were conducted through semi-structured interviews. Interviews are frequently used in qualitative research and are fundamental for researchers to create a deeper knowledge of social phenomena (Gill et al., 2008). Similarly, according to Hox & Boeije (2005), a significant benefit of gathering primary data, through for example, interviews, is that it enables the implementation of theoretical concepts and research designs to be customised to the research question, which ensures cohesiveness throughout the research. In this research, semi-structured interviews were used to comprehend senior management's role in cybersecurity culture. The interviews allowed the authors to generate a structured interview whilst also providing the possibility to explore relevant concepts that arose during the interview (Adeoye-Olatunde et al., 2021). The interview was sectioned into five themes: i) Presentation of the Interviewee, ii) Cybersecurity, iii) Cybersecurity Culture, iv) Senior Management, and v) Awareness Training. Further, the semi-structured interviews in this study enabled the authors to identify cybersecurity factors, strategies and technological perspectives that influenced the interviewees' cybersecurity thoughts and experiences with senior management (Gill et al., 2008). The authors created an interview guide, which can be found in Appendix 3, in advance with relevant questions. The interviewees were supplied with the questions prior to the interview to foster a thorough discussion. However, providing questions to the interviewees beforehand can limit candid and outspokenness and create generalised answers (Silverman, 1997). Nonetheless, due to subject sensitivity, the authors recognised the need for the interviewees to prepare.

Before the interviews, the authors sent out an introductory email containing the background of the research, a description of the interview, the interview guide, and the consent form. All interviews were held on Microsoft Teams due to travel distance, time management, and accessibility, allowing less pressure on the interviewees. However, there are several limitations to conducting interviews through online meetings, notably the loss of body language, social cues, and facial expressions, as well as technical disruptions that may have diminished the effectiveness of the interviews (Van Zeeland et al., 2021). Furthermore, the interviews lasted thirty to sixty minutes, of which five minutes were used to explain the research being conducted, the consent form, offering anonymity and starting the recording and transcription. After the interviews, the authors gave each other constructive feedback, modified questions and sent follow-up emails to three interviewees for clarification.



Case & Company	Interview ID	Origin of company	Date, duration and location of interview	Total number of interviews	Position within the company
Case 1: Company A		Sweden		3	
	1.1		2023-10-16, 33:12 min, Microsoft Teams	1	Senior Project Manager Financial Crime Prevention
	1.2		2023-10-30, 40:22, Microsoft Teams	1	Chief Technology Officer
	1.3		2023-11-08, min, 43:34, Microsoft Teams	1	Head of AML in Financial Crime Prevention

Case & Company	Interview ID	Origin of company	Date, duration and location of interview	Total number of interviews	Position within the company
Case 2: Company B		Sweden		3	
	2.1		2023-10-18, 43:56 min, Microsoft Teams	1	Head of Security
	2.2		2023-11-03, 54:09, Microsoft Teams	1	Cybersecurity Consultant
	2.3		2023-11-06, 41:37 min, Microsoft Teams	1	Compliance Manager

Case & Company	Interview ID	Origin of company	Date, duration and location of interview	Total number of interviews	Position within the company
Case 3: Company C		Sweden		3	
	3.1		2023-11-02, 48:44 min, Microsoft Teams	1	Chief Information Technology Officer
	3.2		2023-11-03, 38:40, Microsoft Teams	1	Coordinator

Figure 1: Overview of Primary Data

3.2.3 Sampling Approach

In preparation for the interviews, a participant selection process was considered to pinpoint participants. The objective of the selection process was to choose interviewees who could provide meaningful insights into the research question. Given the extensiveness of all accessible data, the data volume can be narrowed down through sampling methods where a representative subset is chosen from a large population (Easterby-Smith et al., 2015). The method used for the interviews in this research is non-probability sampling. Research can use two distinct sampling methods: Probability sampling and non-probability sampling (Easterby-Smith et al., 2015). Non-probability sampling suggests that the selection of units from the population is not randomised and thereby has a higher probability of being included in the sample (Bryman & Bryman, 2013). Given the nature of our research and the objective of the participant selection process, it becomes critical to interview carefully selected people in managerial positions with cybersecurity insights. By screening participants to select interviewees that meet the criteria for the research, a non-probability sampling approach was implemented (Easterby-Smith et al., 2015).

The first criterion considered when selecting the sample was that the interviewee chosen should be in a managerial role, enabling them to exercise authority. The second criterion was the interviewee's familiarity with security policies and procedures. The interviewee's managerial role within the organisation often suggests their familiarity with the organisation's current security practices. Using familiarity with security procedures as a criterion when selecting interviewees allows deeper insights and more detailed conversations during the interviews.

As stated in this research, a non-probability sampling approach was employed, specifically utilising the snowball sampling technique. Snowball sampling was chosen because of its advantage of reaching individuals who might otherwise be inaccessible (Naderifar et al., 2017). Starting with a few initial participants, these individuals were asked to refer other potential participants they knew who met the study's criteria. Gaining an initial foothold within an organisation was crucial in connecting with participants relevant to cybersecurity. As such, our first step involved reaching out to individuals in companies with already established connections. The initial interviews and email exchanges were used to ask participants to recommend others they knew who fit the study's criteria. The authors initially leveraged their network to reach out and contact the first interviewees. The authors conducted eight interviews across three companies within the set time frame.

3.2.4 Secondary Data

The primary data findings, the semi-structured interviews, were used to address the limitations of prior research and the inconsistencies in the literature that were found during the literature review. The results of the interviews revealed a variety of themes, some of which were confirmed by additional kinds of data, particularly secondary data. Secondary data provides the ability to investigate the correlation between variables and themes within a sample, which previously has yet to be thoroughly studied, which may lead to novel findings that can contribute to existing research (Dunn et al., 2015). The secondary data used in this research were organisational documents and internal emails. In addition, secondary data was also gathered through internet-based search engines.

3.2.5 Data Analysis

The Gioia method was implemented to approach the data in a structured manner (Gioia et al., 2012). The Gioia method is specifically suggested for qualitative analysis and abductive research. Consequently, this method aligns well with the analytical requirements of the study. The method offers a systematic approach to examining the collected data through several steps, aiding the authors in the data analysis. To prepare the primary data for the Gioia analysis method, individual notes were taken to capture key details, all while the interviews were recorded and transcribed using the automated Microsoft Teams transcription function. The notes were particularly beneficial when the transcripts were revisited and compared to the notes taken. If the transcripts were missing data, the notes could be used to correct significant mistakes impacting the findings, ensuring a more comprehensive and accurate representation of the data. The authors individually reviewed the transcribed questions and answers, along with accompanying notes, to achieve a thorough understanding of the interviews. Subsequently, each interview was collectively reviewed to pinpoint relevant and essential data. As the data was being selected, it was necessary to communicate and crosscheck each other’s work to avoid researcher bias.

As stated, the Gioia data analysis method was utilised for the coding process. Coding refers to forming groups, themes, and patterns out of data. Codes then emerge from the data to describe the groups using either one or several words, or short phrases (Miles et al., 2014). The Gioia method starts with pinpointing initial first-order codes, moves on to more comprehensive second-order themes, and finally results in defining aggregated dimensions. This systematic approach helps in highlighting common patterns and themes, as pointed out by Gioia et al. (2012).

To begin the coding process, it was decided that the authors would individually code the data to ensure that no relevant data was overlooked. Segments relevant to the objectives of the study were labelled with single or several words or short phrases to help find links when collectively reviewing the data. The individual labels were combined to identify recurring patterns and define the 1st order codes (16 codes). In the second phase of the Gioia method, the authors formed the 2nd-order themes (8 themes) by linking and grouping the 1st-order codes. The 2nd-order themes were awareness, continuous improvement, responsibility, involvement, implementation, human factor, reality training programs, and mandatory training. Lastly, the 2nd-order themes brought together 4 3rd-order aggregated dimensions: engagement, presence, relationship, and competence.

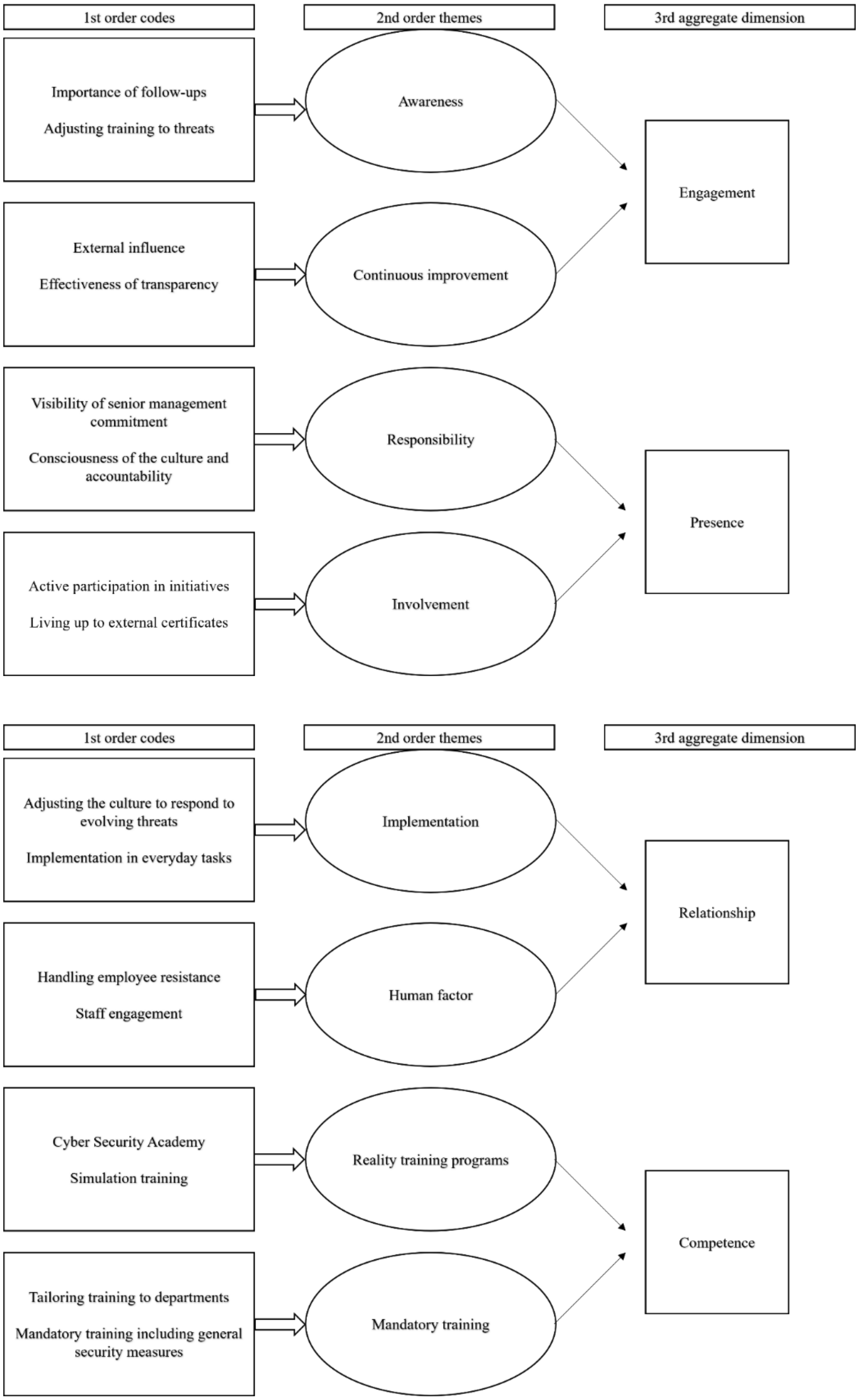

1st order codes
2nd order themes
3rd aggregate dimension
Importance of follow-ups
Adjusting training to threats
Awareness
External influence
Effectiveness of transparency
Continuous improvement
Engagement
Visibility of senior management commitment
Consciousness of the culture and accountability
Responsibility
Active participation in initiatives
Living up to external certificates
Involvement
Presence
1st order codes
2nd order themes
3rd aggregate dimension
Adjusting the culture to respond to evolving threats
Implementation in everyday tasks
Implementation
Handling employee resistance
Staff engagement
Human factor
Relationship
Cyber Security Academy
Simulation training
Reality training programs
Tailoring training to departments
Mandatory training including general security measures
Mandatory training
Competence

Figure 2: Structure of Data Analysis

3.3 Trustworthiness

Trustworthiness is the level of confidence in a study’s data and method that guarantees research quality (Pilot & Beck, 2014). Four criteria were developed by Lincoln and Guba (1985) to establish research trustworthiness and quality, namely, credibility, transferability, dependability, and confirmability.

3.3.1 Credibility

Credibility pertains to the issue of consistency and coherence between participants’ views and how the researcher represents them. If the explanation is consistent with the description and the description is credible, the research gains greater trustworthiness (Janesick, 2000). This was ensured by accurately describing each interviewee’s experience so that the interviewees could instantly identify the experience described to the authors in the interviews (Cope, 2014). This was done by emailing the interviewees with follow-up questions, clarification, and confirmation of meaning. Moreover, according to Lincoln and Guba (1985), credibility in research is the method that increases the likelihood that the conclusions will be deemed trustworthy and the ability to demonstrate the credibility of the conclusions by prolonged engagement, persistent observation, and triangulation. In this research, the authors applied data triangulation by gathering information from additional sources, such as organisational documents and internal emails, to cross-check the data and its interpretations. The authors could better comprehend senior management’s role in cybersecurity culture through interviewees as it allowed for a glimpse into the organisation’s cybersecurity culture and leadership, whilst internal documents confirmed the author's perception and subjective opinions. As a result, the combination of sources and subsequent triangulation ensured credibility.

3.3.2 Transferability

To create a trustworthy report, transferability alludes to the author’s competence to adapt the study’s findings to different situations, groups, and places, also known as generalisability (Elo et al., 2014). To enable transferability, the authors included sufficient detail about cybersecurity culture and senior management so that a reader could determine whether the actual cybersecurity environment is comparable to the one they are accustomed to and whether the conclusion on senior management’s role can legitimately be applied to their own organisational circumstances (Shenton, 2004). The data collection and analysis were disclosed in sections 4.2.1, 4.2.2 and 4.2.5, allowing transparency in these procedures. The data allows readers to conclude the transferability of senior management’s role in cybersecurity culture. However, as the authors cannot foresee readers who wish to transfer the findings, the reader's setting must resemble the researcher’s setting to an extent (Kuper et al., 2008). Notably, due to a smaller sample size with organisations in different sectors, transferring the findings may be difficult as the findings are somewhat subjective to the interviewee’s experiences. Nonetheless, the research may contain transferability for organisations in Sweden seeking to improve their cybersecurity culture or organisations wanting to increase management’s role in cybersecurity culture.

3.3.3 Dependability

According to Nowell et al. (2017), dependability demands that the research process is traceable, logical, and comprehensively documented. To achieve dependability, according to Nowell et al. (2017), the authors kept clear documentation of the data collection process by recording the semi-structured interviews, taking notes during the interview, and using an automated transcript function. The purpose of taking notes was to eliminate the probability of the automated transcript function missing essential data and to ensure an accurate representation of the interviewee's perceptions were documented. Furthermore, Saunders et al. (2019) explain that dependability refers to the consistency and replicability of a study, which ensures that the process is consistent and that the results are repeatable under similar conditions. Thus, before documenting the data collection process, the authors clearly explained a multiple case study that uses semi-structured interviews to collect raw data and presented the current research on cybersecurity culture to help make the research replicable. Additionally, throughout the research process, communicating with peers and tutors through seminars and individual tutoring helped give the authors objective viewpoints and ensured that the methodologies were consistent and potential biases were avoided.

3.3.4 Confirmability

Confirmability addresses the degree of neutrality of researchers, ensuring that interpretations and conclusions come directly from the data rather than researchers' biases (Creswell, 2013; Lincoln

& Guba, 1985). The authors made efforts to maintain neutrality in the relationships with interviewees by recognising the influence of their roles, including avoiding leading questions during interviews and only asking follow-up questions for clarity to avoid misunderstandings. As cybersecurity is a complex issue, the authors had to refrain from asking too many clarification questions, firstly to not lead the interview in the wrong direction, but also to distance themselves from their own understanding and knowledge of cybersecurity and remain neutral. Therefore, the authors wanted to represent the data collected through the interviewees to resemble reality, which was done by reminding interviewees that their personal perspectives and experiences were the primary focus (Polit & Beck, 2010). Moreover, the authors continuously communicated with peers and tutors to incorporate an objective perspective into the research process to reduce personal bias.

3.4 Ethical Considerations

In qualitative research that involves individuals as study subjects, relational, contextual, and evolving ethical considerations are constant and require ethical standards to be adhered to (Pietilä et al., 2019). The in-depth nature of a research process in a qualitative study offers ethical concerns and considerations (Afrin, 2018) to protect both the researchers and the participants. The authors committed to following a series of ethical guidelines by Afrin (2018) to guarantee voluntary participation and consent, the right to withdraw at any time, permission for transcription and video recording and full anonymity, both for the individual and the organisation.

Consideration for ethical behaviour was of top priority for the authors and was catered to from the very beginning. When the authors contacted the potential interviewee participants, the intention and meaning of the initial contact was clearly stated to ensure the participant’s right to consent. The emails were accompanied by a consent form, the thesis background, purpose, and research question, and all the interview questions. Most importantly, the authors clearly expressed the right to anonymity for both the organisation and the participant. The purpose of this was to reduce potential harm to participants or their organisations due to sensitive material whilst also ensuring their comfort. Furthermore, during the interviews, the authors introduced themselves and engaged in small talk to strengthen the relationship further and reassure the author’s intent for the interview. Lastly, the authors proceeded to explicitly state the usage of the data, how the data was managed and the procedure of deleting recordings, transcription, and all other documents after the data analysis, as well as sending out emails of when the data had been deleted.

4. EMPIRICAL FINDINGS

This chapter delves into the findings of the interviews. This section allows for an in-depth presentation of the development of themes from both primary and secondary sources. The themes are divided into subcategories and contain a thorough description with examples of quotes from the findings. These themes are deemed to be the most appropriate for the theoretical contribution.

The empirical findings of this thesis were derived from eight semi-structured interviews, which highlighted the role of senior management's influence on cybersecurity culture and awareness training. Four aggregate dimensions were identified using primary data: presence, engagement, relationship, and competence.

4.1 Engagement

A successful cybersecurity culture can be recognised by its members' shared understanding of security concerns, dedication to training and awareness in the face of evolving threats. Our interviewees reasoned that keeping employees informed and involved motivates staff to respond to threats more efficiently. Schaufeli et al. (2002) describe engagement as "a positive, fulfilling, work-related state of mind that is characterised by vigour, dedication and absorption." Indeed, organisations that establish engagement through cooperation from senior management and individual employee engagement can improve performance and outperform rivals (Megha, 2015). It is, therefore, evidently in the organisation's interest to comprehend the factors that influence engagement.

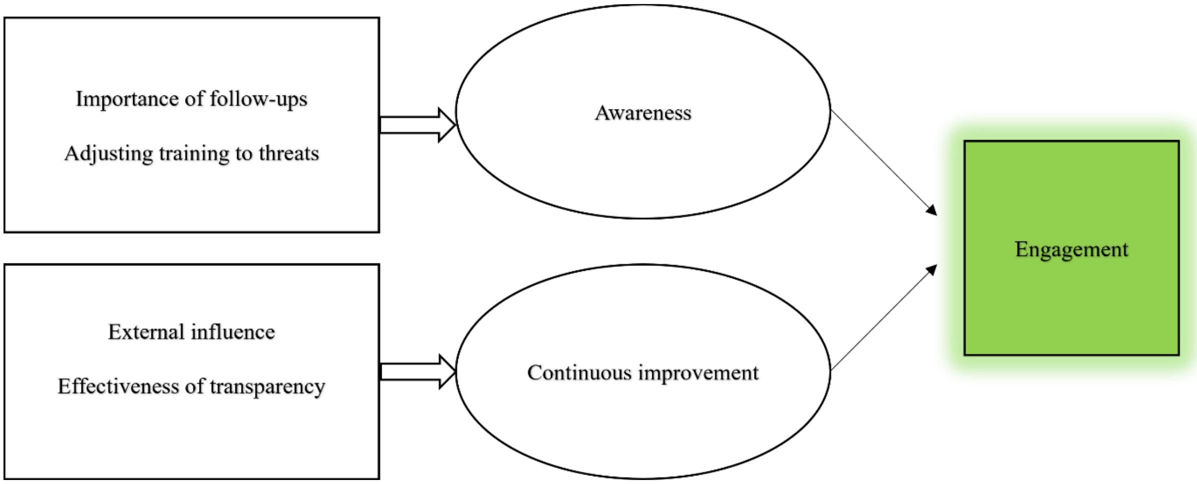


Figure 3: First Aggregate dimension

4.1.1 Awareness

Cybersecurity is an ever-evolving threat, which requires a cybersecurity culture to be flexible, adaptable, and focused on creating aware employees. Our interviewees argued that an employee and organisation that is well informed is more adaptable and has a deeper awareness of cybersecurity procedures. However, majority of the interviews, clarified that the culture is far from perfect.

> *If I were to describe the status of it, I would say it's somewhat inconsistent. – ID 2.1*

Company C agreed that the culture requires more work and time.

> *"I don't really know how to position it, but it can be improved. There is a basic awareness of cybersecurity, but then the translation of this into one's profession and the recognition of its relevance in one's professional practice is where we can work on things." – ID 3.1*

Thus, it was clear that there was awareness to the fact that the culture is evolving, and that these organisations continuously strive to strengthen it. As we noted from two interviewees:

> *"Definitely, it has evolved because it's constantly happening, it's happening all the time, and we are reminded all the time, and as a company, we make sure to remind our employees continuously." – ID 1.1*

> *"I would say that it's getting better and better. I would say that awareness is increasing. We have a lot of campaigns around it. For example, we have Cybersecurity Month in October. We distribute quite a bit of material, so I think that it's improving and strengthening." – ID 2.3*

Nonetheless, the interviewees did not see it as a vulnerability, but rather a chance to improve. Showcasing that the difficulties of implementing a culture and awareness of organisational flaws, leaves room for developing solutions.

> *"We try to acknowledge the inconsistencies in our culture. This helps the organisation to be aware of our flaws and what we must work on." – ID 2.1*

A common theme of the development of culture, is implementation of awareness in employees and actual awareness trainings, shown here by all three companies.

> *“It has evolved over time, and this is actually thanks to the fact that we have engaged in activities internally, as well as we have seen the impact on society as well as on our customers who have been affected by cybersecurity incidents.” – ID 3.1*

> “*This month, we have Cybersecurity Month, which we have every October, and it's initiated from our global function where we have a pretty large team dedicated solely to cybersecurity. We can also participate in different exercises. We will have an updated cybersecurity policy launching on November 1st, also initiated globally, but of course, it's our responsibility to implement it in our organisation.” – ID 2.1*

> *“As I could have shown you here today, we've decorated the entrance with mannequins this week to remind our employees that someone might be eavesdropping at the café. Even the menu in the cafeteria had components to remind us of this.” – ID 1.1*

Thus, for organisations to implement cybersecurity culture, an awareness of what is lacking is required to meet the needs and standards of cybersecurity in organisations.

The implementation of awareness in employees has also generated a safer environment, where employees know how to handle a security breach, but also, if something were to be compromised, there is a level of awareness on how to handle the situation.

> *“The culture of being vigilant and what to look out for, but at the same time, if employees have done something that could compromise security, then they know exactly where to go to report it and that really increases awareness of how to report and what steps to take.” – ID 2.3*

Additionally, Company C further reinforces the argument that employees are well-informed about accessing help and managing security breaches, as in their intranet, they offer links and guidelines on how to respond, what to report, and whom to contact in the event of a potential breach (Documents, internal company material, Company C, 2023).

Furthermore, the interviewees argue that an aware employee is a secure employee, and without awareness, or a strong cybersecurity culture, engagement would be much lower.

> *“In the way that you, what should I say, are active in, for example, reporting suspicious emails instead of just deleting them, but also by signing up for our webinar sessions and reading and commenting on intranet articles and newsletters. I believe that if we didn't*

> *have a strong cybersecurity culture, we would have much lower engagement and response activities from our employees." – ID 3.1*

Similarly, Company A reasoned that encouraging employees to create a more aware mindset through guest lecturers or experts helps in the aiding a security mindset.

> *"One becomes very aware when attending these lectures and listening to these presentations. You become very conscious of the risks, workplace security, and how much actually happens and the works of the actual culture of cybersecurity. It's easy to think that, well, this only affects others. This only affects other companies. It doesn't affect us, but yes, it does." – ID 2.3*

Additionally, the societal landscape has influenced employees to become more aware as cybersecurity threats are continuous and are prevalent in everyday life and organisations use these real-life situations to engage employees and to implement trainings.

> "*I would say that the new world we live in, the attention for cybersecurity, is created in society. It's the one, I would say, that absolutely influences the desire to participate, not only because we create new material or say that we have to do the training, but it's actually more, I believe, external influence. You read about it, you see it in the news, and you are personally affected when you can't go to the store or such. That's what really creates engagement, and that's what we need to work on translating, that if this happens to us, it would be in this way. We use this to secure higher engagement in trainings and a stronger culture." – ID 2.1*

4.1.2 Continuous Improvement

The authors found that engagement in cybersecurity was significant for interviewees and that the organisations aimed at creating an aware employee. All organisations heavily indicated that just as cybersecurity is evolving, so is their culture. When the interviewees were asked if the culture has changed throughout the years, all organisations signified that is has. Company B stated:

> *"Each individual's perspective on it differs. What's happening out there and how we are, it changes all the time. So, for me, this is an extremely dynamic landscape where age, culture, and technology are constantly evolving. Our youngest guy, who is 23, has certain*

> *views, while our eldest employee, who is 61, has different views based on his experience and background." – ID 2.2*

When asked why the culture has changed, ID 1.2 explained that a reason can be the social threats of today.

> "*It is primarily the volatility in the negative geopolitical developments, and it is reflected in the cybercriminal landscape. We are therefore continuously guarding the environment to see what we are up against and finding strategies to handle it."*- ID 1.2

Company B agrees that their cybersecurity culture has changed, not only due to new sophisticated threats, but also the increase of digitalisation.

> *"When COVID-19 arrived, there was a significant increase in digitalisation, which acted as a catalyst. It had been part of the plans for some time, but it suddenly became a necessity. It had already begun before, but in the context of COVID-19, the real significant shift took place." – ID 2.1*

Additionally, Company B also stated that digitalization is complex and requires cultures to change to keep up with the shifts in society.

> *"It's a complex domain we live in today with digitalisation. Things change every day and to manage these shifts, culture and protocol need to change with it." – ID 2.2*

Although the culture has changed to cater to the new development of cybersecurity threats, there is always room for improvement, which is clearly an overlapping theme from the three companies:

> *"We will always have to improve our strategies, knowledge and understanding of cybersecurity, as it changes every day. We must improve our protocols to match the newest threat." – ID 2.1*

> *"We constantly need to improve behaviour, improve acceptance, and improve a willingness to contribute to the work." – ID 1.1*

> *"It becomes more and more important; it's not a matter of if but when we will be attacked — everyone will be eventually. So, it's crucial to be vigilant, and it's very important that everyone has this culture of being aware." – ID 3.2*

The continuous improvement was a persistent theme as well as the understanding of cybersecurity culture adaptation, and how this impacts employees.

> *“Changing any culture of any organisation is difficult, and especially in the case of security. It's complex and difficult to understand for the normal employee. It makes it hard to integrate the culture of cybersecurity.” – ID 2.1*

The interviewees also signify a change of cybersecurity culture throughout the years, where organisations face challenges to improve culture and awareness throughout the entire company, not just for those who are trained IT experts. As company A states:

> *“We have had to change our entire approach, aiming to make it understandable for all employees. Our goal is to describe and convey security in a way that everyone can understand, regardless of their previous knowledge on the subject, that's where our culture awareness team is focused.” – ID 1.3*

Two interviewees stated that improvements were found specifically in trainings.

> *“The training has improved; it's more precise. They provide better examples of various events that are highly relevant to us. It's an ongoing adaptation to how the threats appear.” – ID 1.2*

> *“Our trainings are more tailored to real life scenarios and showcase situations that our staff actually can be in” – ID 2.1*

Moreover, Company B reasons that being transparent when discussing the threats of cybersecurity, generates transparency for employees, who will thus feel more informed and aware of the threat at hand, and grant possibility to be aware of the situation.

> *“What stands out is that we are transparent and share some insights that we gain from external sources, for example, the threat landscape, what we discover from threat simulations, and, of course, real incidents to our employees, to increase engagement.” – ID 2.1*

Which heightens the acceptance and understanding of improved and modified protocols.

> *“There are continuous new updates on the computer and the phone, at the pace at which things are evolving. So, when I started, I had one login. Now, I have four logins before I*

> *can access my applications and work. So, it's ongoing. New improvements to help us do things right." – ID 1.1*

Additionally, Company C's security protocol reinforces the usage of multi-factor authentication and describes the usage and need for such procedures (Internal company documents, Company C, 2023).

However, Company B also mentions, that the new modified procedures, should not be too complicated.

> *"It's important that we implement security into daily operations, but it must also be simple. We can't complicate everything too much, because then people won't follow what they're supposed to. Everything must be simple. For example, when it comes to different tools and various passwords to access different things. Suddenly everything is a bit complicated. We need to create things that are simple." – ID 2.3*

Hence, engaging employees through the conversation of new and emerging cybersecurity threats and new security measures or protocols showcases engagement from their senior management, which generates more aware employees and a safer organisation.

4.2 Presence

From the primary data, it was apparent that the significance of senior management's presence on cybersecurity success, was to be held to high regard. Presence refers to senior management's active participation in their organisation to showcase their involvement and the responsibility they take, to achieve cybersecurity culture. Senior management's ability to portray the relevance and importance of cybersecurity was proven to be crucial for the organisation to collectively apply a safe and secure behaviour in daily tasks.

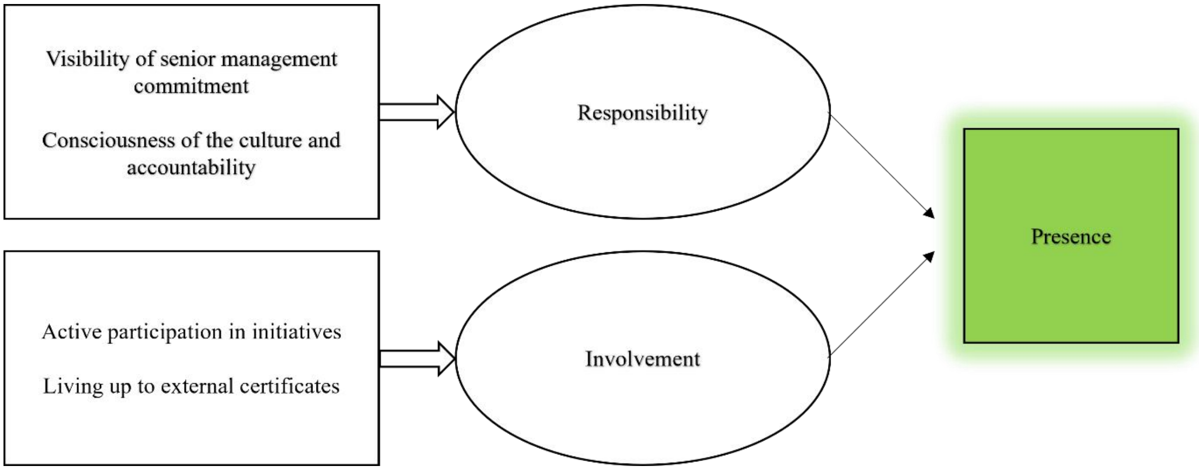

Visibility of senior management commitment
Consciousness of the culture and accountability
Active participation in initiatives
Living up to external certificates
Responsibility
Involvement
Presence

Figure 4: Second Aggregate dimension

4.2.1 Responsibility

Our interviewees emphasized that the responsibility of senior management in the implementation and organisation of cybersecurity protocol was fundamental for the organisation to set goals and aims to stive for. Company A and B stated:

> *"Ultimately management is accountable for a great deal of what we as a Company A must be able to live up to and what we must be able to demonstrate in, for example, compliance with regulations where supervisory authorities measure and follow up, but also what our customers expect us to do be able to demonstrate on the basis that we have a very well-functioning defence." – ID 1.2*

> *"Senior management is responsible for both the implementation and advocacy, as they are the one who must advocate for the need for security in organisations." – ID 1.1*

Additionally, Company C highlights the weight of senior management's responsibility in directing and showcasing cybersecurity and how this influence affects the organisation.

> *"After all, they have the responsibility to both ensure that strategies are developed and that the organisation is provided with funds to implement, but also to follow up on how the implementation goes, if it has an effect. So, management affects in that sense and if there has actually been an impact in our organisation." – ID 3.1*

The findings showed that senior management has a defining influence on the whole organisation as they instil a cyber conscious culture in the organisation by prioritising cybersecurity. Indeed, Company C states that *"The management more or less sets the framework for how important this is to the business." – ID 3.1* and *"Senior management has a significant impact within the organisation, fostering a culture of cyber consciousness by giving priority to cybersecurity." -ID 2*.3. Thus, management's perception of cybersecurity impacts every employee as it highlights the importance of cybersecurity in day-to-day operations. Senior management is responsible for understanding the risks and weaknesses of the organisation, and to clarify those to their employees. Interviewee 1.2 stated:

> *"I am not allowed to go into any details, but in general you can say that we are responsible as management by being able to explain why it is so important. Sometimes we talk a little bit about how this is a prerequisite for actually being able to exist." – ID 1.2*

4.2.2 Involvement

For the implementation of cybersecurity, our interviewees reasoned that senior management's involvement communicated the importance of cybersecurity. It is apparent that employees are more inclined to embrace cybersecurity as a central component of their daily operations, when they are aware of how important it is to the organisation's success and survival, as noted by company B and C.

> *"Yes, absolutely, it's a crucial component. If this is something communicated from senior management, that this is an area of importance for the organisation, it will definitely impact how it is embraced throughout the company." – ID 3.1*

> *"It would be quite challenging to advocate for this without obtaining buy-in from top management, considering the significant amount of work time it regularly requires from many individuals." – ID 2.1*

Company A states that to ensure employees understanding of management's position on the relevance of cybersecurity, it is crucial to involve and interact with the whole organisation.

> *"That I am available and that I help the teams out in the organisation by being either an expert to exemplify or as support, for example, in planning future activities. And also, to describe why we prioritize this, what it means, and what it is that we reinforce." – ID 1.2*

The interviewees also stated that senior managements involvement in participating in awareness trainings was volatile for a collective understanding.

> *"They have to participate just like all other employees, so they are not excluded. Their participation helps signify the importance of completing trainings." – ID 3.1*

Furthermore, Company B agreed, and stated that senior management's involvement in trainings also helped generate feedback.

> *"They also attend the trainings so they can leave their feedback. Was it good or wasn't it good?" – ID 2.1*

When asked what organisations can further do to strengthen the cybersecurity culture, Company A stated that:

> *"Sometimes we utilise our senior management. Perhaps they are featured in an article, an event, or a panel discussion, which they are very willing to participate in, almost too often. This way, it becomes even more apparent and clear that this is not just an isolated security group's dream but something that we actually involve the entire organisation in." – ID 1.2*

Indeed, the usage of senior management to involve the organisation is an influential tactic. Interviewee ID 3.1 agrees:

> *"Yes, what we can always do is to bring this up on the agenda and talk about its relevance. Why this is something important for the company and what could happen if we don't focus on it, if we don't allocate enough resources to think about cybersecurity in our operations? I believe it's important for both people in my role, but even more crucial for those representing higher management, to really bring it up and discuss it because it makes it much more relevant, than when it comes from me, it's expected. This is my job. I work full-time on this, but when it comes from people recognized from different management groups working on business development, and they also say that this is important, it carries more weight." – ID 3.1*

Thus, the presence of leaders, their responsibility as well as their involvement, signifies to the organisation the urgency of understanding and developing a cybersecurity culture, positively influencing a cybersecurity culture.

4.3 Relationship

The “Relationship” dimension in the pictured coding figure explores the data surrounding senior management’s engagement with staff to shape the cybersecurity culture and control human-related risk. The aggregated dimension *Relationship* is divided into 2nd order themes named: *Implementation* and *Human Factor*.

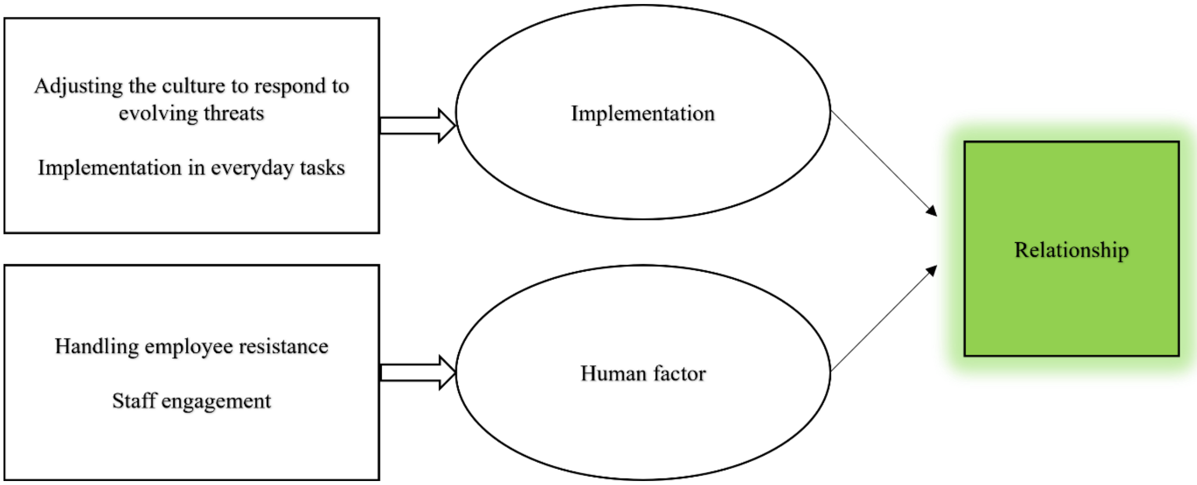

Adjusting the culture to respond to evolving threats
Implementation in everyday tasks
Implementation
Handling employee resistance
Staff engagement
Human factor
Relationship

Figure 5: Third Aggregate dimension

4.3.1 Human Factor

This theme emerged as an observation from the collected data explaining the handling of staff resistance and how to engage the staff in enforcing a cybersecurity culture.

The Case Companies agree that it is critical to make the complex topic of cybersecurity comprehensible to engage the staff in its enforcement. An interviewee mentions the importance of developing an understandable cybersecurity education to help engage the staff.

> *“We have had to change the whole approach and make it comprehensible for all employees, not just for those who are knowledgeable in security, but describe and explain it in a way that it becomes understandable for everyone.” – ID 1.2*

When asking the interviewees about how they would handle scepticism among employees regarding cybersecurity one of the interviewees pointed out that it is crucial to make the conversation not about technological solutions, but on a valuable common goal – the customer.

> *"It's very simple; one should always start from what is most important to us, and that is our customers, ensuring that nothing ever happens to the customer's data or assets. That's where you begin. You can never start with a product or a technical thing; if you do, it fails." – ID 1.1*

A pattern that was detected across interviews was that it was extremely rare for employees to not want to participate. This indicates that all parts of the organisation accept and recognise the importance of the company's training initiatives. One of the interviewees credits the high participation rate to the hard work that goes into making the training attractive and understandable.

> *"Yes, there is a tremendous interest in participating. But again, it's the reward for all the work that my colleagues do to make this attractive, understandable, and relevant." – ID 1.2*

While resistance from employees is rare in the interviewed cases it was mentioned in one of the interviews that variations in interest levels could be a more common challenge. The interviewee then went on to explain the need for training despite one's differences in knowledge.

> *"Resistance is extremely rare. There are individual cases among all our employees, however, there might be a lack of interest. Yes, that can exist. It somewhat depends on whether one feels that this is relevant or if one thinks that this is something they already have under control. But the fact is, even those who are experts in and have Ph.Ds. in phishing fall for phishing emails, so it's a bit like this. Yes, I hear what you're saying, but the reality is that everyone needs to take this type of awareness training." – ID 3.1*

Another participant mentions their observation that one might be uninterested in participating because of the repetitiveness of the training. They then continue to explain their strategic approach to handle the disinterest by designing the training to keep the engagement high.

> *"It's more that one finds it somewhat uninteresting to undergo the same type of training regularly. I took this last year and the year before that, and now that I'm beginning to understand it, must I really do this again? But employees do it. We have packaged these trainings so cleverly and efficiently, taking into account the feedback we receive, trying to improve and slightly change the content each year." – ID 2.1*

4.3.2 Implementation

It is stated in the interviews that the cybersecurity initiatives are successful when it is observable that the members of the organisation can seamlessly implement a cyber-conscious behaviour when performing their usual tasks.

> *"The aim is that our employees go about their usual tasks with a heightened sense of security, applying what they've learned almost subconsciously. If they can do that, we're building a secure organisation as we owe that to our customers."* – ID 2.1

An interesting viewpoint is introduced in one of the interviews as it is explained that while implementing security measures in ordinary tasks is vital, there must be a balance between the increased cybersecurity measures and work efficiency.

> *"There are sometimes three logins to access a workstation, and there's also face recognition. It's like we're adding layer upon layer, on top of the security level. With the applications we use daily, it becomes quite noticeable. Then there's the question: Do we really need to enter the password for the fifth time every day just to be able to work? No, it's not very efficient. Instead, we're working from the other direction, using things like facial recognition, etc., to make it quite simple."* – ID 1.3

This observation highlights that security measures are important, but they cannot become an obstacle to productivity. Extending this remark, another interviewee offers a more holistic approach to cybersecurity, highlighting its integration into all operations of the organisation.

> *"It's not just about how I log in; it's about the security around everything we do, such as having our badges visible when we enter the building, having robust shell protection, and using tools that require two-factor authentication. The whole concept is also linked to the wellness and training aspects, making it quite a holistic approach to cybersecurity. It's not just about protecting your password or avoiding writing it down on a note under the computer. It's a fairly holistic view, and it applies when we develop systems, etc. We always conduct penetration tests; our cybersecurity culture is quite strict."* – ID 2.3

The "Relationship" dimension concludes that senior management must actively engage with all parts of the organisation to address human vulnerabilities and control compliance with implemented training initiatives. They do so by continuous follow-ups and keeping the educational content interesting.

4.4 Competence

Competence emerges as a dimension derived from the 2nd order themes: *Reality training programs* and *Mandatory training*. The dimension summarizes the collected primary data that outlined how organisations go about preparing themselves with up-to-date knowledge and abilities to combat cyber threats.

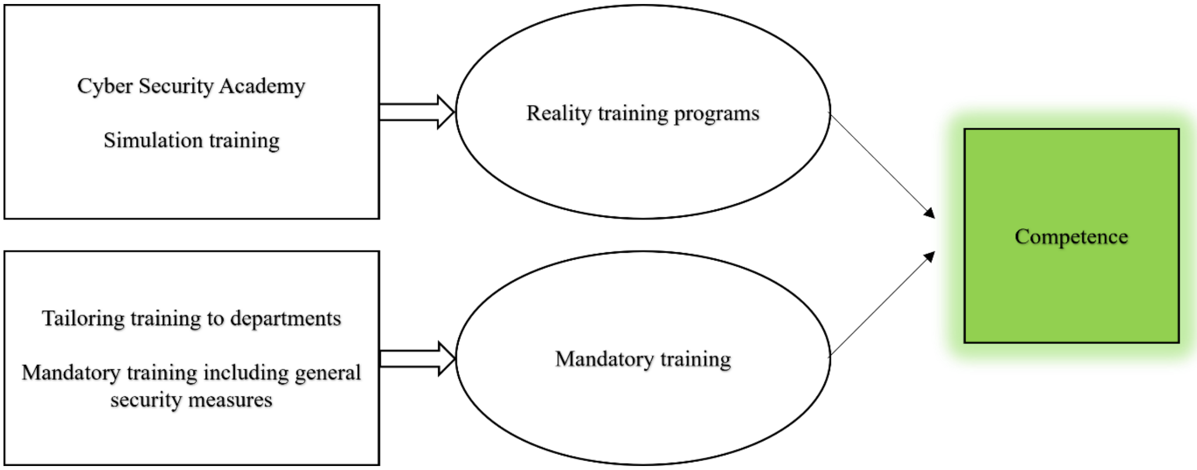

Cyber Security Academy
Simulation training
Reality training programs
Tailoring training to departments
Mandatory training including general security measures
Mandatory training
Competence

Figure 6: Fourth Aggregate dimension

4.4.1 Reality Training Programs

A highlighted security measure mentioned by several of the interviewees was reality training programs emphasizing the importance of realistic situations preparing the members of the organisation to react to actual threats.

> *"It has simply become so evident with this type of threat against us that, just like pilots, we must train in simulators." – ID 1.2*

According to the intranet of Company A (Documents, internal company material, Company A, 2023):

> *"One of the most common ways cyber criminals get access to your data is through your employees. Adversaries send fraudulent emails impersonating someone in your organisation and will either ask for personal details or for access to certain files. Links often seem legitimate to an untrained eye and it's easy to fall into the trap."*

The information presented on the intranet underscores the importance of reality training programs to train the eye of employees.

The interviewees specified phishing simulations to be effective and easy to implement extensively across the entire organisation. The effective impact of the phishing training was captured in numbers showcasing the reduction of click-through rates in simulated phishing emails.

> *"They receive regular emails that are fake phishing emails, and we have tried to teach them a behaviour to report all emails that seem suspicious, whether they believe it is a drill email or a real one. This has greatly increased our reporting capability and the attentiveness of the staff. We can see today that before we started this, we had a so-called fail rate of about 10% on all the simulated emails we sent, which were clicked on. Today, our fail rate has gone down to under 1%. So, it has had a quite significant effect that we can measure." – ID 3.1*

When the interviewee was asked about the most effective strategies for improving cybersecurity awareness, the phishing simulations were yet again mentioned.

> *"I must say that I think the phishing stimulation with the questions is very good because it comes when you are sitting and working without you being prepared." – ID 1.3*

> *"I believe a lot in the effect of the phishing simulation with the micro training because there we can really see, based on who is active in the tool how good they are at avoiding clicking on incorrect links or documents in emails. So there, I think that one gets a very clear follow-up that it has an effect. It's easy to show management that this investment has an impact." – ID 2.3*

An innovative approach to instilling knowledge and competence throughout the organisation is an in-house training initiative referred to as a "Cyber Security Academy". The initiative was unique to one of the interviews.

> *"Internally, we have created a Cybersecurity Academy where we take out a fairly large number of colleagues who participate for a semester. We have developed it with various modules. These modules are to frame the discussion more easily, now we are talking about this area, security in the cloud for example." – ID 1.2*

4.4.2 Mandatory Training

The data revealed that ‘Mandatory Training’ is a consistent theme across the conducted interviews. It was explained as initiatives and training activities that must be undertaken by all employees, either when entering the organisation or as a repetitive annual procedure.

> *“There is a training for all existing employees that is conducted annually, it is a package with various modules of which security is one.” – ID 2.3*

When encouraged to specify who exactly is encouraged to participate in the mandatory training, one interviewee playfully responded:

> *“It includes all employees, full-time, part-time- holiday workers, and all consultants who, in practice, work as if they were employed so that they get access to our system and data. But not someone who services the coffee machines, for example.” – ID 3.1*

The statement made by the interviewee illustrates the organisation’s commitment to making sure that every individual, in every position, has a fundamental understanding of the organisational cybersecurity procedures.

The interviewees emphasized the importance of repetitive training to ensure that safety precautions become second nature to employees. The risks of not engaging in regular training practices were encapsulated by one of the interviewees, who explained:

> *“Personally, I believe this is a matter of regularly doing these things. If we pause and then start again, we will, unfortunately, regress in terms of awareness, because one becomes accustomed to these regular reminders and the reinforcement they provide.” – ID 1.1*

The “Competence” dimension highlights the importance of reality training programs and mandatory training, to prepare all parts of the organisation with the ability to respond to potential cyber threats.

5. ANALYSIS

This chapter analyses the empirical findings on how senior management influences cybersecurity culture and awareness training, as well as the introduction to a new framework. The purpose of this chapter is to link the themes found in primary and secondary data to the literature and framework.

Eight interviews were conducted to explore senior management's role in cybersecurity culture, particularly its influence on awareness training. Through our fieldwork, the authors gained an understanding of cybersecurity culture in organisations and its interconnectedness to senior management. The analysis offers insight through the constructed themes of how the elements of senior management influence cybersecurity culture, as well as a new framework derived from the M-TISM model (Rajan et al., 2021) and developed through the findings, the CyberGuard Framework.

5.1 Developing the Senior Management CyberGuard Framework

While theories on cybersecurity culture exist and provide an overview of components necessary to create a resilient culture, such as those presented by Bada et al. (2021) and Mwim et al. (2023), many fail to analyse the influence senior management has on implementing a cybersecurity culture, specifically the required steps for senior management to take to manage employees in cybersecurity. Based on the empirical findings and insights from the M-TISM Cybersecurity Management Model, a framework has been constructed. The framework regards the influence of senior management, the interrelationship between senior management, awareness training, cybersecurity culture and the individual components in senior management that guide the management of humans in cybersecurity culture. The framework consists of four main factors, as described in chapter four, with added concepts derived from the cybersecurity management M-TISM model. The CyberGuard Framework is revised with new elements generated throughout the thesis process with factors from the M-TISM model, to illustrate senior management's influence on cybersecurity culture more accurately.

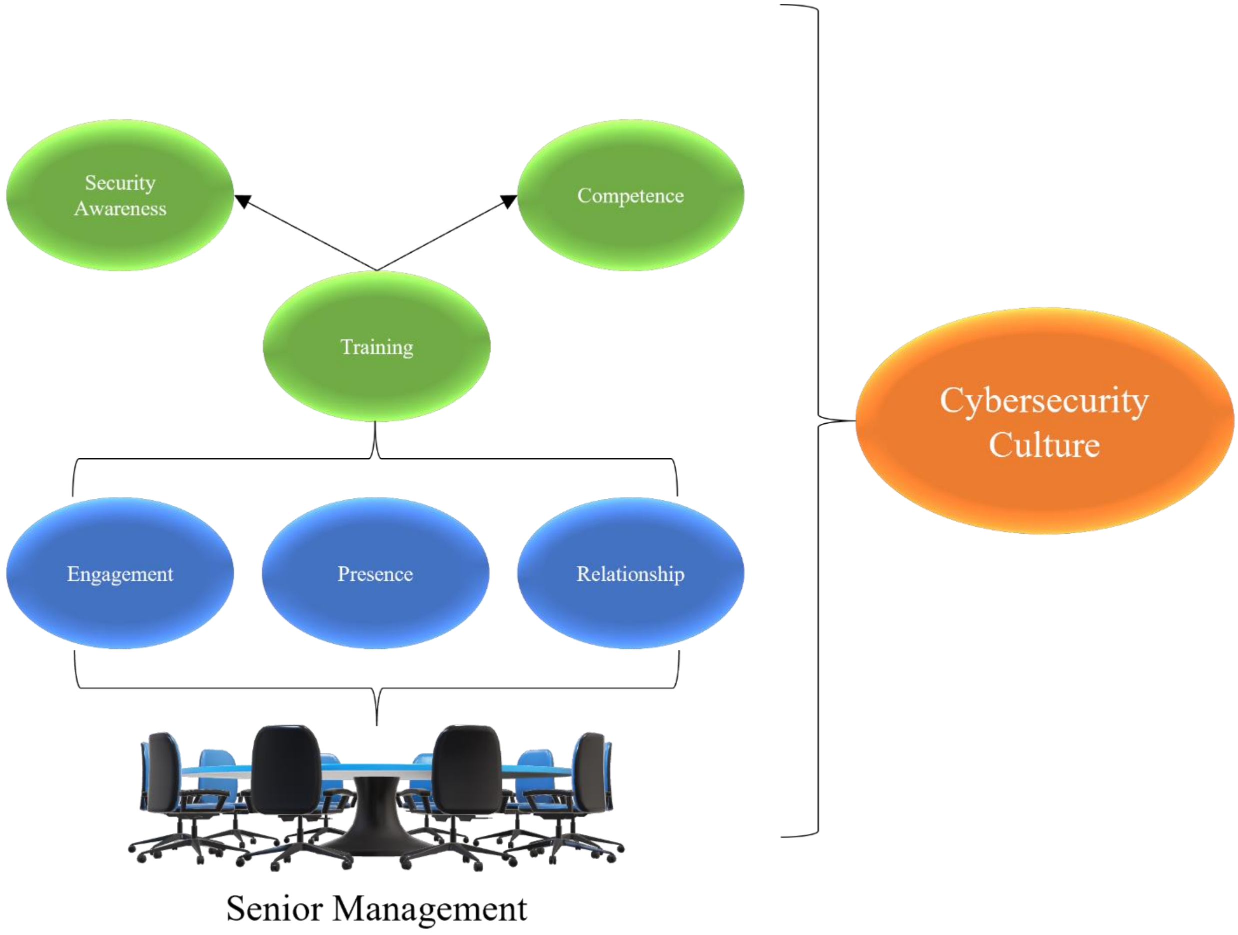


Figure 7: The Senior Management CyberGuard Framework

The findings revealed four aggregate dimensions: engagement, presence, relationship, and competence. These four dimensions have been accompanied by senior management, governance, training, security awareness and cybersecurity culture from the M-TISM Model. According to Mwim & Mtsweni (2022), literature needs to establish standards and strategies to develop an appropriate cybersecurity culture that effectively mitigates human error and understands the management of employees in cybersecurity. The framework showcases the process of senior management to reach a resilient cybersecurity culture. The framework starts with senior management and three significant elements: engagement, presence, and relationship which are crucial to reach a satisfying level of training, thereby creating aware and competent employees. From training, security awareness and competence are derived to uphold, sustain, and maintain a cybersecurity culture. The framework insists that all elements are equally important and needed to create a culture. This framework is meant to guide and direct senior management into understanding their influence and using it to influence the cybersecurity culture within their organisations positively.

5.2 Strengthening Cybersecurity Culture through Engagement

Using primary and secondary data, our empirical findings reveal that senior management is a significant factor in cybersecurity culture. The first part of the framework introduces senior management as one of the main factors of cybersecurity culture and, more specifically, their governance and engagement. The findings signified the importance of engagement in senior management and employees and the factors necessary to achieve it. Indeed, our findings reveal that for senior management to influence employees and sustain an overall organisational engagement, senior management must engage in creating awareness and continuously improving their strategies, which is crucial for the success of implementing a cybersecurity culture.

Rajan et al. (2015) M-TISM model elaborates on the importance of senior management and the influence their governance has on establishing cybersecurity. Notably, the threat of cyberattacks must be considered and addressed by management, as senior management is essential in forming and sustaining a cybersecurity culture (Rajan et al., 2021). However, the model neglects to acknowledge what factors senior management must sustain to properly influence and engage their employees, which could hinder the implementation of cybersecurity culture and employee engagement. The M-TISM model states that senior management should be involved in the monitoring and decision-making of cybersecurity, offer cybersecurity awareness training, and support the organisation (Rajan et al., 2021). Still, it lacks in clarifying how management should proceed to do just that. Therefore, the CyberGuard framework take this into account and created three factors to ensure governance and engagement from senior management and employees.

The increasing concern about cyber-attacks and the level of sophistication has impacted the organisation's ability to manage employee security behaviour (Cleveland & Cleveland, 2018), leading to difficulty in establishing awareness and strategies. Indeed, employee security behaviour is inefficient due to an overall organisational absence of cybersecurity readiness. Thus, the pillars, awareness and continuous improvement were generated to raise employee security behaviour to its full potential. Through the interviews, it became clear that there was an underlying awareness of cybersecurity in employees, which stemmed from internal activities such as security training, cybersecurity months, lectures from guest speakers, and external factors such as the volatility in geopolitics. However, the application of awareness in the workplace and the understanding of its significance for daily tasks and professional practice is where most organisations lack. This was noticeable throughout the interviews as all organisations showcased difficulties in integrating awareness in its full capacity, in daily tasks. Indeed, existing literature by Huang & Pearlson (2019) states that without strong leadership, awareness training and education are ineffective. Thus, it shows that organisations need to implement stronger management to further create awareness and engagement. Similarly, Triplett (2022) argues that the responsibility of awareness falls under senior management hence, the lack of secure behaviour and engagement can be attributed to the lack of engagement from senior management. On the contrary, Company A stated that their overall cybersecurity awareness amongst employees was high, but they still found issues with keeping their employees engaged. This aligns with Furnell (2008) stating that despite a positive relationship between awareness and employee behaviour, there is a gap between awareness and corresponding practises and behaviours.

Additionally, our study showed how external factors require organisations to regularly improve their training and strategies to match the risks and threats affecting the organisations. Nonetheless, these strategies must be simple and easy to follow and cannot be too complex for the everyday employee. As stated in our findings, a high level of security, entailing multiple passwords, phones, and tools to access applications, creates frustration. Thus, the need for constant improvement of strategies is required not only for cyber threats but also for daily operational use for employees. The M-TISM model neglects the aspect of simplicity in its research on training and awareness, and therefore, also the aspect that continuous improvement requires organisations to engage employees to the extent where cybersecurity practises are understood and cared for whilst not limiting and complicating daily tasks. Therefore, the need for a framework that continuously puts pressure on its organisation to signify the relevance of constant awareness is required to be able to continuously improve strategies.

5.3 The Importance of Senior Management Presence in Cybersecurity Culture

Senior management presence emerges from the findings as a significant influence on cybersecurity culture, meaning that the responsibility and involvement of senior management in cybersecurity, has a direct influence on employees. This is strengthened by Hu et al. (2012), stating that employee perception and attitude about cybersecurity policies are influenced by the actions of senior management, and that there is a clear impact on employee's behaviour regarding security compliance. Therefore, by increasing senior management presence, through responsibility and involvement, the success of cybersecurity culture can be enhanced, as employee's security behaviour is positively reinforced by senior management.

The findings reveal the need for two pillars, responsibility, and involvement, in fulfilling the criteria of presence in the CyberGuard model. Senior management must not only take responsibility for the organisations shared beliefs and assumptions of cybersecurity, but also the involvement of promoting these beliefs and assumptions to their employees (Von Solms & Von Solms, 2004). The authors argue that the responsibility of promoting the importance and priority of cybersecurity, for the whole organisation to maintain the same belief, falls under senior management. Indeed, to create any resilient culture, employees must understand and have sufficient knowledge about the assumptions that their organisations preach (Von Solms & Von Solms, 2004). This became evident in the findings as the interviewees all stated that, firstly, management is responsible for setting the level of priority cybersecurity has in an organisation (Triplett, 2022). The priorities in the three companies were clearly different, as due to their various sectors, the level of priority required was a contrasting factor. Indeed, organisational requirements for a bank will be widely different from a fashion retailer or insurance company (Krauss, 2014), showcasing that their senior management presence will also vary. As the M-TISM model does not take this into consideration, it complicates the comparability between organisations. Nonetheless, the authors argue that all three companies have succeeded in displaying the priority to their employees, as the findings reveal similar understanding and knowledge about cybersecurity. The findings reveal that Company A had a clear position and assumption about cybersecurity, and the authors found that their overall cybersecurity culture was strong, as the organisation, through interviews, provided a united front and shared a similar perception of the priority of cybersecurity (Von Solms & Von Solms, 2004a). However, due to Company A being in the banking sector, it begs the question, is Company A’s senior management more responsible and involved, or is the requirement to meet certain security standards just higher, making it difficult to compare to other sectors? Indeed, one can argue that Company B and C provide a strong front and that its senior management has prioritised cybersecurity without being required to follow the same regulations and security requirements as Company A (Krauss, 2014). There is no distinction made between clarifying the different requirements for contrasting organisations in the M-TISM Model nor how senior management should take this into consideration. Thus, there is a lack of knowledge on how to apply the M-TISM model to organisations' senior management and being able to compare them, making it difficult to understand the reasoning behind why certain companies have a more efficient cybersecurity culture and, hence, how to then use their strategies in another organisation. This certainly calls for the investigation of senior management's influence on cybersecurity culture. Understanding the influence will allow for the measurement of different organisations and comparisons between sectors, generating the possibility of creating a standard level of cybersecurity and comparing and analysing the culture (Gcaza & Von Solms, 2017). The authors argue that creating an organisational level of cybersecurity culture will simplify the understanding of senior management, generate better procedures and comparisons, as well as the possibility for other organisations to improve their strategies. Indeed, without measurements or standard levels of cybersecurity, organisations may face difficulties implementing strategic strategies and protocols catered to their own organisational needs (Van't Wout, 2018) and being able to measure and compare their cybersecurity levels (Gcaza & Von Solms, 2017) as well as understanding how senior management can better take responsibility and involve themself into cybersecurity culture.

Secondly, Von Solms & Von Solms (2004a) stated that setting the tone and sharing the same cybersecurity beliefs in an organisation, is not efficient enough, senior management must also promote these security beliefs through more practical settings. This involvement requires senior management to display the organisations assumptions, and how they intend to meet and fulfil these assumptions. Indeed, our findings show that all companies had some form of cybersecurity awareness team that dictates the training and educations, which are then thoroughly promoted by senior management. Thus, security awareness trainings, follow ups and other practical cybersecurity initiatives are crucial to maintain the organisational assumptions, increase the knowledge of cybersecurity, and the standard level of security awareness (Von Solms & Von Solms, 2004a). Indeed, organisations with employees who attain a better understanding of security awareness, tend to have better cybersecurity protocols and knowledge, creating a stronger cybersecurity culture (Cleveland & Cleveland, 2018). The findings reveal that all three companies provide similar trainings and initiatives, with similar content, length, and quantity. However, that authors argue that due to a stronger cybersecurity culture at Company A, because of a more present and engaged senior management, which was decided upon through the interviews, assumptions and trainings are more efficient and employees have a higher level of security awareness. Hence, it is prevalent, that the presence of senior management is crucial to the establishment of a cybersecurity culture, practiced by the entire organisation.

The findings show that the participation of senior management, both by creating assumptions and practically promoting them, in cybersecurity initiatives is essential in demonstrating that cybersecurity is applicable to all levels of the organisation. The presence of senior management is presented in the CyberGuard framework as the initiatives of senior management, through responsibility and involvement, and are essential to set the tone for the entire organisation's approach to cybersecurity. This aligns with the M-TISM model, which states that senior management aids in the implementation of cybersecurity management by offering the support and resources necessary (Rajan et al., 2021).

5.4 The Significance of Competence in Security Awareness

In analysing the findings and the literature on cybersecurity, a recurring theme is the concept of security awareness. The literature states that security awareness is essential to an organisation's cybersecurity culture (Zwilling et al., 2020). The concept of competence in this study, as revealed by the findings, refers to senior management preparing members of the organisation with the necessary tools to effectively protect the organisation against cyber threats, including security awareness training. Senior management plays a vital role in cybersecurity by providing resources, support, and training programs while monitoring and participating in decision-making processes (Berry & Berry, 2018).

The findings exhibited that all cases studied implemented yearly mandatory training for staff members to educate themselves with the proper knowledge required to combat evolving cyber threats. As previously expressed in cybersecurity literature, if members of the organisation are not properly informed of cybersecurity issues, it is unlikely that technological systems safeguard the organisation alone (Dahbur et al., 2017; Wiley et al., 2020; Rajan et al., 2021). However, the authors argue that it is important to be mindful that senior management's responsibility in this context extends beyond just providing these mandatory training programs. As a result, a critical aspect for senior management in providing training to enhance overall organisational awareness is the tracking and monitoring of participation and progress. Hence, it is not enough to provide the training, senior management must have the competence to verify compliance and awareness within their employees, instead of simply assuming it. The findings highlighted that simulation training, particularly phishing simulations, effectively monitors and evaluates progress in cybersecurity awareness. Notably, simulation training was implemented by all three case companies as they are arguably effective in providing practical experiences that allow the staff members to experience cyber threat scenarios without real consequences. By monitoring the progress of the phishing simulations, the interviewees could showcase a significant reduction in their fail rate. Consequently, the authors argue that this kind of data can be a persuasive argument proving the value of cybersecurity training to management and stakeholders as it leads to enhanced cybersecurity readiness and, therefore, improved organisational performance (Hasan et al., 2021). Thus, it is reasonable to consider continued or increased allocation of resources toward such training programs. Drawing from Knowles et al. (2015) and the M-TISM model (Rajan et al., 2021), allocation and resource governance fall under the responsibility of senior management. Thus, competence is required to understand cybersecurity and the needs and training employees require.

Additionally, the findings demonstrated that the tracking and monitoring of compliance is critical to avoid a false sense of security within the organisation. In alignment with the research of Von Solms and Von Solms (2004a), it is essential to provide the tools necessary to measure and enforce compliance with security policies, as there is no use in establishing comprehensive organisational objectives without the ability to monitor their adherence. Therefore, the authors argue that monitoring validates that the implemented training is effective and prevents a false sense of security. As the authors argue, without the proper tools necessary to measure and enforce compliance, senior management might overestimate the cybersecurity defence of the organisation, as security initiatives are only effective if implemented by the members of the organisation. Thus, monitoring becomes essential to ensure that the training initiatives translate into real-world cybersecurity practices.

5.5 The Relevance of Relationships in Cybersecurity Culture

It emerged from the findings that relationships are a crucial factor that influences the establishment of a resilient cybersecurity culture. The dimension “Relationship”, also included as a critical factor in the CyberGuard Framework, refers to the importance of senior management actively engaging in dialogue with the members of the organisation to align their personal beliefs and foster an environment where open communication and feedback is valuable to be able to integrate cybersecurity into the organisational culture strategically.

The findings repeatedly outlined the importance of making the cybersecurity training initiatives understandable and relatable. This approach to implementing a successful cybersecurity culture with effective training initiatives aligns with previous literature and the M-TISM model that suggests that senior management is essential in shaping effective cybersecurity strategies (Rajan et al., 2021; Iovan & Iovan, 2016). The findings indicate that for cybersecurity initiatives to be truly comprehensible, organisations must avoid a traditional "one size fits all" approach to successfully engage the staff in the process of enhancing awareness. Shifting away from the "one size fits all" approach acknowledges the different levels of knowledge and technical background throughout the organisation. This confirms the research of Rajan et al. (2015), where the M-TISM model explains that senior management is responsible for making strategic decisions that are understandable to all organisational levels. The authors argue that the process of making the security initiatives comprehensible extends beyond the design of the educational material and training. It includes senior managers frequently interacting with all parts of the organisation and using the established relationships to effectively communicate the objectives of the educational material to align senior management beliefs with the rest of the organisation (Von Solms & Von Solms, 2004). As expressed by the Chief Technology Officer at Case Company A, an essential part of the managerial role is remaining accessible for feedback, offering support by providing practical examples, and participating in discussions. Hence, the authors argue that the accessibility and involvement of senior managers foster a relationship with the staff members where open communication helps make the security initiatives comprehensible. The authors recognise the role of relationships in shaping a cybersecurity culture. Therefore, the dimension is incorporated into the CyberGuard framework. Indeed, Company A demonstrated strong relationships between its senior managers and the rest of the organisation, capturing the attention of the authors. The strong relationships were not only due to regulatory compliance and consumer expectations. Instead, they were influenced by senior management intentionally making cybersecurity a priority and communicating its importance to employees through active engagement.

Our findings exhibited that cybersecurity implementation is when security procedures become second nature to employees performing their daily tasks and routines. The findings are extended by one of the case studies, recommending a holistic approach and that cybersecurity should not be an isolated function but an integrated aspect of all activities in the organisation. The holistic approach mentioned falls under the responsibilities of senior management (Iovan & Iovan, 2016; Knowles et al., 2015) and aligns with the previous findings of Von Solms and Von Solms (2004a) that argue that for security policies to be effective, they must be integrated into the broader organisational culture. The authors argue, in support of the findings and previous literature, that a holistic approach demonstrates the importance of senior management’s role in implementing and deeply integrating cybersecurity into the organisational culture to foster a mindset among the members of the organisation where cybersecurity is understood and practised collectively with a shared goal to secure the organisation. However, to thoroughly integrate security procedures, they must be perceived as manageable by the ones integrating them (Von Solms & Von Solms, 2004). The findings indicate that there must be a balance between work efficiency and safety procedures. For instance, requiring employees to use five different passwords to access a workplace database most likely gets in the way of them remaining efficient in completing their daily tasks. As a result, it is crucial for senior management to understand what is practical for different departments and individuals handling different levels of sensitive data. This is achieved by promoting a relationship where open communication is encouraged, and feedback is considered.

Nonetheless, the authors claim that organisations handling sensitive data, like Companies A and C, typically have longer and more tedious security processes to protect their assets. Consequently, it becomes more necessary to communicate the significance of these security measures, underlining the need for relationships allowing open and clear communication. As explained by D'Arcy et al. (2014), employees can often find additional security measures quite annoying and inconvenient. Thus, the authors argue that it is necessary for senior management to become acquainted with different parts of the organisation, to understand which cybersecurity methods are suitable for each department.

Furthermore, it was observed from the findings that all case companies found it extremely rare for staff to show resistance to participating in the company’s cybersecurity initiatives. The pattern indicates that the organisations value and accept the importance of cybersecurity. Case Company A explained that the high levels of participation and engagement were accredited to all the work that makes security initiatives attractive, understandable, and relevant. In alignment with the M-TISM model and the CyberGuard framework, the emerging data, as explained by Case Company A, can largely be attributed to the involvement of senior management and their ability to effectively communicate the critical role of cybersecurity to all the organisation’s members. Indeed, the high level of participation serves as a testament to senior management’s ability to align the organisation’s policies with employees’ personal beliefs and assumptions. Aligning beliefs is crucial in successfully implementing organisational policies (Von Solms and Von Solms, 2004). Furthermore, the literature emphasises frequent training to avoid the fading of knowledge gained from the training sessions (Uchendu et al., 2021). However, the findings reveal that an area of concern is complacent employees who become disengaged as they are demanded to participate in repetitive training where they feel as if they already understand the knowledge being taught. Thus, the authors argue that senior management can avoid the issue of complacent employees by directly engaging with staff and maintaining a communicative relationship. This allows for employee feedback and can help brainstorm better ways to engage employees to feel heard and seen in their relationships with their senior managers, who must show genuine interest in their employees’ experiences.

The four aggregate dimensions: engagement, presence, competence, and relationship are examined in this analysis to explore senior management’s influence on cybersecurity culture. The analysis highlights the significance of senior management in fostering a cybersecurity culture as it establishes an organisational perspective on cybersecurity, a theoretical framework, CyberGuard, and discusses the influence of senior management. Indeed, to manage and mitigate the ever-evolving landscape and threat of cyber-attacks, a cybersecurity culture is needed.

6. CONCLUSION

This chapter presents the conclusions of the key findings regarding the research question. The authors further discuss the theoretical contributions, practical implications, limitations and future research.

6.1 Answering the Research Question

This thesis aimed to explore how senior management influences cybersecurity culture and awareness training. Based on our findings, senior management, built on engagement, presence, relationship and competence, is crucial in cybersecurity culture. Senior management influence can result in a more secure and appropriate cybersecurity culture (Triplett, 2022). Indeed, senior management influences the practical implications in the organisation, such as trainings, as well as the assumptions and beliefs of its employees. Senior management influences the engagement, involvement and responsibility of protecting and safeguarding the organisations assets, and how this is reciprocated to the whole organisation. Furthermore, senior management addresses and manages the priority of cybersecurity in the organisation. Senior managements passiveness in promoting cybersecurity protocol, can influence employees to disregard cybersecurity initiatives (Puhakainen & Siponen, 2010). Hence, employee behaviour and attitude are greatly impacted by senior management engagement and presence, showcasing a positive correlation between senior management influence and employee behaviour and beliefs (Puhakainen & Siponen, 2010). Moreover, senior management may significantly enhance an organisation's cybersecurity strategy if correct measures and policies are implemented to recognise human behaviour and processes. Thus, it is required of senior management to comprehend cybersecurity and the trainings needed, to provide employees with knowledge and competence in preforming a safe and secure cybersecurity behaviour, which is connected to their own engagement and presence. As a result, this can create a positive development of awareness and reinforce employee's behaviour regarding cybersecurity (Triplett, 2022). Conclusively, the usage of senior management and their influence, can efficiently engage their employees, create awareness, provide support and competence, and ultimately lead to a successful cybersecurity culture.

6.2 Theoretical Contributions

This thesis and the empirical findings contribute to the literature on senior management's influence on cybersecurity. Firstly, the thesis theoretically contributes to the senior management cybersecurity culture literature, as it further builds upon research conducted by Gcaza & Von Solms (2017), Hasan et al. (2021), Knowles et al. (2015), Mwim et al. (2023), Rajan et al. (2021), Triplett (2022), Van't Wout (2018), Von Solms & Von Solms (2004) and the factors of engagement, presence, relationship, and competence. The thesis contributes novel perspectives to the existing literature by offering a theoretical framework, the CyberGuard Framework. The framework encapsulates the findings and shows the significance of senior management's engagement, presence, relationship, and competence in implementing cybersecurity culture in organisations. The framework allows for the research question to be answered and contribute to the body of knowledge on cybersecurity culture by highlighting the significance of senior management's influence on cybersecurity culture.

Secondly, the thesis contributes to cybersecurity literature by focusing on integrating human-inclusive methods into the cybersecurity culture in combination with support from senior management. Indeed, the findings reveal this is best done by strengthening senior management through engagement and presence. This study extends the research of Bada et al. (2021) and Mwim et al. (2023), emphasising the importance of human-inclusive strategies to mitigate cyber threats. The thesis provides insight into these factors and their interrelationships whilst also showcasing the pivotal role of senior management in handling those challenges. As a result, the thesis provides how senior management can understand their influence by prioritising relationships with their employees and improving their competence, and as such, how to use their influence to enhance and leverage cybersecurity culture.

Thirdly, the study further adds valuable insight into cybersecurity culture by showcasing how implementing human-inclusive methods can increase organisations' cybersecurity readiness. The thesis increases understanding of human factors that affect the implementation of a cybersecurity culture and, through that, emphasises the vital role that employees play in fostering a culture of cybersecurity. Indeed, previous research has focused on technological solutions (Holstein et al., 2015). As a result, this thesis adds to the existing literature on human-inclusive methods and how to manage employee engagement towards cybersecurity initiatives.

6.3 Practical Implications

This thesis contributes to practice by highlighting the critical role of senior management in developing and reinforcing an organisation's cybersecurity culture. The findings show the importance of senior management’s engagement and presence in leadership to demonstrate dedication to the organisational cybersecurity objectives. Indeed, by actively participating and demonstrating their commitment to cybersecurity objectives, senior managers align their interests with employees and create relationships that prioritise trust and open communication, which can help foster a cybersecurity culture. By consistently showcasing engagement and presence for cybersecurity, senior managers are setting a standard for the organisation’s members, helping reduce employee negligence and making employees more receptive to organisational cybersecurity procedures. As a result, individual employee engagement, improvement and overall organisational engagement towards cybersecurity initiatives, such as security awareness training, may increase. Furthermore, a strong cybersecurity culture is supported by comprehensive security training initiatives. Hence, it is essential that the training communicates the importance of cybersecurity to all parts of the organisation and provides the necessary tools for employees to function in their daily operations without creating cybersecurity vulnerabilities. These implications can increase employee engagement and help foster human-inclusive methods that can increase the organisation’s cybersecurity readiness and as a result, their cybersecurity culture.

6.4 Limitations and Future Research

This thesis has limitations that should be highlighted and pointed out for complete transparency. The first limitation of the study is concerned with the chosen multiple case study research design. The specific conditions of each individual case can make it difficult to replicate the findings, presenting challenges when making comparisons and contrasts across the different cases. The second limitation is regarding the limited number of interviews conducted in this thesis, a larger sample size could have contributed to a better understanding of senior management influence, and increased credibility by showcasing that the findings are not limited to a certain group’s experience. Finally, the third limitation is concerned with the geographical context of the thesis. Focusing on Swedish organisations limits the transferability of the findings to different geographical locations. The geographical context, in terms of organizational and cultural differences, might lead to different cybersecurity approaches. Hence, the applicability of the outcomes of this thesis is limited. For future studies, it would be interesting to extend the research beyond the geographical setting of Sweden, as we believe different cultural contexts will influence different results. Future research could include comparative studies using more case companies and different cultural contexts to examine differences across countries. As the nature of cybersecurity is complex and ever evolving, it demands ongoing research and attention. Hence, following up this study with similar research to track the evolution of the subject is critical. Additionally, it would be of interest to conduct long-term studies to investigate the long-lasting effect of senior management practices and the cultural change over time.

References

2021 Cyber Security Report. (2021). Check Point Software. https://www.checkpoint.com/pages/cyber-security-report-2021/

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *JACCP: Journal of the American College of Clinical Pharmacy*, *4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441

Alharahsheh, H. H., & Pius, A. (2019). A Review of key paradigms: positivism VS interpretivism. *Global Academic Journal of Humantities and Social Sciences*. https://www.researchgate.net/publication/338244145_A_Review_of_key_paradigms_positivism_VS_interpretivism

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Al-Shehri, Y., & Clarke, N. (2012). Information Security Awareness and Culture. *Centre for Information Security and Network Research*,. http://bjournal.co.uk/paper/BJASS_6_1/BJASS_06_01_07.pdf

Ander, T. (2022). *Informationssäkerhetskultur*. Pug Förlag.

Ani, U., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/jsit-02-2018-0028

Arifin, S. R. M. (2018). Ethical considerations in qualitative study. *International Journal of Care Scholars*, *1*(2), 30–33. https://doi.org/10.31436/ijcs.v1i2.82

Auffret, J., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., Stein, F., Sokol, L., Allor, P., & Warweg, P. (2017). Cybersecurity Leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, *17*(01), 1740001. https://doi.org/10.1142/s0219265917400011

Bada, M., Sasse, A., & Nurse, J. R. C. (2021). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society, 2015*. https://www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf

Banks, N. (2016). Practise what you preach. *Computer Fraud & Security*, *2016*(4), 5–8. https://doi.org/10.1016/s1361-3723(16)30035-5

Beauchamp, T. L., & Childress, J. F. (2012). Principles of Biomedical ethics. In *The MIT Press eBooks*. https://doi.org/10.7551/mitpress/9079.003.0009

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability*, *13*(24), 13761. https://doi.org/10.3390/su132413761

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1. https://doi.org/10.1504/ijbcrm.2018.090580

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human Performance in Cybersecurity: a research agenda. *Proceedings of the Human Factors and Ergonomics Society . . . Annual Meeting*, *55*(1), 1115–1119. https://doi.org/10.1177/1071181311551233

Bryman, A., & Bryman, P. O. S. R. A. (2013). *Social research methods*.

Carpenter, P. (2019). *Transformational security awareness: What neuroscientists, storytellers, and marketers can teach us about driving secure behaviors*. https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119566380

Chapman, P. (2020). Are your IT staff ready for the pandemic-driven insider threat? *Network Security*, *2020*(4), 8–11. https://doi.org/10.1016/s1353-4858(20)30042-8

Chen, C. C., Shaw, R. S., & Yang, S. C. (2005). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning & Performance Journal*, *24*(1), 1–14.

Cleveland, S., & Cleveland, M. (2018). Toward Cybersecurity leadership framework. *CORE*. https://core.ac.uk/display/301374951?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

Collis, J., & Hussey, R. (2013). *Business research: A Practical Guide for Undergraduate and Postgraduate Students*. Red Globe Press.

Collis, J., & Hussey, R. (2021). *Business research: A Practical Guide for Students*. Bloomsbury Publishing.

Cope, D. G. (2014). Methods and Meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, *41*(1), 89–91. https://doi.org/10.1188/14.onf.89-91

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing Among Five Approaches*. SAGE.

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of Security Awareness: A Qualitative and Quantitative study. *International Management Review*, *13*(1), 37. https://www.questia.com/library/journal/1P3-4321221661/assessment-of-security-awareness-a-qualitative-and

Da Veiga, A., Астахова, Л. В., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/mis0742-1222310210

Dunn, S. L., Arslanian-Engoren, C., DeKoekkoek, T., Jadack, R. A., & Scott, L. D. (2015). Secondary data analysis as an efficient and effective approach to nursing research. *Western Journal of Nursing Research*, *37*(10), 1295–1307. https://doi.org/10.1177/0193945915570042

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2015). *Management and business research*. SAGE.

Edmonstone, J., & Western, J. (2002). Leadership development in health care: what do we know? *Journal of Management in Medicine*, *16*(1), 34–47. https://doi.org/10.1108/02689230210428616

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities And Challenges. *Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/amj.2007.24160888

El-Bably, A. Y. (2021). *View of Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management*. https://journals.nauss.edu.sa/index.php/JISCR/article/view/1508/1024

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis. *SAGE Open*, *4*(1), 215824401452263. https://doi.org/10.1177/2158244014522633

Ertan, A. (2020, April 24). *Cyber Security Behaviour In Organisations*. Royal Holloway University of London. https://doi.org/10.48550/arXiv.2004.11768

European Commission. *Data protection in the EU*. (2023, July 4). European Commission. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#fundamental-rights

Federal Bureau of Investigation. (2022). *Internet Crime Complaint Center releases 2022 statistics*. Federal Bureau of Investigation. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

Federal Trade Commission. *Gramm-Leach-Bliley Act*. (2023, June 16). Federal Trade Commission. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *PubMed*, *9*(2), 185–195. https://pubmed.ncbi.nlm.nih.gov/26642176

Freeze, D. (2023). *Cybercrime To Cost The World 8 Trillion Annually In 2023*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, *2008*(4), 6–9. https://doi.org/10.1016/s1361-3723(08)70064-2

Gcaza, N., & Von Solms, R. (2017a). Cybersecurity Culture: an Ill-Defined Problem. In *IFIP advances in information and communication technology* (pp. 98–109). https://doi.org/10.1007/978-3-319-58553-6_9

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. L. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking qualitative rigor in inductive research. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Glaspie, H. W., & Karwowski, W. (2017). Human Factors in Information Security Culture: A Literature review. In *Advances in intelligent systems and computing* (pp. 269–280). https://doi.org/10.1007/978-3-319-60585-2_25

Grix, J. (2002). Introducing students to the generic terminology of social research. *Politics*, *22*(3), 175–186. https://doi.org/10.1111/1467-9256.00173

Harvey-Jordan, S., & Long, S. (2001). The process and the pitfalls of semi-structured interviews: The Journal of the Health Visitors' Association. Community Practitioner, 74(6), 219. http://ezproxy.library.usyd.edu.au/login?url=https://www.proquest.com/scholarly-journals/process-pitfalls-semi-structured-interviews/docview/213313284/se-2

Hasan, S., Ali, M., Kurnia, S., & Ramayah, T. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5). https://doi.org/10.1007/s43546-023-00477-6

Hassandoust, F., Subasinghage, M., & Johnston, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information & Management*, *59*(1), 103574. https://doi.org/10.1016/j.im.2021.103574

Holstein, D., Cease, T. W., & Seewald, M. G. (2015). Application and Management of Cybersecurity Measures for Protection and Control. 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 76–83. https://doi.org/10.1109/CyberC.2015.80

Hox, J., & Boeije, R. (2005). Data collection, primary versus secondary. *Encyclopedia of Social Measurement*, *1*. https://www.joophox.net/publist/ESM_DCOL05.pdf

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

Huang, K., & Pearlson, K. (2019). For what technology can't fix: building a model of organizational cybersecurity culture. *Proceedings of the . . . Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2019.769

Humaidi, N., & Balakrishnan, V. (2015). Leadership Styles and Information Security Compliance Behavior: The mediator Effect of Information Security Awareness.

International Journal of Information and Education Technology, *5*(4), 311–318. https://doi.org/10.7763/ijiet.2015.v5.522

Hurley, E., Dietrich, T., & Rundle-Thiele, S. (2021). Integrating Theory in Co-design: An Abductive approach. *Australasian Marketing Journal (Amj)*, *29*(1), 66–77. https://doi.org/10.1177/1839334921998541

IBM. (2021). *Cost of a data breach 2023 | IBM*. https://www.ibm.com/reports/data-breach

Iovan, Ş., & Iovan, A. (2016). From Cyber Threats To Cyber-Crime. *Journal of Information Systems and Operations Management*, *10*(2), 425–434. https://ideas.repec.org/a/rau/journl/v10y2016i2p425-434.html

James, H. S. (1999). Reinforcing ethical decision making through organizational structure. *Journal of Business Ethics*, *28*(1), 43–58.

Janesick, V. J. (2000). *The Dance of Qualitative Research: Metaphor, Methodology, and Meaning*. Handbook of Qualitative Research.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolpg, C. (2019). *Towards an improved understanding of human factors in cybersecurity*. IEEE Conference Publication. https://ieeexplore.ieee.org/abstract/document/8998491

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Krauss, R. (2015). *When it comes to information security, not all industries are alike*. https://www.bitdefender.com/blog/businessinsights/information-security-industry-differences/

Kuper, A., Lingard, L., & Levinson, W. (2008). Critically appraising qualitative research. *BMJ*, *337*(aug07 3), a1035. https://doi.org/10.1136/bmj.a1035

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: literature review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

Legal IT Insider. (2022). Cybersecurity Comment: Boyd Legal warn that people need to plan their digital estates before they die. *Legal IT Insider*. https://legaltechnology.com/2018/03/07/cybersecurity-comment-boyd-legal-warn-that-people-need-to-plan-their-digital-estates-before-they-die/

Lehto, M., & Limnéll, J. (2020). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139–148. https://doi.org/10.1080/19393555.2020.1813851

Li, L., He, W., Da Xu, L., Ash, I. K., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lincoln, Y. S., Guba, E. G., & Pilotta, J. J. (1985). Naturalistic inquiry. *International Journal of Intercultural Relations*, *9*(4), 438–439. https://doi.org/10.1016/0147-1767(85)90062-8

McCrohan, K. F., Engel, K. L., & Harvey, J. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

Megha, S. (2015). *A BRIEF REVIEW OF EMPLOYEE ENGAGEMENT:DEFINITION, ANTECEDENTS AND APPROACHES.* Prestige International Journal of Management & IT- Sanchayan. https://www.proquest.com/docview/2533815562?pq-origsite=gscholar&fromopenview=true

Meija, G. (2019). *Examining the impact of major security breaches on organizational performance: Should investing in cybersecurity be a requirement for companies?* Utica College.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data analysis*. SAGE.

Mwim, E. N., & Mtsweni, J. (2022). Systematic Review of Factors that Influence the Cybersecurity Culture. In *IFIP advances in information and communication technology* (pp. 147–172). https://doi.org/10.1007/978-3-031-12172-2_12

Mwim, E. N., Mtsweni, J., & Chimbo, B. (2023). Conceptual Mapping of the Cybersecurity Culture to Human Factor Domain Framework. In *Future of Information and Communication* (pp. 729–742). https://doi.org/10.1007/978-3-031-28073-3_49

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: a purposeful method of sampling in qualitative research. https://doi.org/10.5812/sdme.67670

Nicholson, S. (2019). How ethical hacking can protect organisations from a greater threat. *Computer Fraud & Security*, *2019*(5), 15–19. https://doi.org/10.1016/s1361-3723(19)30054-5

Nowell, L., Norris, J. M., White, D., & Moules, N. J. (2017). Thematic analysis. *International Journal of Qualitative Methods*, *16*(1), 160940691773384. https://doi.org/10.1177/1609406917733847

Oreg, S., Vakola, M., & Armenakis, A. A. (2011). Change recipients’ reactions to organizational change. *The Journal of Applied Behavioral Science*, *47*(4), 461–524. https://doi.org/10.1177/0021886310396550

Park, J. H., Rathore, S., Sharma, P. K., Loia, V., & Jeong, Y. S. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, *421*, 43–69. https://doi.org/10.1016/j.ins.2017.08.063

Park, M., & Chai, S. (2018). Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance. *Proceedings of the . . . Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2018.595

Patton, M. Q. (1999). *Enhancing the quality and credibility of qualitative analysis.* PubMed Central (PMC). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1089059/

Pearson, N. (2014). A larger problem: financial and reputational risks. *Computer Fraud & Security*, *2014*(4), 11–13. https://doi.org/10.1016/s1361-3723(14)70480-4

Pelgrin, W. (2014). *A Model for Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor and Leadership*. M.E Hathaway. https://doi.org/10.3233/978-1-61499-372-8-107

Pietilä, A., Nurmi, S., Halkoaho, A., & Kyngäs, H. (2019). Qualitative research: Ethical considerations. In *Springer eBooks* (pp. 49–69). https://doi.org/10.1007/978-3-030-30199-6_6

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Polit, D. F., & Beck, C. T. (2010). *Essentials of nursing research: Appraising Evidence for Nursing Practice*. Lippincott Williams & Wilkins.

Porter Sr, J. (2019). *Transformational Leadership and its approach to cybersecurity implementation - ProQuest* [PhD Dissertation]. Capitol Technology University.

Puhakainen, P., & Siponen, M. T. (2010). Improving Employees' compliance through Information Systems Security Training: An Action Research study. *Management Information Systems Quarterly*, *34*(4), 757. https://doi.org/10.2307/25750704

Rajan, R., Rana, N. P., Parameswar, N., Dhir, S., Sushil, S., & Dwivedi, Y. K. (2021). Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technological Forecasting and Social Change*, *170*, 120872. https://doi.org/10.1016/j.techfore.2021.120872

Ramluckan, T., Van Niekerk, B., & Martins, I. (2020). A change management perspective to implementing a cyber security culture. *Conference: 19th European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/EWS.20.059

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures organizations to societies. *ResearchGate*.

https://www.researchgate.net/publication/281107085_From_Information_Security_to_Cyber_Security_Cultures_Organizations_to_Societies

Saravanan, A., & Bama, S. S. (2019). A review on cyber security and the fifth generation cyberattacks. *Oriental Journal of Computer Science and Technology*, *12*(2), 50–56. https://doi.org/10.13005/ojcst12.02.04

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students*. Pearson Education.

Schultz, E. E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002

Schwandt, T. A. (2001). The SAGE Dictionary of Qualitative Inquiry. In *SAGE Publications, Inc. eBooks*. https://doi.org/10.4135/9781412986281

Serpa, S. N. F. (2016). An overview of the concept of organisational culture. *repositorio.uac.pt*. https://doi.org/10.3923/ibm.2016.51.61

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/efi-2004-22201

Silverman, D. J. (1997). Interpreting qualitative data methods for analysing talk, text and interaction. *The Modern Language Journal*, *81*(1), 136. https://doi.org/10.2307/329190

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Smith, S., Winchester, D., Bunker, D., & Jaimeson, R. (2010). Circuits of Power: A study of mandated compliance to an information Systems Security "De jure" standard in a government organization. *Management Information Systems Quarterly*, *34*(3), 463. https://doi.org/10.2307/25750687

Tavory, I., & Timmermans, S. (2014). *Abductive Analysis: theorizing qualitative research*.

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). *An investigation on cyber security threats and security models*. IEEE Conference Publication. https://ieeexplore.ieee.org/abstract/document/7371499

The National Insitute of Standards and Technology. (n.d.). https://csrc.nist.gov/. https://csrc.nist.gov/glossary/term/attack

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586. https://doi.org/10.3390/jcp2030029

Tsou, H., & Hsu, S. H. (2015). Performance effects of technology–organization–environment openness, service co-production, and digital-resource readiness: The case of the IT industry. *International Journal of Information Management*, *35*(1), 1–14. https://doi.org/10.1016/j.ijinfomgt.2014.09.001

Tyler, T. R., Callahan, P. E., & Frost, J. (2007). Armed, and dangerous: Motivating rule adherence among agents of social control. *Law & Society Review*, *41*(2), 457–492.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

UK Information Commissioner's Office. (2017). https://ico.org.uk/.

Van ’t Wout, C. (2018). Develop and maintain a cybersecurity organisational culture. *ResearchGate*.https://www.researchgate.net/publication/334052953_Develop_and_Maintain_a_Cybersecurity_Organisational_Culture

Van Zeeland, I., Van Den Broeck, W., Boonen, M., & Tintel, S. (2021). Effects of digital mediation and familiarity in online video interviews between peers. *Methodological Innovations*, *14*(3), 205979912110607. https://doi.org/10.1177/20597991211060743

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Von Solms, B., & Von Solms, R. (2004a). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

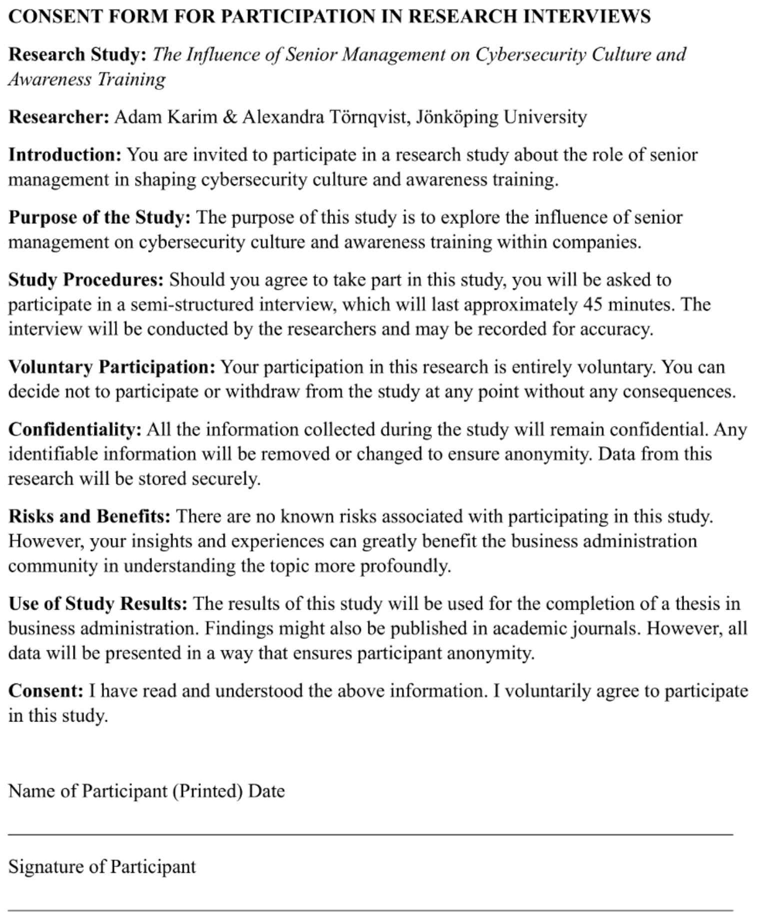
Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275–279. https://doi.org/10.1016/j.cose.2004.01.013

Wiley, A. M., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basım, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Appendix



CONSENT FORM FOR PARTICIPATION IN RESEARCH INTERVIEWS

Research Study: *The Influence of Senior Management on Cybersecurity Culture and Awareness Training*

Researcher: Adam Karim & Alexandra Törnqvist, Jönköping University

Introduction: You are invited to participate in a research study about the role of senior management in shaping cybersecurity culture and awareness training.

Purpose of the Study: The purpose of this study is to explore the influence of senior management on cybersecurity culture and awareness training within companies.

Study Procedures: Should you agree to take part in this study, you will be asked to participate in a semi-structured interview, which will last approximately 45 minutes. The interview will be conducted by the researchers and may be recorded for accuracy.

Voluntary Participation: Your participation in this research is entirely voluntary. You can decide not to participate or withdraw from the study at any point without any consequences.

Confidentiality: All the information collected during the study will remain confidential. Any identifiable information will be removed or changed to ensure anonymity. Data from this research will be stored securely.

Risks and Benefits: There are no known risks associated with participating in this study. However, your insights and experiences can greatly benefit the business administration community in understanding the topic more profoundly.

Use of Study Results: The results of this study will be used for the completion of a thesis in business administration. Findings might also be published in academic journals. However, all data will be presented in a way that ensures participant anonymity.

Consent: I have read and understood the above information. I voluntarily agree to participate in this study.

Name of Participant (Printed) Date

____

Signature of Participant

____

Appendix 1: Consent Form

Hello XX,

I hope all is well with you. I received your email from XX. Thank you so much for your willingness to participate in the thesis.

My name is Alexandra Törnqvist, and I am currently studying at Jönköping International Business School, writing my bachelor thesis in cybersecurity and leadership with my partner Adam Karim.

The thesis is an analysis of the influence organisational leadership, more specifically, senior management, has on cybersecurity and cybersecurity culture, and how this influence affects cybersecurity within the organisation. This can entail, how management influences cybersecurity campaigns, employee's attitudes and beliefs toward cybersecurity, security measures and information initiatives.

The interview will be based on 35 questions, sent to you in advanced. These questions will not inquire about specific cybersecurity measures but will ask about your organisations protocol and how the organisation handles with these issues. You and your organisation have the option to remain anonymous and if possible, we would like to record and transcribe the interview for an easier coding process. All data will be deleted upon completion of the thesis.

I will attach the questions along with our background information, containing our research question to provide a better understanding of the thesis. Please feel free to provide feedback or let me know if you are unable to answer certain questions. The interview is expected to last between 40-55 minutes.

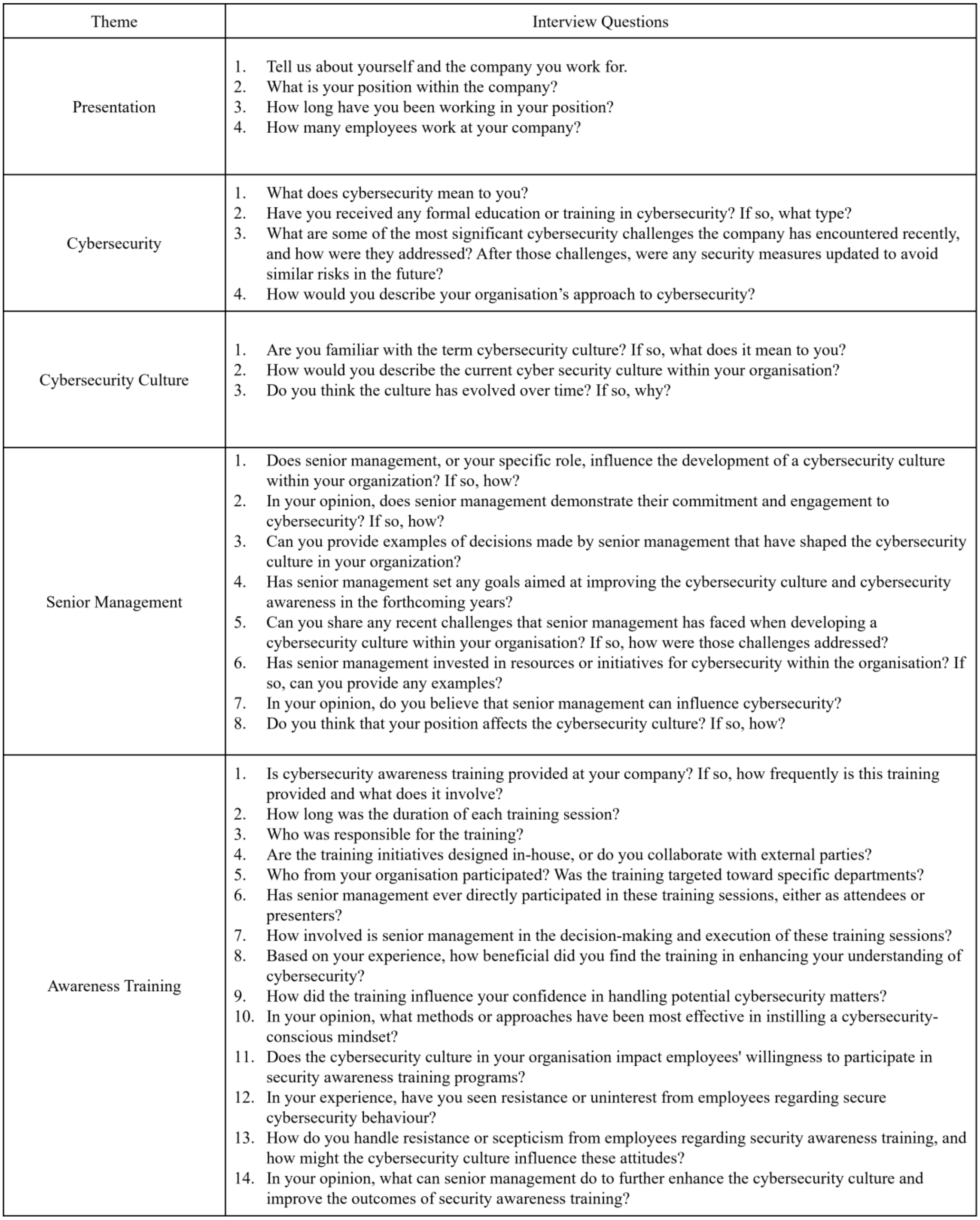
Do you have any availability for the next few weeks ahead? If so, which day and time would suit you the best? We are flexible and happy to work around your schedule.

Once again, thank you so much for your participation.

Kind Regards,

Alexandra Törnqvist and Adam Karim

Appendix 2: Contact email



Theme	Interview Questions
Presentation	1. Tell us about yourself and the company you work for. 2. What is your position within the company? 3. How long have you been working in your position? 4. How many employees work at your company?
Cybersecurity	1. What does cybersecurity mean to you? 2. Have you received any formal education or training in cybersecurity? If so, what type? 3. What are some of the most significant cybersecurity challenges the company has encountered recently, and how were they addressed? After those challenges, were any security measures updated to avoid similar risks in the future? 4. How would you describe your organisation's approach to cybersecurity?
Cybersecurity Culture	1. Are you familiar with the term cybersecurity culture? If so, what does it mean to you? 2. How would you describe the current cyber security culture within your organisation? 3. Do you think the culture has evolved over time? If so, why?
Senior Management	1. Does senior management, or your specific role, influence the development of a cybersecurity culture within your organization? If so, how? 2. In your opinion, does senior management demonstrate their commitment and engagement to cybersecurity? If so, how? 3. Can you provide examples of decisions made by senior management that have shaped the cybersecurity culture in your organization? 4. Has senior management set any goals aimed at improving the cybersecurity culture and cybersecurity awareness in the forthcoming years? 5. Can you share any recent challenges that senior management has faced when developing a cybersecurity culture within your organisation? If so, how were those challenges addressed? 6. Has senior management invested in resources or initiatives for cybersecurity within the organisation? If so, can you provide any examples? 7. In your opinion, do you believe that senior management can influence cybersecurity? 8. Do you think that your position affects the cybersecurity culture? If so, how?
Awareness Training	1. Is cybersecurity awareness training provided at your company? If so, how frequently is this training provided and what does it involve? 2. How long was the duration of each training session? 3. Who was responsible for the training? 4. Are the training initiatives designed in-house, or do you collaborate with external parties? 5. Who from your organisation participated? Was the training targeted toward specific departments? 6. Has senior management ever directly participated in these training sessions, either as attendees or presenters? 7. How involved is senior management in the decision-making and execution of these training sessions? 8. Based on your experience, how beneficial did you find the training in enhancing your understanding of cybersecurity? 9. How did the training influence your confidence in handling potential cybersecurity matters? 10. In your opinion, what methods or approaches have been most effective in instilling a cybersecurity-conscious mindset? 11. Does the cybersecurity culture in your organisation impact employees' willingness to participate in security awareness training programs? 12. In your experience, have you seen resistance or uninterest from employees regarding secure cybersecurity behaviour? 13. How do you handle resistance or scepticism from employees regarding security awareness training, and how might the cybersecurity culture influence these attitudes? 14. In your opinion, what can senior management do to further enhance the cybersecurity culture and improve the outcomes of security awareness training?

Appendix 3: Interview guide