



SCHOOL OF ECONOMICS AND MANAGEMENT

Department of Informatics

Identifying Cybersecurity Training Strategies Across Companies

A Descriptive Study

Thesis 15 HEC, course SYSK16 in Information Systems

Authors: Sebastian Bengtsson
Annie Kempf

Supervisor: Odd Steen

Examiners: Paul Pierce
Benjamin Weaver

Identifying Cybersecurity Training Strategies Across Companies: A Descriptive Study

AUTHORS: Sebastian Bengtsson & Annie Kempf

PUBLISHER: Department of Informatics, Lund School of Economics and Management,
Lund University

FORMAL EXAMINER: Osama Mansour, PhD

PRESENTED: May, 2024

DOCUMENT TYPE: Bachelor's Thesis

NUMBER OF PAGES: 70

KEYWORDS: Cybersecurity Training, Organizational Culture in Cybersecurity, Security Frameworks, Cyber Risk Management

ABSTRACT (MAX. 200 ORD):

Digital transformation is blending digital and physical realms, transforming industries and amplifying cybersecurity challenges, emphasizing the need for robust training that addresses human vulnerabilities, important since human error causes 9% of cyber-attacks. The conducted literature review highlighted a need for ongoing adaptation of cybersecurity frameworks, a shift towards blended training methods, and the importance of organizational culture in cybersecurity training. This thesis aimed to identify and describe which cybersecurity training strategies companies currently use to enhance employee cybersecurity awareness. Through descriptive qualitative research and individual interviews, this study showed that organizations adopt a multifaceted approach. Key strategies include adherence to frameworks like ISO 27001, which dictate cybersecurity practices but have limited influence on training methods. Organizations blend traditional and innovative methods such as gamification, simulations, and web-based modules, focusing on practicality and engagement with regular updates and micro-training sessions. Leadership plays an important role in fostering a proactive cybersecurity culture, emphasizing learning from mistakes and maintaining security across various working environments. Overall, companies utilize diverse training techniques and cultural leadership to equip employees against cybersecurity threats.

Table of Contents

1 Introduction.....	1
1.1 Background.....	1
1.2 Problem Area.....	1
1.3 Research Question.....	2
1.4 Purpose.....	3
1.5 Delimitations.....	3
2 Literature Review.....	4
2.1 Cybersecurity Frameworks, Standards and Models.....	4
2.1.1 Overview.....	4
2.1.2 Challenges.....	5
2.1.3 Summary and Critical Review.....	6
2.2 Cybersecurity Awareness Training Methods.....	7
2.2.1 Overview.....	7
2.2.2 Training Methods.....	7
2.2.3 Summary and Critical Review.....	8
2.3 Influence of Company Culture and Structure.....	9
2.3.1 Overview.....	9
2.3.2 Summary and Critical Review.....	10
2.4 Literature Summary.....	10
3 Research Methodology.....	11
3.1 Literature Collection and Review.....	11
3.2 Data Collection.....	15
3.2.1 Semi-structured Individual Interviews.....	15
3.2.2 Interview Guide.....	16
3.2.3 Informant Selection.....	17
3.3 Data Analysis Preparation and Process.....	19
3.3.1 Transcription.....	19
3.3.2 Data Storing.....	22
3.3.3 Member Checking.....	22
3.3.4 Data Coding.....	23
3.3.5 Data Analysis.....	26
3.4 Research Quality.....	28
3.4.1 Credibility and Confirmability.....	28
3.4.2 Transferability.....	30
3.4.3 Dependability.....	30
3.4.4 Trustworthiness.....	31

3.5 Ethical Considerations.....	31
4 Results.....	33
4.1 Theme 1: Frameworks, Standards and Models.....	33
4.1.1 Usage of Frameworks, Standards and Models to Influence Security Training Strategy.....	33
4.1.2 Keeping the training content updated.....	34
4.2 Theme 2: Training Methods.....	35
4.2.1 Method Types.....	35
4.2.2 Frequency and Length.....	37
4.2.3 In-house or External Providers.....	38
4.3 Theme 3: Organizational Culture.....	39
4.3.1 Fostering a Cybersecurity Culture.....	39
4.3.2 Challenges.....	40
4.3.3 Training Tailored to Different Employee Groups or Individuals.....	41
4.3.4 Remote Working.....	42
4.3.5 Social Media.....	43
5 Discussion.....	45
5.1 Key Findings and Interpretation of Results.....	45
5.1.1 Frameworks, Standards, and Models.....	45
5.1.2 Training Methods.....	46
5.1.3 Organizational Culture.....	49
5.1.4 Synthesis of Findings.....	50
5.2 Limitations.....	51
5.3 Suggestions for Future Research.....	52
6 Conclusion.....	53
Appendix A - Interview Guide.....	54
Appendix B - Codebook.....	56
Appendix H - AI Report.....	62
References.....	63

Figures

Figure 2.1: Elements of Cybersecurity Culture (Corradini, 2020, p. 66)	9
Figure 3.1: Example Invitation Email	19
Figure 3.2: Whisper Transcription	20
Figure 3.3: MAXQDA Transcription	20
Figure 3.4: Google Docs Transcription	21
Figure 3.5: Transcription Formatting and Labeling	22
Figure 3.6: Transcript Validation Email	23
Figure 3.7: Codebook	24
Figure 3.8: Transcription Coding Section-By-Section	26
Figure 3.9: Presentation of Results	28

Tables

Table 2.1: Types of Training Methods (Corradini, 2020, p. 127)	8
Table 3.1: Literature Search Keywords	11
Table 3.2: Search Results per Keyword and Online Database	12
Table 3.3: Literature Concept Matrix	13
Table 3.4: Main themes and Subthemes	14
Table 3.5: Source Mapping of Interview Questions	16
Table 3.6: Table of Informants	18
Table 3.7: Main Coding Categories and Code Abbreviations	25
Table 3.8: Code Count and Relative Frequency	27
Table 3.9: Top Most Frequently Coded Subthemes	28
Table 3.10: Results of Intercoder Agreement Test	29
Table B1: Codebook: Main Coding Categories	56
Table B2: Codebook: Coding Categories with Definitions and Examples	56

1 Introduction

1.1 Background

Digital transformation is merging the digital and physical worlds, changing industries and society. This shift, powered by big data, cloud computing, and the Internet of Things (IoT), is not only about new technologies but also about changing business models and how people interact. Cybersecurity is becoming increasingly important in this context (George, 2020; Möller, 2020b). The widespread use of cloud computing shows how business operations are evolving, and it also points to growing cybersecurity issues due to more digital infrastructure and more IoT devices. These changes are moving us towards a world that relies heavily on data and connectivity, where technology drives innovation and changes traditional boundaries. However, this also brings greater cyber risks, making it crucial to have strong, comprehensive cybersecurity measures to protect the digital environment and ensure its safe growth (Evans, 2022).

Cybersecurity frameworks serve as important blueprints for organizations to defend against a broad spectrum of cyber threats, integrating standardized approaches, risk quantification, and strategic policies to bolster digital protection. These frameworks guide the implementation of defense mechanisms, evolve from basic guidelines to sophisticated directives, and encompass a deep understanding of threats ranging from phishing and ransomware to advanced persistent threats and cyberespionage. While these frameworks are important in developing an organization's resilience to technological threats, they also shed light on a critical aspect often overshadowed by the focus on technical defenses: the human factor (Evans, 2022; Watters, 2023). Despite advanced cybersecurity measures, the human element remains a large vulnerability, with human error at the core of many successful cyber-attacks. As organizations strive to safeguard their operational integrity and protect sensitive assets in an increasingly interconnected digital world, the need for an integrated approach that addresses both technological and human vulnerabilities becomes paramount (Alsharif et al., 2021).

This recognition of human vulnerabilities influenced our decision to focus our thesis on cybersecurity, spurred especially by the recent ransomware attack on TietoEvry in early 2024, as reported on their website (Tietoevry.com, n.d.). This event, coupled with our personal enthusiasm for cybersecurity and experience in workplace cybersecurity training, guided our choice of topic.

1.2 Problem Area

Human elements play a pivotal role in the realm of cybersecurity, being at the heart of the majority of security risks and cyber-attacks. Specifically, 95% of successful cyber-attacks are caused by human error. This statistic highlights how important the human aspect is in cybersecurity weaknesses, showing that even with advanced technology, humans are still a key pathway for security breaches. Even comprehensive layers of security measures are often

insufficient to hinder the ingenious tactics employed by malicious actors who explore human psychology. A big majority of web attacks are due to social engineering (Alsharif et al., 2021). These insights illuminates the complex interplay between human behavior and cybersecurity risks, highlighting the need for a security-minded culture that not only relies on technological solutions but also fundamentally understands and mitigates human-centric risks.

Every organization member must grasp their role in cybersecurity. Many security strategies fail due to a lack of lasting behavior change, highlighting the need for increased skill sets in privacy and risk management. Integrating cyber risk management into the core business strategy not only protects but also promotes innovation, positioning cybersecurity as a key driver of business improvement (Evans, 2022).

The problem area for this thesis addresses the important role of human elements in cybersecurity, where human error is identified as the root cause in the large majority of successful cyber-attacks, particularly those involving social engineering. This indicates an intersection between human behavior and cybersecurity vulnerabilities, and highlights a gap in cybersecurity: the effectiveness of training strategies aimed at enhancing awareness within the workforce (Alsharif et al., 2021). The existing discrepancy in cybersecurity training approaches, especially in the context of social engineering and the underestimated risks posed by social media usage in corporate environments, underscores the need for an examination of training methodologies (Evans, 2022). Additionally, as a result of a literature review, this thesis identifies a lack of studies concerning the cybersecurity training strategies currently employed by companies.

1.3 Research Question

Addressing the issue of the growing need for enhanced cybersecurity training within workforces—to mitigate and potentially reduce enterprise cyber attacks (Evans, 2022; Möller, 2020; Watters, 2023), particularly those orchestrated through social engineering (Alsharif et al., 2021)—a need for research which will add to the body of knowledge in this subject is warranted. With respect to limited resources and time, a focused area regarding the different cybersecurity training strategies that companies are currently using, has been chosen. The reason for why we chose this particular focus area is because of personal interest, as previously mentioned. A descriptive study will be conducted, and so this thesis poses the question:

What training strategies are companies currently using to enhance cybersecurity awareness among employees?

In this thesis, the definition of ‘strategy’ is defined as a detailed plan for achieving success in a certain situation, or as a way of doing something or dealing with something (Cambridge Dictionary, 2024c). ‘Training’ is defined as the process of learning the skills you need to do a particular activity (Cambridge Dictionary, 2024d). Whereas, the particular activity referred to in this thesis is ‘awareness’, which is defined as the understanding of a situation or subject at the present time based on information and experience (Cambridge Dictionary, 2024a). Unlike in-depth training, the primary objective of enhancing ‘cybersecurity awareness’ is to cultivate an environment where individuals are not just aware but are also prepared to take the correct actions in response to security risks (Bada et al., 2019).

1.4 Purpose

The purpose of this study is to identify and describe cybersecurity training strategies that are aimed to enhance awareness among the workforce within companies. While recognizing that the research in this study will not solve a problem on its own, it will still add value by understanding how educational methods vary, potentially creating insights that can inform policymakers and industry leaders.

We seek to describe the various training strategies used across a number of companies, providing an in-depth analysis of how cybersecurity awareness is currently enhanced in those particular companies.

1.5 Delimitations

This thesis seeks to identify and describe the range of cybersecurity training strategies employed across various industries, with a specific focus on the strategies' alignment with frameworks, models and standards, training methods, and organizational culture. However, our scope will not extend to evaluating the effectiveness of these strategies. We will also not examine the success rates of the training strategies, nor will we analyze the costs or resources required for their implementation and maintenance. Additionally, our study is structured to be descriptive rather than explanatory; therefore, we will not explore the underlying reasons why companies choose specific training strategies.

Furthermore, this thesis will focus solely on the cybersecurity strategies currently employed by companies, excluding any examination of strategies used in the past or those planned for the future, resulting in a short and contemporary study. Lastly, the study is intended to gather data from a management perspective, not an employee perspective.

2 Literature Review

Upon reviewing the literature regarding Cybersecurity Awareness Training Strategies, the many identified themes have been divided into three major key areas: 1. Frameworks, Standards and Models, 2. Training Methods, and 3. Organizational Culture. The literature review has therefore been structured around these three areas.

2.1 Cybersecurity Frameworks, Standards and Models

2.1.1 Overview

The term 'framework' is defined as 'a supporting structure around which something can be built' (Cambridge Dictionary, 2024b). In this thesis, a 'cybersecurity framework' refers to the structural foundation upon which a company builds its cybersecurity strategy. These frameworks are important for organizations to effectively manage and mitigate cybersecurity risks (Ben Salamah et al., 2023) and to implement security awareness training (Corradini, 2020). Additionally, frameworks actively promote the integration of security awareness training as an essential component of organizational cybersecurity measures (McIntosh et al., 2024). Therefore, in this thesis, frameworks are deemed a relevant aspect when discussing cybersecurity training strategies.

The development and implementation of comprehensive frameworks are important for protecting systems and networks. Over time, many methods, techniques, checklists, and tools have been developed to help manage cybersecurity more systematically. Among these, the ISO/IEC 27001 and the NIST cybersecurity framework stand out for their widespread adoption and impact on IT and operational technologies (Culot et al., 2019). The ISO/IEC 27001, developed through collaboration between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), is a globally recognized standard that outlines a comprehensive list of security controls and objectives. It is designed to ensure the effective implementation of information security policies without compromising organizational productivity (El-Bably, 2021). However, despite its broad use, some experts argue that the wide-ranging nature of the ISO/IEC 27001 can make it challenging to implement, especially with the fast changes in technology and the complex aspects of cybersecurity (Culot et al., 2019).

On the other hand, the NIST Cybersecurity Framework, developed by the U.S. National Institute of Standards and Technology, provides a set of methodologies and procedures aimed at helping organizations assess and improve their ability to prevent, detect, and respond to cyberattacks (Falco & Rosenbach, 2022). It is praised for its role in enhancing the cybersecurity of e-government systems and other critical infrastructure, emphasizing a structured process that encompasses five core components: Identify, Protect, Detect, Respond, and Recover (Handri, Putro & Sensuse, 2023).

Despite their different beginnings and main focuses, both frameworks share many key elements and security requirements (Handri et al., 2023). This overlap highlights a universal approach to cybersecurity, emphasizing the importance of protective measures and the need for cyber resilience. The ISO/IEC 27001:2022 framework, in particular, focuses on resilience. The collaboration between various international groups, such as ISO, IEC, the International Society of Automation (ISA), and the European Union Agency for Network and Information Security (ENISA), shows a worldwide agreement on the need for strong cybersecurity standards. This joint effort has resulted in the development and improvement of standards that meet the specific security needs of various industries, helping to protect organizations, critical infrastructures, and consumer devices that are connected to the Internet (Djebbar & Nordström, 2023).

Aside from the widely recognized ISO/IEC and NIST frameworks, several other models focus on integration of various organizational aspects and human factors into cybersecurity management. One such model is the Strategic Alignment Model (SAM), which emphasizes the harmonious articulation of business strategy, IT strategy, organizational infrastructure, and IT processes to enable strategic IT management (Belalcázar et al., 2017). Recognizing the need to incorporate the human element into cybersecurity, the Organizational Behaviour Model suggests an approach that combines technological and human factors within organizations. Similarly, the Information Security Culture Framework (ISFC) integrates humans, technology, and organization to assess information security culture effectively. Frameworks like the Competing Security Cultures Framework (CSCF) and the Information Security Culture Assessment (ISCA) aim to identify risk elements and foster a security culture by focusing on employee behavior. The Security Culture Toolkit, another innovative approach, uses a multidimensional perspective to address an organization's security needs by connecting people, tools, and processes (Corradini, 2020).

For remote working scenarios, the CAT framework has been proposed to enhance cybersecurity awareness and training, helping organizations assess and manage their employee's cybersecurity capabilities (Hijji & Alam, 2022). Additionally, the CyberSec Labs framework offers a hands-on approach to improving cybersecurity skills through various exercises and recommendations, including those from the Open Web Application Security Project (OWASP) (Kose et al., 2021). Another innovative model, the CENSOR framework, focuses on decision support for cybersecurity investments, considering the dynamics of cyberattacks and the need for strategic mitigation measures (Tsiodra et al., 2023). There are a number of other frameworks, especially recently developed ones (Hijji & Alam, 2022), showcasing that the work to develop effective frameworks, standards and models is ongoing.

2.1.2 Challenges

Cybersecurity frameworks are important tools for organizations to manage and mitigate cybersecurity risks effectively. However, several challenges hinder their effectiveness and adaptability across different organizational contexts. One significant issue is the generic nature of many existing cybersecurity frameworks, making them difficult to adapt to specific organizational needs, especially in areas like social media risks. The Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR) was developed to address this gap, focusing on incorporating social media cybersecurity policies and adapting to employees' training needs and preferences (Ben Salamah et al., 2023).

Employee perception is another challenge, as training frameworks often do not consider individual learning styles, leading to materials that can be perceived as time-consuming, non-inviting, or intimidating. The need for frameworks that accommodate employee preferences is important to enhance engagement and effectiveness in cybersecurity training. The adaptability of frameworks to cater to all employees is questioned, given their diverse levels of knowledge and preferences. While some frameworks, like those recommended by ENISA, consider human aspects, they often focus on general awareness rather than specific areas like social media. Moreover, the one-size-fits-all approach in cybersecurity training is widely recognized as ineffective. Tailoring training to individual needs is essential for fostering effective cybersecurity awareness across an organization (Ben Salamah et al., 2023).

Assessing security maturity within organizations presents its own set of challenges. Existing methodologies struggle to cover all levels of information security culture comprehensively, indicating a need for more nuanced assessment approaches (Corradini, 2020). The interconnected nature of the modern world adds complexity to cybersecurity management. The involvement of various stakeholders, including suppliers, customers, and international partners, is necessary to address cybersecurity at a systemic level, requiring strong collaboration across sectors (Culot et al., 2019). Finally, the excess of available cybersecurity standards and frameworks complicates the process of selecting the most appropriate one for a specific system. The lack of a comprehensive comparison and overlap among these standards adds to the challenge, making it difficult for organizations to navigate the selection process effectively (Djebbar & Nordström, 2023).

2.1.3 Summary and Critical Review

The literature on cybersecurity frameworks is rich and varied, reflecting a field that is both critical and dynamic. While the ISO/IEC 27001 and NIST frameworks provide basic guidelines for cybersecurity, the constant change in digital threats means these frameworks need ongoing updates and adjustments. Organizations face challenges in applying these guidelines. They must balance broad, general standards with the specific details needed for effective cybersecurity in a fast-evolving tech world. Additionally, other proposed frameworks and models like SAM, CSCF, ISCA, CAT, and CENSOR highlight different strategies, underlining the importance of combining strategic, human, and technological factors to develop a thorough cybersecurity approach. The existing issues with cybersecurity frameworks highlight the need for adaptable, user-focused, and collaborative methods in creating and applying these frameworks to make them practical, engaging, and suitable for the unique needs of various organizations.

The articles reviewed here contribute to a nuanced picture of how these frameworks are developed, implemented, and evaluated, each bringing a unique perspective to the multifaceted challenges of cybersecurity. The literature identifies which frameworks are commonly used, but we could not locate any literature regarding how these frameworks are actually applied in structuring security training strategies within real-world companies. Further exploration and description of this relationship could enrich the field. Therefore, in this thesis, frameworks will be considered an aspect when exploring what cybersecurity training strategies companies currently employ.

2.2 Cybersecurity Awareness Training Methods

2.2.1 Overview

In this thesis, ‘awareness’ is defined as the understanding of a situation or subject at the present time based on information and experience (Cambridge Dictionary, 2024a). Awareness training in cybersecurity is designed to change behaviors, ensuring that people don't just receive information but understand and are motivated to act on it. It's the main way organizations communicate what secure behaviors are needed from everyone, from employees to managers. According to NIST Special Publication 800-16, the goal is to make people aware of security issues so they can recognize and deal with them effectively. This type of training helps ensure that everyone knows the security practices and puts them into action every day (Bada et al., 2019). Therefore, awareness training is, in this thesis, considered a relevant aspect when discussing cybersecurity training strategies.

In the world of cybersecurity, how companies train and make people aware is key to protecting an organization from online threats. With more security issues happening because of human mistakes, it is clear that strong training and awareness programs are important. Attackers are getting better at taking advantage of people's weaknesses, so it is crucial that training goes beyond just the technical components (Giriraj et al., 2022). Cybersecurity training needs to be tailored to fit different people's jobs within an organization. It's important to make sure that the training matches the specific needs of different groups of employees. This is because training works best when it considers what employees prefer in learning (Flores et al., 2023).

Choosing the right training methods should start with understanding what the organization needs. This step helps set the goals and choose the right tools and ways to teach, making sure the training really works (Corradini, 2020). When employees know how to spot and deal with security risks, it helps build a strong culture of cybersecurity in the organization (Flores et al., 2023). We also need to remember that a lot of cybersecurity problems are caused by people making mistakes. This shows how important it is for everyone in an organization to have good training to reduce these risks (Giriraj et al., 2022). So, the aim of cybersecurity training is not just about sharing knowledge; it's about building a real understanding and awareness in employees to stop security incidents, which in turn keeps the organization safe (He et al., 2019).

Moreover, the impact of social media on corporate cybersecurity is often underestimated, with less than 40% of companies having a dedicated policy. A comprehensive approach, including robust social media guidelines and internet policies, is crucial for mitigating risks like defamation and protecting intellectual property, thereby strengthening overall resilience (Evans, 2022).

2.2.2 Training Methods

In cybersecurity, diverse training methods, from traditional instructor-led sessions to innovative tech-driven strategies, are crucial for enhancing individuals' abilities to combat cyber threats. Traditional methods promote active engagement and knowledge sharing through direct interaction (Corradini, 2020). However, traditional methods lack the immersion that game-based training offers. Advances in digital technology have led to methods like the

Attacker-Centric Gamified Approach, where participants role-play as cyber attackers to understand friendly tactics deeply (Adams & Makramalla, 2015). Tabletop exercises are another form of simulation-based training where trainees collaboratively navigate hypothetical cybersecurity incidents, honing their problem-solving skills in a structured environment (Angafor et al., 2020).

Technology integration in training has made learning more engaging and realistic. For example, video-based training with interactive elements and VR or AR use offers dynamic experiences that mirror real-world cybersecurity challenges (Qawasmeh et al., 2024). E-learning platforms facilitate flexible, remote, self-paced learning, ideal for organizations with geographically dispersed teams. Informal learning via webinars and personalized paths through coaching also enhance cybersecurity skills tailored to specific roles (Corradini, 2020).

Table 2.1: Types of training methods, (adapted from Corradini, 2020, p.127)

Methods	Examples
Conventional	Instructor-led classrooms, seminars
Interactive and experiential	Case study, role-playing, gamification, simulation
Online	Web-based training, self-paced training, instructor-led training, webinars
Informal methods	Coaching, mentoring, informational learning
Blended approaches	Combination of different training methods

2.2.3 Summary and Critical Review

It seems the literature acknowledges the enduring value of traditional methods, emphasizing the effectiveness of instructor-led classroom settings in fostering direct, face-to-face interactions. However, the evolution of digital technologies has catalyzed a shift toward more innovative training methods (Corradini, 2020; Qawasmeh et al., 2024). The literature underscores the importance of a blended approach to training, which combines the strengths of various methods to cater to diverse learning preferences and organizational needs (Corradini, 2020; Flores et al., 2023).

The literature presents a compelling argument for the need to adapt cybersecurity training methods to the changing technological landscape and the diverse needs of learners. A critical insight from the review is the necessity for organizations to not only diversify their training methods but also to ensure that these methods are grounded in evidence-based practices that can be tailored to specific organizational contexts and employee roles (Adams & Makramalla, 2015; Angafor et al., 2020; Corradini, 2020; Flores et al., 2023; Giriraj et al., 2022; He et al., 2019; Qawasmeh et al., 2024). While there seems to be plenty of literature describing and comparing the different cybersecurity methods that exist, there seems to be a lack of literature looking into what methods are actually being used within companies.

2.3 Influence of Company Culture and Structure

2.3.1 Overview

Simply transferring knowledge about good security practices isn't enough; it must be combined with behavioral strategies to foster positive cybersecurity habits within an organization (Bada et al., 2019). The literature consistently shows that training alone is insufficient to address the increasing cyber threats (Bada et al., 2019; Corradini, 2020; Daengsi et al., 2021; El-Bably, 2021; Greulich et al., 2024). Therefore, organizational culture plays a role in shaping effective cybersecurity training strategies, and is deemed a relevant aspect regarding this subject.

Creating a cybersecurity culture requires leadership to actively promote and engage in training, setting a company-wide example. A diverse workforce also enhances an organization's cybersecurity capabilities by offering varied perspectives that strengthen defenses (Corradini, 2020). This is supported by specialized training programs designed to meet the unique needs of various departments, recognizing that knowledge levels and training requirements can differ significantly within an organization (Daengsi et al., 2021). Employee involvement is essential, with adherence to cybersecurity rules often based on individual evaluations of costs and benefits (Corradini, 2020; El-Bably, 2021). Organizations can boost compliance with security protocols by fostering a positive workplace and continuously educating employees on cybersecurity. Trust and awareness are important, emphasizing the need for a strategy that promotes active engagement in security measures without complacent (Greulich et al., 2024).

Cybersecurity culture	Examples	In practice
Artifacts	Awareness training Technological devices Employees' behaviour	What we see
Values	Documents and papers describing values and principles of the organization Rules of conduct	What we share
Basic assumptions	Sense of time connected to the idea of progress and advancement in technology Consideration on the human contribution to work environment	What we think and believe

Figure 2.1: Elements of Cybersecurity Culture (Corradini, 2020, p. 66)

Organizational culture in cybersecurity includes both visible aspects like technology use and deeper, hidden elements like values and deep-seated beliefs that define an organization's core identity. This complex culture influences how decisions are made and how people view security, emphasizing the need for comprehensive cybersecurity strategies that match the organization's overall culture and its subcultures. This alignment helps improve security awareness and behavior throughout the organization (Corradini, 2020).

2.3.2 Summary and Critical Review

The literature on how company culture and structure affect cybersecurity is extensive but not fully explored. It presents cybersecurity not merely as a technical issue, but as a component of organizational behavior and operations. It calls for an integrated approach where cybersecurity is seamlessly incorporated into daily organizational activities, shaped by leadership, influenced by diverse employee perspectives, and responsive to shifts in trust and awareness among individuals (Bada et al., 2015; Corradini, 2020; Daengsi et al., 2021; El-Bably, 2021; Greulich et al., 2024). These findings are confirmed by a conference article covering a decade of studies (Vasudevan et al., 2023) which asserts that effective cybersecurity training must transcend mere compliance, integrating human, social, and technological factors to address individual behaviors and organizational needs. However, it also emphasizes the need for further research regarding a more comprehensive understanding of how different aspects interplay in the context of cybersecurity training.

2.4 Literature Summary

The critical literature review reveals that while foundational cybersecurity frameworks like ISO/IEC 27001 and NIST are important, they must continually adapt to the evolving digital threat landscape. This necessitates a balance between the generality of broad standards and the specificity needed for effective implementation in diverse technological environments (Culot et al., 2019; Djebbar & Nordström, 2023; El-Bably, 2021; Falco & Rosenbach, 2022; Handri et al., 2023). Various frameworks such as SAM, CSCF, and others underscore the integration of strategic, human, and technological dimensions to enhance cybersecurity postures (Belalcázar et al., 2017; Corradini, 2020; Hijji & Alam, 2022; Kose et al., 2021; Tsiodra et al., 2023). The literature also highlights a shift from traditional instructor-led training to innovative, blended methods that cater to diverse learning preferences and are grounded in evidence-based practices (Adams & Makramalla, 2015; Alsharif, Mishra & AlShehri, 2021; Angafor et al., 2020; Corradini, 2020; Evans, 2022; Qawasmeh et al., 2024), suggesting a need for more research into actual training methods employed by companies. Moreover, the importance of integrating cybersecurity into organizational culture is emphasized, advocating for a holistic approach that considers leadership, employee perspectives, and the interplay of trust and awareness (Bada, Sasse & Nurse, 2019; Corradini, 2020; Daengsi et al., 2021; El-Bably, 2021; Greulich et al., 2024). However, gaps exist in understanding how frameworks and training methods are applied within real-world settings, indicating opportunities for further study to explore these relationships more deeply.

After a comprehensive review of the literature on cybersecurity training strategies, it is clear that several aspects must be considered in their development. We identified the most prominent ones as: 1. Frameworks, Standards, and Models, 2. Training Methods, and 3. Organizational Culture. These elements seem essential for the effective formulation and implementation of cybersecurity training strategies. Frameworks, standards, and models emphasize the necessity of implementing awareness training, yet they often do not specify the types or methods of training to be used. Consequently, it is up to individual companies to determine which training methods their strategies should incorporate. Additionally, the literature consistently highlights the significance of organizational culture in influencing how employees accept and engage with awareness training.

3 Research Methodology

3.1 Literature Collection and Review

According to Oates (2006), a literature review can be broken down into seven different activities: searching, obtaining, assessing, reading, critically evaluating and writing a critical review. Henceforth, this is how we chose to conduct our literature collection and review.

For the ‘searching’ and ‘obtaining’ part of this thesis, we conducted a systematic literature review. Typically, the aim of a literature review is to collect all existing literature relevant to the topic (Jacobsen, 2024). However, given time and resource constraints, we adapted our approach to instead gather as much relevant literature as possible. In this part of the review, we followed the first four steps of a six-step guide which consists of the following phases: (1) Defining search keywords, (2) Choosing literature sources, (3) Choosing exclusion and inclusion criteria, (4) The search (Jacobsen, 2024). The fifth part of the guide is ‘First assessment of literature relevance’, which is the equivalent of the ‘assessing’ and ‘reading’ from Oates (2006). The final sixth step is the review of the final included literature is the equivalent to the ‘critically evaluating’ and ‘writing a critical review’ part from Oates (2006). The way we conducted these last two steps will be explained later in this chapter.

To conduct the systematic literature review, we defined the following key search terms, all prefixed with ‘Cybersecurity’:

Table 3.1: Keywords used during the literature search

Search Stage	Search Term (Cybersecurity-)
Initial search	Training
	Training Strategy
	Training for Employees
	Training in the Workplace
	Awareness
Final search	Framework
	Training Framework
	Models
	Standards

	Training Method
	Culture

Each search term belongs to a search stage. The first search stage is the ‘Initial search’, while the rest of the search terms were derived from this initial search, and used during a final literature search. We chose two online databases, LUBsearch and Google Scholar, as sources for our literature. We filtered out results that were published earlier than 2015, in order to not get literature that felt too out-of-date.

Table 3.2: Number of search results per keyword and online database

Keyword (Cybersecurity-)/Nbr of Results	LUBsearch	Google Scholar
Training	8 142	25 100
Training Strategy	764	22 700
Training for Employees	816	17 000
Training in the Workplace	97	16 900
Awareness Training	1 387	17 000
Training Framework	1 094	26 800
Training Model	2 549	19 700
Training Standard	485	19 000
Training Method	1 988	17 300
Culture	1 345	17 400

As demonstrated in Table 3.2, each keyword generated hundreds, and sometimes thousands, of search results. Due to time constraints, it was not feasible to review every result. Therefore, we prioritized the results by relevance and investigated the first 50 entries.

Upon reviewing the literature found during the initial search, which is the ‘assessing’ and ‘reading’ part of this thesis (Oates, 2006), we identified eight key aspects of the collected literature: 1. Descriptions of Cybersecurity Training Methods, 2. Case Studies and Examples, 3. Comparative Studies, 4. Industry-Specific Cybersecurity Needs, 5. Cybersecurity Training Frameworks and Models, 6. Influence of Company Culture and Structure, 7. Trends in Cybersecurity Training, and 8. Effective Methods. Thereafter, we went ahead and collected further literature relevant to these eight prominent aspects. At this stage, we also collected further literature by going “back in time” and searching the collected literature's bibliography (Jacobsen, 2024).

To direct the reader's attention to the concepts, rather than the authors, we made a deliberate choice to write concept-centric, rather than author-centric (Oates, 2006). To help us structure our thesis around concepts, rather than authors, we made a matrix that mapped out which literature covered which concepts. During the initial literature review mentioned above, we identified eight prominent aspects, which are coded as letters. After thoroughly reviewing and comparing the literature to each of these eight identified themes, it was evident that we were not able to find rich literature for each one of them. Because of this, two of the themes were removed ('Industry-Specific Cybersecurity Training Needs' and 'Trends in cybersecurity Training'), and two of the themes were divided into subgroups (Descriptions of Cybersecurity Training Methods' and 'Cybersecurity Frameworks and Models').

Table 3.3: Literature Concept Matrix – (A) Descriptions of Cybersecurity Training Methods, (B) Case Studies and Examples, (C) Comparative Studies, (D) Industry-Specific Cybersecurity Needs, (E) Cybersecurity Training Frameworks and Models, (F) Influence of Company Culture and Structure, (G) Trends in Cybersecurity Training, and (H) Effective Methods

Author/Concept	A	B	C	D	E	F	G	H
Adams	X							
Angafor	X							
Belaloazar		X			X			
Ben Salamah					X			X
Ghaskraborty								
Corradini	X				X	X		X
Culot					X			
Daengsi			X			X		
Djebbar			X		X			
El-Bably					X	X		
Evans	X	X			X	X		
Falco		X			X			
Flores	X			X			X	
Girraj	X			X				
Greulich						X		
Handri					X			
He	X		X					X
Hijji		X			X			
Kose	X				X			
Kwon			X		X			X
Lei Shen	X				X			
Moldovan			X					
Möller					X			X
Pawlicka								
Prümmer	X		X				X	X
Qawasmeah	X	X	X					X
Reeves "Get a red..."					X			
Reeves "Generic..."					X			X
Rohan					X			
RONCHI								
Sanjac					X			
Scotfield					X			
Sharma					X			
Tally	X							
Tayebani								
Tsiotra		X			X			
Udono								
Vasudevan						X		X
Zhang					X			
Prevalence	13	6	7	2	23	6	2	9
Decision	Divide	Keep	Keep	Remove	Divide	Keep	Remove	Keep

As illustrated in Table 3.3, each concept/theme is represented by a specific letter in the table columns. The rows list the first author of each article, conference presentation, or book identified in the final literature search. We marked an ‘X’ next to each theme covered by a given literature work. We then tallied the number of literature works associated with each of the eight themes, which helped us understand their prevalence. This analysis led us to refine our chosen themes for the review. Each column has a ‘Decision’ at the bottom, which is showcasing how we ultimately handled the category. The matrix revealed that themes A (Descriptions of Cybersecurity Training Methods) and E (Cybersecurity Training Frameworks and Models) were more common than others, prompting us to subdivide these categories for more detailed exploration. Conversely, themes D (Industry-Specific Cybersecurity Needs) and G (Trends in Cybersecurity Training) had scant literature, leading to their elimination from our review. Columns D and G were therefore grayed out to show their removal visually. Some of the author names in the rows are crossed out, this is because we could not find any of the eight identified themes in these, and they were therefore deemed irrelevant to the subject of the thesis.

Subsequently, we conducted a narrative literature review, characterized by its focus on discussing and interpreting prominent themes within the collected literature. This approach allowed us to synthesize and present the findings as a coherent narrative, providing insights into the subject (Andreasson & Johansson, 2024). Ultimately, the previously identified prominent themes from our literature review on “Cybersecurity Training Strategies” were categorized into three main categories: 1. Frameworks, Models and Standards, 2. Training Methods, and 3. Organizational Culture. The literature review was in the end structured around these three key aspects. Further reading of the literature resulted in that not all the literature listed in the matrix above was used. This was because it was not deemed relevant to the study.

Table 3.4: Six prominent themes categorized into three main categories – (A) Descriptions of Cybersecurity Training Methods, (B) Case Studies and Examples, (C) Comparative Studies, (E) Cybersecurity Training Frameworks and Models, (F) Influence of Company Culture and Structure, and (H) Effective Methods

Main Category	Subcategory
Frameworks, Standards and Models	B, C, E
Training Methods	A, B, C, H
Organizational Culture	B, C, F

Then, for the ‘critically evaluating’ and ‘writing a critical review’ part of this thesis (Oates, 2006), we expanded on this narrative review to conduct a critical one for each of the collective literature regarding the prominent themes/aspects found during the initial review. We identified how the studies conducted in the literature could have been enhanced, as well as what areas seem to lack literature. This critical review made our problem area clearer and further confirmed that this thesis would help fill in the gap of missing literature within the area.

3.2 Data Collection

3.2.1 *Semi-structured Individual Interviews*

To answer the research question for this thesis, we needed to obtain detailed information about the cybersecurity training strategies used in companies today. In this thesis, we conducted a descriptive study and determined that an intensive method design would best suit our study's purpose, as it allows us to delve deeper into a specific phenomenon. Given the complexity of the information we sought, we opted for a method that involved collecting data in the form of words, rather than numbers. As intensive method designs typically generate qualitative data, our study was therefore qualitative. Furthermore, an intensive study supports the possibility of creating theoretical (analytical) generalization, which is our goal in this qualitative study (Jacobsen, 2024). We will discuss theoretical generalization further in Chapter 3.4.2, Transferability.

Although our intent was not to collect personal data, it is reasonable to assume that internal corporate information on cybersecurity training strategies could be sensitive. Informants are more likely to share sensitive information during interviews than in surveys (Oates, 2006), which is why we chose interviews as our data collection method. Interviews are particularly suitable for sensitive issues and when informants may be reluctant to document information on paper. We conducted semi-structured interviews, allowing informants to respond more freely, introduce their own questions and thoughts, and enabling us to ask spontaneous questions that yielded additional data beyond what structured interview questions would provide (Oates, 2006).

Before the interviews, we sent all informants the questions from our interview guide to allow them time to prepare, promoting openness and trust. We also opted to host the interviews in locations where informants would feel most comfortable, either in their office on site or online. While we preferred physical meetings for their ability to foster trust, openness, and a good flow of conversation (Jacobsen, 2024), some interviews had to be conducted online due to time constraints.

For documentation, we audio- and video-recorded the interviews. Online interviews were video recorded using Microsoft Teams' built-in function, while on-site interviews were audio recorded using a personal smartphone with the iPhone's 'Voice Memos' app. Data was saved locally on a personal computer to avoid cloud storage. On-site interviews also included field notes as backup documentation in case of audio recording failures. We conducted six interviews in total, and these recordings were later transcribed, processed, and analyzed—more on this in Chapter 3.3, Data Analysis Preparation and Process.

For structuring the interview, we created an interview guide (detailed further in Chapter 3.2.2, Interview Guide), containing highly structured questions while maintaining the flexibility of semi-structured interviews. We conducted a trial interview with one of the informants at the beginning of the study to refine our approach for the 'real' interviews. This trial lasted about 20 minutes, setting our expectation that subsequent interviews would not exceed 30 minutes. Although 30 minutes is typically short for gathering detailed information (Jacobsen, 2024), our structured interview guide allowed us to obtain the insights we sought (and more).

During each interview, we started with an introduction, restated the purpose of the study, and collected basic information about the respondent and the company. We consciously avoided

directing the conversation, allowing the informant to speak freely on any subject. We made a concerted effort to display interest and adopt listening positions to make the informant comfortable and encourage more open and detailed responses. We avoided interrupting the informant, fostering longer and more informative replies (Jacobsen, 2024).

3.2.2 Interview Guide

For the semi-structured interviews we developed an interview guide based on our literature review, containing 16 questions. The purpose of these interviews is to encourage informants to share their own thoughts freely. Although our approach leaned towards a structured format, the guide we created was still quite detailed, resulting in what could be described as a highly structured interview guide (Jacobsen, 2024). We organized the interview questions into themes based on the three key aspects identified in the literature review: 1. Frameworks, Models, and Standards, 2. Training Methods, and 3. Organizational Culture. One question was formed as a contextual question, considering companies can develop their training material either in-house or by external provider, or both. Some questions were designed to elicit more open responses, while others required specific answers based on the literature, such as questions about remote workers or social media use. We made a deliberate effort to ask open-ended questions to facilitate a more expansive discussion (Oates, 2006).

Table 3.5: Source Mapping of Interview Questions to Accounting Literature Review Sections

Aspect	Interview Question	Literature Review Section
Frameworks, Standards and Models	Do you follow a specific framework, model, or standard in developing your cybersecurity training programs?	Sec. 2.1.1: Cybersecurity Frameworks, Standards and Models, pp. 4-5
	In what ways does this framework, model, or standard influence the design of your cybersecurity training?	Sec. 2.1.1: Cybersecurity Frameworks, Standards and Models, pp. 4-5
	How do you ensure that your training content remains current with evolving cybersecurity practices and threats?	Sec. 1.1: Background, p. 1
	Have there been any modifications or enhancements to your training strategies concerning remote employees?	Sec. 2.1.1: Cybersecurity Frameworks, Standards and Models, p. 5
	Are there specific strategies in place to heighten cybersecurity awareness about social media risks?	Sec. 2.1.2: Challenges, pp. 5-6
Training Methods	What types of training are you implementing to enhance cybersecurity awareness among your employees?	Sec. 2.2.1: Cybersecurity Awareness Training Methods, p. 7
	Do you utilize a singular training method, or do you employ a combination of multiple methods?	Sec. 2.2.2: Training Methods, p. 8
	Please specify the training methods you employ (see list).	Sec. 2.2.2: Training Methods, p. 8
	Do you develop your cybersecurity awareness training materials internally, or do you engage external providers? Can you elaborate on which one?	<i>Contextual question</i>
	If external providers are employed, could you identify the provider and specify the service or product being used?	Sec. 2.2.2: Training Methods, p. 8

	How frequently are employees required to undergo this training?	Sec. 2.2.2: Training Methods, pp. 7-8
	What is the typical duration of these training sessions?	Sec. 2.2.2: Training Methods, pp. 7-8
Organizational Culture	What strategies are in place to cultivate a culture of cybersecurity awareness within your organization?	Sec. 2.3.1: Influence of Company and Culture, p. 9
	Is the cybersecurity training customized to accommodate the diverse needs of different employee groups within your organization? Please describe how.	Sec. 2.3.1: Influence of Company and Culture, p. 9
	What measures are in place to ensure that leadership and management actively promote a culture of cybersecurity?	Sec. 2.3.1: Influence of Company and Culture, p. 9
	How is cybersecurity awareness integrated into the core values of your organization?	Sec. 2.3.1: Influence of Company and Culture, p. 9

The complete interview guide is available in Appendix A. It begins with an introduction that restates the study's purpose to the informant, prompts the interviewer to request permission to record the conversation, and informs the informant about their rights to confidentiality and anonymity. The informant is also asked to provide their name and company role. Following the introduction, the guide includes a total of sixteen questions that are derived and organized thematically based on the literature review. The guide concludes with a prompt for the interviewer to ask the informant if they have any questions or additional thoughts (Oates, 2006).

3.2.3 Informant Selection

When choosing our selection method, we first developed an overview of the types of informants we wanted to interview. We aimed to find informants from companies that conduct cybersecurity training, which are logically assumed to have some form of cybersecurity training strategy in place. We structured our method selection into three phases: 1. Getting an overview of all potential informants, 2. Specifying inclusion and exclusion criteria, and 3. Specifying selection criteria (Jacobsen, 2024). The first phase involved imagining we had unlimited time, money, and analytical resources, and considering whom we would choose to interview under those circumstances. For us, that meant targeting informants from all companies that conduct cybersecurity awareness training. However, given our limited resources, we quickly moved to the next phase: specifying inclusion and exclusion criteria. In this thesis, we consciously avoided restricting the pool of informants. We anticipated challenges in finding candidates due to time constraints and a potential lack of interest from companies in participating in the study. Therefore, our inclusion and exclusion criteria were essentially the same as our initial overview of desired informants from the first phase. For the final phase, specifying selection criteria, we chose 'Information' as the formal selection criterion (Jacobsen, 2024). This meant we selected companies that we believed could provide extensive and relevant information for our thesis topic. When sending out invitations for our study, we requested interviews with an informant who is directly involved or knowledgeable about the cybersecurity training strategy at their company.

We employed a form of convenience sampling (Andreasson & Johansson, 2024) in selecting candidates. We sent invitations to about twenty companies based on our information selection

criteria. Ultimately, three companies responded with an interest in participating in the study. We found two additional candidates through personal contacts, giving us a total of five informants. Our selection method can also be seen as somewhat random (Andreasson & Johansson, 2024), as we randomly chose informants who were deemed to have relevant information about the topic of this thesis.

Table 3.6: Table of informants

Informant	Role	Interview length	Interview Date
I1	Security Manager	20:23	16-04-2024
I2	Chief Operating Officer (COO)	24:53	16-04-2024
I3	ERP Project Manager	20:27	17-04-2024
I4	Information Security Auditor	27:56	18-04-2024
I5	Chief Information Officer (CIO)	25:00	19-04-2024

Even though none of the informants in this study expressed a wish to be anonymous, we have chosen to keep them anonymous. This is because we want the focus to remain on the content and implications on the findings, rather than the identities of the informants. Ultimately the informants consisted of five informants from five different companies in various industries, and with varying IT roles. To enhance the transferability (Oates, 2006) of this research, here is detailed background information for each of the informants:

- Informant 1 is responsible for information security at his company, focusing on driving the management system and ensuring compliance with security practices. Although he isn't part of the management team, he works closely with it, coordinating with the IT manager, CTO, and CPO. His company develops and sells CRM software, offering both cloud-based solutions and on-premise installations, emphasizing security across their product lines.
- Informant 2 oversees corporate IT, security frameworks, and enterprise architecture at his company, which is an IoT company that builds and sells secure IoT communications across various business verticals. He manages a large team including a Chief Information Security Officer and Director of Corporate IT, aiming to integrate business units effectively across the organization's broad geographic and digital footprint.
- Informant 3, primarily a project manager at her company, recently oversaw business IT and operations. Her role includes managing ERP integration, BI, and data-driven applications, focusing heavily on AI and related technologies. Her company operates entirely in the cloud and provides extensive consulting services, mainly to clients in the food industry.
- Informant 4 specializes in M365 and security as an ISO auditor within his consultancy firm, which develops intranets and other systems for clients. His role is critical in ensuring the company adheres to various standards and regulations, leveraging his expertise in security to enhance the firm's offerings and compliance.
- As the IT manager at his company, Informant 5 has built the IT department from scratch and is involved in all aspects of IT management including security, budgeting, and license management. He also contributes to operational technologies, coordinating

extensively with both internal staff and external consultants to ensure robust security and operational efficacy in a company focused on utilities and essential services.

Moreover, all informants (and companies) were invited by email, and each of them verbally consented to participating in an interview. The consents are regarded as informed (Oates, 2006) since we repeatedly sent out information regarding the purpose of the study, and that it will entail an interview.

Hej,

Mitt namn är Annie och jag studerar just nu det systemvetenskapliga kandidatprogrammet vid Lunds universitet. Tillsammans med min partner Sebastian genomför vi en undersökning gällande utbildning inom cybersäkerhet hos IT-företag, som är en del av vårt examensarbete. Vi undrar om det finns någon på [REDACTED] som är involverad i utbildningen av cybersäkerhet i ert företag, och som hade kunnat ställa upp på en kort intervju med oss? Intervjun skulle omfatta frågor om hur era utbildningar och kurser inom cybersäkerhet för era anställda är strukturerade och hur de tillämpas. Intervjun tar inte mer än 30 minuter och vi hade uppskattat er medverkan enormt.

Om ni är intresserade så mejlar vi intervjufrågorna på förhand så att ni får chans att förbereda er.

Med vänliga hälsningar,
Annie & Sebastian

Figure 3.1: An example initial invitation email that we sent out to some of the informants, we also invited informants through personal connections

3.3 Data Analysis Preparation and Process

3.3.1 Transcription

The initial phase of any qualitative analysis involves transcribing interviews (Jacobsen, 2024). Therefore, after collecting our interview data, we promptly transcribed the audio recordings. This step is crucial because written data is easier to analyze than audio-only data (Oates, 2006). Moreover, transcription allows others to verify the raw data, facilitating the evaluation of our interpretations (Jacobsen, 2024). In this thesis, we employed several methods to transcribe all five interviews. Initially, we used an automatic transcription tool named "Whisper" (OpenAI, 2022) for two of the recordings. Whisper is an open-source Automatic Speech Recognition (ASR) model developed by OpenAI, designed specifically for transcription and translation tasks. This tool was recommended by our Director of Studies and the formal examiner of this thesis. We operated Whisper on our private computer to ensure that no data was transferred to third parties, thus adhering to the Lund University School of Economics and Management's guidelines for handling personal data in student projects. Whisper is freely available for download, and we utilized a tutorial video posted by our Director of Studies on the learning platform 'Canvas' to guide us through the process.

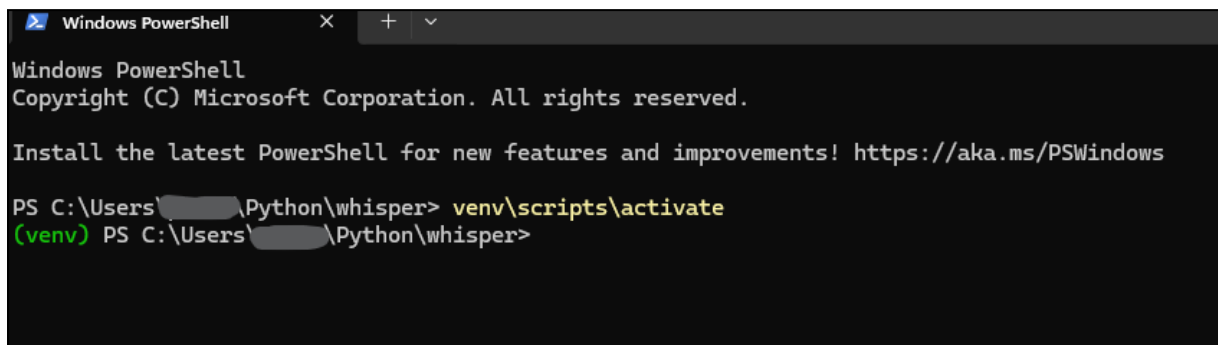


Figure 3.2: How we ran ‘Whisper’ locally in the PowerShell terminal on the computer

However, we found that using this tool was too time-consuming. Given that the transcripts produced by Whisper still required additional, time-consuming adjustments, we decided to switch to another tool. The next tool we used is called ‘MAXQDA’ (MAXQDA, 2024), a qualitative data analysis application that provides advanced coding, retrieval, transcription, and visualization tools. This tool stores data exclusively on GDPR-compliant servers, and the media files automatically get deleted after seven days if not manually initiated. We primarily used MAXQDA as a transcription tool to refine the transcripts generated by Whisper, aligning them more closely with our desired format. We downloaded MAXQDA from its official website and utilized their 14-day free trial.

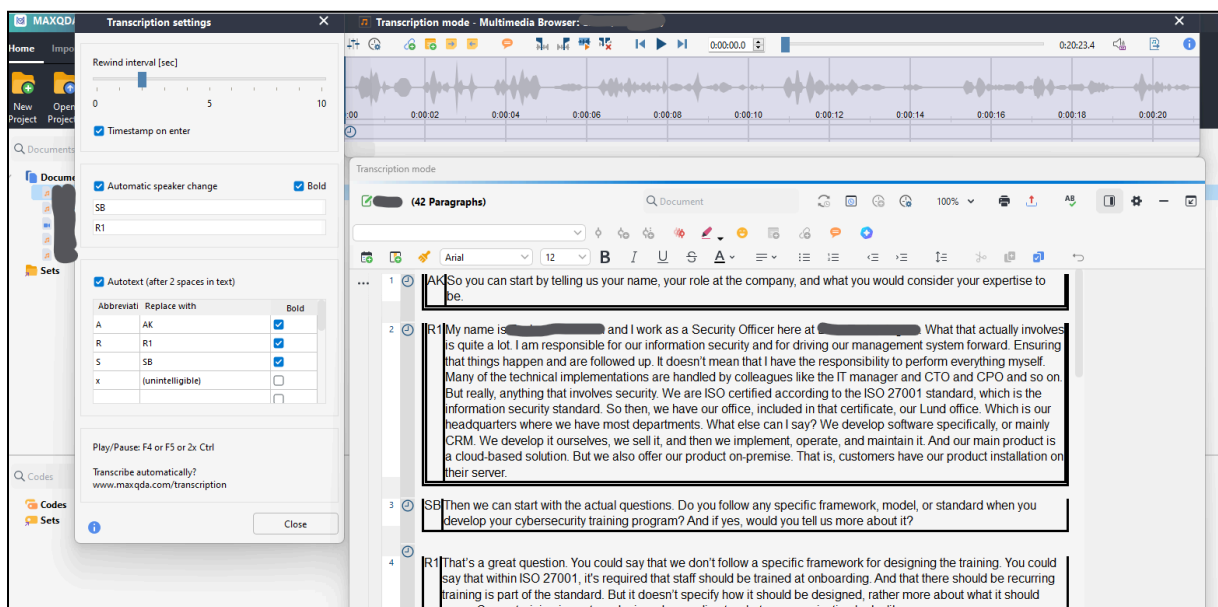


Figure 3.3: How we transcribed audio recordings using ‘MAXQDA’

For the remaining three audio recordings, we opted to transcribe them manually using the Voice Typing tool in ‘Google Docs’ (Google, 2024a). We chose manual transcription ultimately because it proved to be the least time-consuming approach overall, and dictation further reduced the time required.

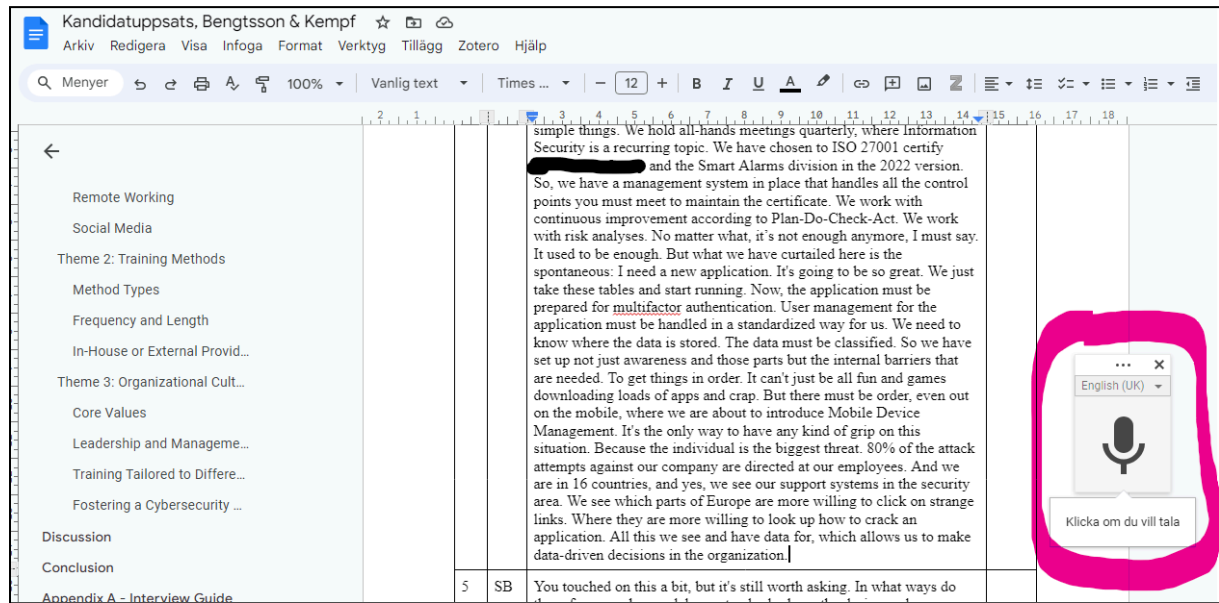


Figure 3.4: How we transcribed the audio recordings manually through the Voice typing-tool in 'Google Docs'

We performed an intelligent verbatim transcription of the interview audio recordings. An intelligent verbatim transcription is a style of transcription that aims to capture the essence and meaning of spoken words without recording every sound or utterance, like “um” or “like”. Often, intelligent verbatim may be the preferred method as it makes participant quotes more readable by omitting excessive repetitions and verbal fillers (McMullin, 2023). Some of the raw transcriptions from the interviews had an excessive amount of verbal fillers, which made the transcription difficult to read. Therefore, we made the decision to conduct intelligent verbatim transcription, and removed filler sounds manually from the transcriptions.

For the transcription format, we adopted a table with four columns: the first column for the codeline, the second for the speaker's name, the third for the actual transcription, and the fourth reserved for coding at a later stage. We numbered each line in the transcripts to facilitate easy reference to specific responses during subsequent data analysis (Oates, 2006). Additionally, each transcript was labeled with details such as the location, date, duration, participants, and language of the interview (Jacobsen, 2024; Oates, 2006).

Location: Online

Date: 17-04-2024

Length: 20:27 minutes

Participants: Informant 3 (I3), Sebastian Bengtsson (SB), Annie Kempf (AK)

Language: Swedish

#	P	Conversation	Code
1	SB	You can remain anonymous and stop participating in the interview whenever you want, it's up to you. But then we can start a bit with your name, your expertise, and what a company does.	
2	I3	My name is [REDACTED], and I am primarily a project manager at [REDACTED] within ERP, business systems. But since June last year, I have been temporarily responsible for our business IT and business operations, which includes our internal support and support for our customers, as well as our internal IT and IT training. I have just handed that over to [REDACTED], who has been on maternity leave, but I took this interview anyway because quite a lot has happened in this world over the past year.	
3	AK	Can you tell us a bit about what [REDACTED] does, and what kind of company it is?	
4	I3	We are an IT consulting company with four different branches. Firstly, IT business operations, as I mentioned, which involves a lot of support and IT operations. Then we have ERP integration, where we work with business systems and integrations of business systems. Next is BI, where we work with business insights, including data warehouses and reports such as PowerBI, and so on. Lastly, we have data-driven applications, which is the application development side and we work a lot with AI and related areas. So those are our four branches. I mainly work with clients in the food industry. We do not have our own servers;	

Figure 3.5: Formatting and labeling of the transcriptions

3.3.2 Data Storing

Most of the material for the thesis has been stored on 'Google Drive' (Google, 2024b). However, to mitigate the risk of personal data being uploaded to the cloud, the raw data—specifically the audio recordings—was stored locally on our computers. Although the data we collected is not classified as personal data, we deemed it prudent to take this precaution. To prevent the loss of any collected data, we made duplicates of all recordings (Oates, 2006). In the transcriptions stored on Google Drive, we took measures to anonymize the data, obscuring any information that could link the data to specific companies or informants by redacting both informant and company names.

3.3.3 Member Checking

After transcribing the interviews, we sent copies to each informant for review. This process allowed them to verify the accuracy of the facts and confirm that their statements were

correctly interpreted and translated (Oates, 2006). Four out of five informants reported that the transcriptions were generally accurate but noted some spelling errors and incorrect words. For instance, Informant 3 clarified that one of the incoherent words was meant to be “front-end”, and that one of her statements was duplicated. These errors have since been corrected, and all the transcripts have been modified according to the feedback from the informants. The remaining informant indicated that the transcription looked good. Ensuring this accuracy was important for us as it helped enhance the credibility of our study (Oates, 2006).



Figure 3.6: Picture showing the email we sent out to each informant for validation of the transcripts

3.3.4 Data Coding

In this thesis, our data analysis employed a deductive approach (Oates, 2006), as detailed further in Chapter 3.3.5, Data Analysis. This means that we identified themes during the literature review and structured our data analysis around these established themes. We ended up with 41 different codes, and created a codebook to note each code used and the kind of data to which it applies (Oates, 2006). These were the initial 41 codes derived from the literature review:

- | | |
|---|---|
| 1. Frameworks, Standards and Models (Main category) | 10. FSM Remote Working |
| 2. Training Methods (Main category) | 11. Types of FSM Employed |
| 3. Organizational Culture (Main category) | 12. ISO/IEC 27001 |
| 4. FSM Definitions | 13. NIST |
| 5. FSM Challenges | 14. Strategic Alignment Model |
| 6. Integration of Security Training | 15. Information Security Culture Framework |
| 7. FSM Updates and Evolution | 16. Competing Security Cultures Framework |
| 8. Human Factors Integration | 17. Information Security Culture Assessment |
| 9. FSM Social Media | |

- | | |
|--|--|
| 18. The Security Culture Toolkit | 29. TM Social Media |
| 19. CAT framework | 30. TM Remote Working |
| 20. CyberSec Labs framework | 31. Types of Training Methods |
| 21. CENSOR framework | 32. Conventional Methods |
| 22. The Adaptive Cybersecurity Training framework for Social Media Risks | 33. Interactive and Experiential |
| 23. Open Web Application Security Project | 34. Technology-Driven |
| 24. Training Frequency | 35. Informal Learning |
| 25. Training Duration | 36. Blended Approaches |
| 26. Internal Training Material | 37. Security Organizational Culture Strategy |
| 27. External Training Material | 38. Leadership |
| 28. Awareness Training Purpose | 39. Personalization |
| | 40. Core Values |
| | 41. Positive Workplace Environment |

While coding the transcripts, new themes emerged and codes were gradually added to the codebook. The following codes were derived from the data:

- | | |
|---|--|
| 1. Informant Background (Main category) | 7. Description of Security Training |
| 2. Swedish Civil Contingencies Agency (MSB) | 8. Training Results |
| 3. External FSM | 9. Security Culture Surrounding Remote Working |
| 4. Internal FSM | 10. Security Culture Surrounding Social Media |
| 5. Plan-Do-Check-Act | 11. Culture Challenges |
| 6. Zero Trust Security Model | 12. Informant Role |
| | 13. Informant Company |

We in total added 13 more codes during the coding, resulting in 54 total codes. A snippet from the finalized codebook can be seen in Figure 3.7.

Table B1: Main coding categories with their corresponding abbreviation

Main Category	Code Abbreviation
Frameworks, Standards and Models	FSM
Training Methods	TM
Organizational Culture	OC
Informant Background	IB

Table B2: Coding categories with their corresponding abbreviations, definitions, as well as an example taken from the transcripts

Code Name (Abbreviation)	Code Definition	Transcription Example
FSM Definitions (FSM_FD)	Informant describes a framework, model or standard	"In some cases, if we take ISO security, or ISO-27001, which is the security certification, it sometimes places general requirements such as the company should handle backups correctly or that we should not disclose confidential information to unauthorized persons."
Challenges (FSM_Chall)	Informant describes challenges with a framework, model or standard	-
Integration of Security Training (FSM_STI)	Informant describes how the employed framework, model or standard influences the security training	"And the ones we build ourselves are also influenced by, for example, the ISO certification, the requirements and controls that come from the ISO certification and OWASP"
FSM Updates and Evolution (FSM_FUE)	Informant describes how	"We have a security officer who is part of that process. Then we look for

Figure 3.7: Codebook detailed in Appendix B

Since the interviews were semi-structured around questions directly derived from these themes, using the same themes for data analysis ensured that our coding scheme was exhaustive. This means the coding scheme covered every predefined option and captured all relevant themes found in the data (Oates, 2006). Derived from the literature review, we used three main categories for all the created themes: 1. Frameworks, Standards and Models, 2. Training Methods, and 3. Organizational Culture. Then, using these three predefined main themes, we coded for several subthemes corresponding to each of these main themes. In the codebook, each of the codes have a definition and an example from the transcripts. This codebook facilitated the data coding of the transcripts significantly.

Table 3.7: Main coding categories with their corresponding code abbreviation

Main Category	Code Abbreviation
Informant Background	IB
Frameworks, Standards and Models	FSM
Training Methods	TM
Organizational Culture	OC

One change we did with the themes derived from the literature was to move the theme about social media and remote working to the organizational culture-category (from the frameworks, standards and models-category). This is because a recurring theme within the data was that the informants always answered ‘No’ to the question whether they have any specialized training strategies aimed at social media usage and remote working, however, they always added that there are guidelines and restrictions regarding these areas. It seems the companies are trying to incorporate this way of thinking into the culture, rather than include it in specialized training. We also gave types of frameworks, standards and models their own coding category, and we did the same with types of training methods. For the addition of codes during the transcription coding, we added a new main category, Informant Background, so that we had a way to code which parts of the transcriptions that were not directly relevant to the study, but still useful as background information (Oates, 2006).

Consistency in application was maintained as one researcher focused on the data intended for actual use, while another conducted a separate coding process (investigator triangulation) to enhance the research credibility (Oates, 2006).

For this thesis, we opted for textual coding instead of color- or symbol coding, following the recommendation of our thesis supervisor. This choice was made for its simplicity, inclusivity for colorblind readers, and to avoid issues with overlapping themes, which can be problematic with color coding. Additionally, our transcript table design facilitated direct coding into the transcripts in the right-most column labeled 'Code', as demonstrated in Appendices B, C, D, E, and F. During transcription, each question and response was placed in its own cell. However, during coding we opted for something more similar to line-by-line coding. What we mean by that is that we divided the responses into sections and coded them ‘section-by-section’. The reason for that is because we often wanted to code for more than one theme in the same response, and we needed a way to make this visibly clear to the reader. The alternative was to highlight each section and put the code into parenthesis in-text, but this was less visibly clear to the eye.

7	AK	But do you have any sort of cybersecurity training for employees?	
8	I3	Yes, we do. It's a group-wide cybersecurity training developed by a group called [REDACTED], which we are a part of.	TM_ITM
9	I3	They have created a training course that consists of a video, followed by a few questions to answer.	TM_DST TM_TE_TD
10	I3	This is done when you start and then once a year, but a lot of it is common sense.	TM_FR

Figure 3.8: An example of how we divided informant responses to code section-by-section

3.3.5 Data Analysis

After collecting and transcribing the data, we proceeded to perform a qualitative data analysis. This analysis, as outlined by Oates (2006), was deductive, meaning we examined the data using predefined themes from the literature review: 1. Frameworks, Standards and Models, 2. Training Methods, and 3. Organizational Culture. We created a coding scheme consisting of a total of 41 codes, each code belonging to one of these predefined themes.

Our approach involved categorizing data into three segment types as suggested by Oates (2006): 1. Irrelevant segments, which were disregarded; 2. Context segments, used for background information in Chapter 3.2.3; and 3. Relevant segments, which were coded and analyzed according to the literature-derived themes. This method was particularly effective as all interview questions were based on these themes, allowing straightforward coding of responses. Additionally, a second round of coding was conducted to identify any emergent themes not initially aligned with the posed questions. We discovered instances where informants provided insights applicable to other themes, beyond the scope of the original questions. In the end, we coded for a total of 54 different themes and subthemes.

The analysis also extended to comparing cybersecurity training strategies across different companies, identifying both commonalities and distinctions. Efforts were made to summarize and interpret findings within each thematic area. This analysis was conducted manually on a computer.

Ultimately, we also gathered some quantitative data by counting the frequency of codes applied to each theme. In total, the data was coded for 224 times. The results are tabulated below.

Table 3.8: Quantitative table showing how many times a theme was coded for

Code	Count	Relative Frequency (%)
FSM	50	~22
TM	110	~49
OC	64	~29

This quantitative analysis revealed that we coded substantially more for the theme Training Methods (TM) compared to Frameworks, Standards, and Models (FSM) and Organizational Culture (OC). This discrepancy can be partially attributed to the design of our interview guide, which included seven questions for TM, compared to five for both FSM and OC, reasonably generating more data content for the TM-theme.

We also calculated which subthemes were coded for most frequently, as well as which were not coded for at all.

Table 3.9: The top most frequently coded subthemes

Subthemes	Relative Frequency (%)
Description of Security Training	~9
Security Organizational Culture Strategy	~8
External Training Material	~7
Interactive and Experiential Training Type	~6
Training Frequency	~6
Personalization	~5
Definition of Framework, Standard or Model	~5

There were also some subthemes that we did not find any prevalence for in the data, and were therefore not coded for at all. These included challenges and types of frameworks, standards, and models, as well as the purpose of awareness training.

Furthermore, the coded segments were synthesized, compared, and are presented thematically in Chapter 4, Results. This thematic presentation, rather than an informant-centric approach, allows us to maintain a focus on the findings themselves. Accordingly, the results are organized into three primary themes of this thesis: 1. Frameworks, Standards, and Models; 2. Training Methods; and 3. Organizational Culture. Within the results section, we incorporate both the synthesized findings and several illustrative quotes from each informant's transcriptions. Additionally, we discuss the implications of these findings for the companies involved, offering interpretations that highlight their potential impact. Individual transcript segments are referenced in parenthesis in-text, in the format of '(informant:line)'.

1.2.3 In-House or External Providers

Informants 4 and 5 describe significant in-house efforts in developing their cybersecurity training programs. Informant 4 mentions that their organization creates its own training, tailored to meet the specific needs of all employees, alongside using widely recognized platforms like OWASP and DISA (I4:8, I4:23). This approach suggests a high level of control over the content, ensuring that it aligns closely with internal policies and employee roles. Similarly, Informant 5 emphasizes the internal development of training materials, supplemented by inputs from external information services (I5:36, I5:37, I5:38).

"Then of course we take in input and information from external parties where we get the information ourselves. We subscribe to a variety of services with information about different security trends, hot trends and so on and that makes us continuously adapt our training, whatever info you go out with. The actual design is what we do ourselves, but then we use external providers just for—the services we use, Junglemap for microtraining, which is a flexible service that can be linked with various reports to Azure. I built an API that we could use. That's mainly what we use. But otherwise, it's a lot that we develop ourselves on our intranet." (I5:37)

This hybrid approach allows them to design training that is highly specific to their organizational context while staying updated on the latest security trends through subscriptions to services like Junglemap for microtraining.

Contrastingly, Informants 1, 2 and 3 lean more towards leveraging external resources for their training needs. Informant 1 integrates externally produced tools like Secure Flag for specialized training for developers and utilizes open-source platforms like GoPhish to enhance their phishing training campaigns (I1:27, I1:29, I1:39).

Figure 3.9: The way we chose to present our results in Chapter 4, Results

3.4 Research Quality

Given that the study is qualitative in nature, we will adopt an interpretivist approach to discuss research quality (Oates, 2006). This discussion will include an evaluation of several quality criteria appropriate to this framework: trustworthiness, credibility, transferability, dependability, and confirmability.

3.4.1 Credibility and Confirmability

To enhance the credibility and confirmability of our research, several measures were taken. Firstly, we conducted a member checking (Oates, 2006). This meant that after transcribing the interview audio recordings, we sent the transcriptions to each of the informants and asked them to verify them. Four out of five informants responded with feedback, and corrections were therefore made to the transcriptions. Most of the feedback was spelling errors, corrections of words, wishes to remove unnecessary colloquial words and sentences, as well as informational additions. By letting the informants validate the data, we ensure that it shows what the informant intended to communicate. Additionally, this measure was made to mitigate researcher bias by ensuring that the findings are the result of the informants' inputs and not

overly shaped by the researcher's preconceptions. Our conducted member checking is further detailed in Chapter 3.3.3, Member Checking.

We also conducted a form of investigator triangulation (Oates, 2006) during the coding phase of the data analysis, enabling us to investigate the 'intercoder reliability' (Cheung & Tai, 2023). In this thesis, we will refer to this method as 'intercoder agreement' to remove the positivistic aspect, signaling that this is interpretivist research. One of the researchers of this thesis conducted the data coding which is used for the result of this thesis, while the second researcher conducted a separate data coding. Specifically, the second researcher proceeded with the already segmented transcript and coded using the already created coding scheme. We then calculated the percentage agreement by comparing how many coded segments we agreed on, versus which we disagreed on.

Table 3.10: Contingency table showing the results of the intercoder agreement test

	R2 Agrees	R2 Disagrees	Total Codings
R1 Codes	218	6	224
R1 Does Not Code	0	44	44
R2 Codes	218	50	262
R1 + R2 Codes			268

Explanation of each cell in Table 3.10:

- **R1 Codes / R2 Agrees:** This cell (218) shows the number of times Researcher 2 agreed with the codings of Researcher 1.
- **R1 Codes / R2 Disagrees:** This cell (6) shows the number of times Researcher 2 disagreed with the codings of Researcher 1.
- **R1 Codes / Total Codes:** This cell (224) shows the number of times Researcher 1 coded.
- **R1 Does Not Code / R2 Disagrees:** This cell (44) shows the number of additional codes that Researcher 2 added that were not coded by Researcher 1 at all.
- **R2 Codes / R2 Disagrees:** This cell (6+44=50) shows the number of disagrees that researcher 2 had with the codings of researcher 1.
- **R2 Codes / Total Codings:** This cell (218+44=262) shows the number of codings that were made by Researcher 2.
- **R1 + R2 Codes / Total Codings:** This cell (262+6=268) shows the number of codings made by researchers 1 and 2.

In evaluating the intercoder agreement between researcher 1 and 2, we employed a straightforward method to determine the percentage of agreement in coding. Researcher 1 coded a total of 224 instances. Of these, researcher 2 agreed with 218 codings, indicating a high degree of consensus. This results in a calculated agreement percentage of approximately 97%, computed as follows:

$$\text{Agreement Percentage} = \left(\frac{\text{Agreements}}{\text{Total Codings by R1}} \right) \times 100 = \left(\frac{218}{224} \right) \times 100 \approx 97\%$$

However, to capture a comprehensive picture of the intercoder agreement, it was crucial to consider the additional codings made by researcher 2, who coded 44 times when researcher 1 did not code. Incorporating these additional instances modifies the basis of comparison, bringing the total number of codings by both researchers to 268. The overall agreement, taking into account both the matches and mismatches, can thus be recalculated:

$$\text{Overall Agreement Percentage} = \left(\frac{\text{Agreements}}{\text{Total Codings}} \right) \times 100 = \left(\frac{218}{268} \right) \times 100 \approx 81\%$$

In conclusion, the overall agreement percentage has been calculated to approximately 81%. However, 88% of the disagreements were because of additional codings that researcher 2 made, that researcher 1 did not make. Removing these codings from the calculation, we get an agreement percentage of 97%.

3.4.2 Transferability

To facilitate the evaluation of the transferability (Oates, 2006) of the research in this thesis, we provided detailed descriptions of the participants, as seen in Chapter 3.2.3, Informant Selection. We also aimed at achieving complete data saturation by actively looking, and adding, new themes emerging from the data simultaneously to the data analysis. We added a total of 13 new codes during the process of data analysis, as seen in Chapter 3.3.4, Data Coding. Additionally, we have put great effort into making sure the methodology is clearly described so that other researchers can understand the processes used to gather and analyze data, which in turn affects whether findings can be deemed transferable. The transferability of this research was further discussed in Chapter 5.2, Limitations, by discussing how the findings might be relevant to other settings, populations, or contexts.

3.4.3 Dependability

To enhance the dependability of the research presented in this thesis, substantial effort was dedicated to meticulously recording and documenting the research process. This comprehensive documentation includes detailed records of how data was collected, how interview questions were designed and administered, and the methods used for data analysis. We have maintained an audit trail that details all decisions made and any changes to the research process. An example of this is when we thoroughly documented the decision about what method to use for the transcription of the interview audio recordings. We changed methods several times, and recorded each change in Chapter 3.3.1, Transcription. This level of transparency allows for the possibility of conducting an external audit, enabling others to trace the research steps thoroughly and verify our findings and conclusions. Following the guidelines suggested by Oates (2006), we believe that our systematic approach provides a reliable basis for reproducing this study under similar conditions.

3.4.4 *Trustworthiness*

In this thesis, we have comprehensively addressed the dimensions of trustworthiness—credibility, confirmability, transferability, and dependability—integral to qualitative research, particularly within an interpretivist framework. Credibility and confirmability were enhanced through methods such as member checking and investigator triangulation. By involving informants in the verification of transcription data and employing dual coders to cross-validate the coding scheme, we ensured that our findings accurately reflect the informants' perspectives and are grounded firmly in the data rather than in the researcher bias.

Transferability has been addressed by providing detailed descriptions of the study's context and methodological approach. By documenting the selection criteria of informants and the evolution of the coding process, we enable other researchers to gauge the applicability of our findings to other settings. Our discussion in Chapter 5 further explores how these findings might resonate or diverge in different contexts or with different populations, providing a foundation for external relevance. Dependability, important for demonstrating the reliability of our study over time and across similar conditions (Oates, 2006), was supported by an audit trail. This audit trail details all procedural and methodological decisions, ensuring that our study can be replicated with fidelity. This transparency affords other researchers the ability to trace, verify, and reproduce our research under similar conditions.

3.5 Ethical Considerations

Throughout this study, we have adhered to ethical considerations during all methodological procedures. During the initial recruitment phase, invitations to participate clearly outlined the study's purpose and later on, the specific questions asked. Prior to conducting the interviews, all informants and their respective companies were informed verbally about their rights to withdraw from the study at any time, anonymity, confidentiality, and their right to decline participation without any consequences (Oates, 2006).

Informed consent was obtained from all participants; we interpreted their written agreement to participate in the interviews—following a briefing about the study's scope and procedures—as a consent. This process ensured that all participants were fully aware of the nature of the study and their involvement in it before agreeing to participate. Details on the informant selection process and the specific measures taken to secure informed consent are further discussed in Chapter 3.2.3, Informant Selection. Many of the informants have also expressed a wish to read this thesis when it is finished so that they can gain something from participating in the study, which we have all intentions of granting. We have implemented measures to guarantee that all collected data remains secure and is stored safely (Oates, 2006). Further details on our data storage protocols can be found in Chapter 3.3.2, Data Storing. Additionally, we have diligently cited all sources utilized in this research, giving full credit to the original authors to ensure that this thesis is completely free of plagiarism.

Although no ethical dilemmas arose during this research, we proactively developed strategies to address potential ethical concerns. This preparation included planning for situations where informants might request anonymity or confidentiality. During the member checking process, some informants requested the removal of specific sentences or elements from their interview transcripts. We promptly honored these requests by editing the transcripts accordingly.

Furthermore, to preemptively address any concerns about anonymity, we chose to anonymize all informants in our study. By doing so, we ensured that the identity of each participant was protected, maintaining strict confidentiality throughout the research process.

4 Results

4.1 Theme 1: Frameworks, Standards and Models

4.1.1 Usage of Frameworks, Standards and Models to Influence Security Training Strategy

A focus for several organizations is the adoption of ISO 27001, which illustrates a commitment to a standardized approach towards information security. Informants 1, 2 and 4 all reference ISO 27001, each emphasizing different aspects of its implementation. Informant 1 notes that while the standard mandates training at onboarding and requires current training, it allows flexibility in how training is designed, focusing instead on what the training should cover (I1:7). This flexibility is important as it permits customization according to specific organizational needs, as further exemplified by Informant 1's company's approach to custom-designing training to fit their organizational structure. Contrastingly, Informant 4 provides a more granular perspective on how ISO 27001's specific requirements—such as data handling and password encryption—are integrated into training modules (I4:12).

“It depends. In some cases, if we take ISO security, or ISO 27001, which is the security certification, it sometimes places general requirements such as the company should handle backups correctly or that we should not disclose confidential information to unauthorized persons. But sometimes it also imposes specific requirements on what we can and cannot do, for example, that passwords are encrypted. It can vary, depending on the area, depending on the specific thing it requires.” (I4:12)

This indicates a more prescriptive use of the standard, aligning specific operational procedures with compliance requirements. Furthermore, Informant 4's organization conducts regular audits to ensure adherence to these standards, integrating them deeply into organizational practices and culture (I4:16).

Unlike the structured standard adoption seen in other organizations, Informant 5 discusses compliance with national legislation, specifically the Swedish Security Protection Act, which dictates their operational and data handling strategies (I5:10).

“Then there's also an important aspect to the whole thing. We have legislation. We have a national interest. We have a law called the security protection act that the armed forces comply with. That also regulates how we can conduct our operations, IT operations, how we should store our data. It's an important component in how we design our operation and our training.” (I5:10)

This compliance-driven approach underscores a different facet of framework adoption—where external legal requirements supersede internal choices of frameworks or models. Informant 2 further elaborates on creating an internal security framework tailored to organizational needs, supplementing standard practices with customized guidelines that ensure usability and security coexist effectively (I2:21). This bespoke framework approach, coupled with agreements like the Code of Conduct and Acceptable Use Guidelines, illustrates how organizations can extend beyond standard frameworks to cultivate a security-centric organizational culture.

The delivery and frequency of training also reflect organizational adaptation to these frameworks. Informant 4 mentions utilizing both in-person and digital modalities for delivering training on OWASP and DISA (from MSB), accommodating different learning preferences and operational requirements (I4:19, I4:23).

“Then there are the trainings that we send out digitally, for example, DISA to the employees. And then we have OWASP, which is a training that - I think it was 6 weeks - where it's a proper training that developers should go through. And that one is also digital.” (I4:19)

Moreover, the frequency of training, as discussed by Informant 4 (I4:27), is tailored according to the specific requirements of different training programs, with some needing annual refreshers while others, like certain OWASP training, might be required less frequently. This nuanced approach ensures that training remains effective and relevant to the roles and responsibilities of the employees.

Overall, the responses illustrate a spectrum of approaches to developing cybersecurity training, ranging from highly structured frameworks and standards like ISO 27001 and customized solutions to more fluid, integrated methods that blend regulatory compliance with organizational culture and practical security needs.

4.1.2 Keeping the training content updated

Informants highlight the use of continuous monitoring and external sources to stay abreast of the latest cybersecurity threats and vulnerabilities. Informant 3 and 5 emphasize their reliance on national security bulletins and updates, such as those from MSB (Swedish Civil Contingencies Agency), to inform their organizations about recent vulnerabilities and necessary actions (I3:37, I5:58).

“And then all this about updated systems is also super important, so we have several people who subscribe to the updates that MSB sends out every Friday about discovered cybersecurity threats and incidents, and it also mentions if there have been vulnerabilities discovered in different systems. So it's very good to send out to everyone ‘now you must update this’, but otherwise we always want everything to be updated as soon as possible.” (I3:37)

This proactive approach allows them to quickly integrate critical updates into their training programs and operational practices. Informant 5 expands on this by integrating services like Managed Security Services that include SOC (Security Operations Center) functionalities, enhancing their capacity to respond to incidents and update training materials based on real-time insights (I5:59).

Informant 2 addresses a different aspect of keeping training materials up-to-date by outsourcing this function to a third party, Nimblr. This decision is driven by the recognition that maintaining an in-house team for such updates is resource-intensive and may not keep pace with the rapid evolution of cybersecurity threats (I2:62).

“That’s why we have chosen to outsource this. If we had done this ourselves, we would not have kept up. So Nimblr does it for us.” (I2:62)

Outsourcing allows the organization to leverage specialized expertise and ensures that their training content is continually updated without straining their internal resources. Informant 4 describes a comprehensive internal process involving security officers and audits to identify areas where updates are needed. This process not only catches nonconformities and areas for improvement during audits but also integrates these findings into training updates (I4:43). Informant 1 explains taking a more scheduled approach, using quieter periods in the organizational calendar to update security awareness and onboarding materials (I1:59).

“That’s my responsibility. And it’s about relevance and as time allows. There are endless things to do. We could probably use an entire team working on security. So, it’s a lot about prioritizing. In this case, this year, I will use the summer months when there are fewer things happening in the organization that depend on my help, to adjust both the security awareness and onboarding.” (I1:59)

This approach highlights the challenge of resource allocation for maintaining up-to-date training content and the need for prioritization based on organizational capacity and the criticality of updates.

The varying strategies underscore a fundamental challenge across organizations: balancing the need for up-to-date training with resource constraints and operational priorities. While Informants 3 and 5 utilize real-time updates from national security agencies to keep their training relevant, Informant 2 opts for outsourcing to handle the pace of change effectively. Informant 4 integrates updates directly linked to audit findings, ensuring that training is responsive to identified security gaps. Meanwhile, Informant 1’s approach reflects a more structured, albeit less flexible, schedule for updates.

4.2 Theme 2: Training Methods

4.2.1 Method Types

Informant 2 discusses an advanced application of gamification, where an awareness score is dynamically adjusted based on employees' interactions with simulated phishing attempts and training modules provided by a service called Nimblr. This approach not only engages employees in a continuous learning process but also instills a competitive spirit that encourages better security practices (I2:8, I2:20). Similarly, Informant 1 utilizes a tool called ‘SecureFlag’ to integrate gamification into their training, which involves quiz questions interspersed with video materials to reinforce learning outcomes (I1:26). Both Informant 3 and 2 emphasize the use of simulations and realistic phishing tests to train employees in

recognizing and responding to cybersecurity threats. Informant 3 utilizes Google's phishing quiz and conducts their phishing tests to simulate real attack scenarios, making the training highly relevant and practical for employees (I3:14, I3:21).

"Then we often - but at intervals - mention, have you heard about Google's phishing quiz? It's quite handy. It's a good quiz because it shows how convincing phishing emails can be, so we encourage that. We also recently ran a phishing test on our entire staff, and they know about it - they know there was one, but they don't know there's another one coming this Monday." (I3:14)

Informant 5 also mentions using pen-testing and social engineering as part of their security drills, further highlighting the trend toward realistic and practical training exercises (I5:19).

While embracing modern technologies, organizations also maintain traditional training methods. Informant 4 mentions conducting both digital and instructor-led training sessions, including webinars and technology lunches where case studies are discussed (I4:23, I4:22). This blend of methods caters to different learning preferences and ensures comprehensive coverage of necessary skills and knowledge. Informant 1's approach includes a mix of web-based training that employees can complete at their own pace, alongside more structured sessions like onboarding seminars conducted in auditorium settings (I1:21, I1:20). This flexibility allows employees to engage with the material in a manner that suits their schedules and learning preferences.

"Yes, I see it like this: instructor-led and classroom training might fall somewhat under what I consider our onboarding session. I lead these sessions myself in the auditorium. Then, we also offer web-based training or online training at one's own pace, which might also fit within these sessions. I'm referring to the security awareness training or onboarding sessions. Additionally, we are in the process of developing more webinars, which address more specific topics." (I1:20, I1:21)

Several informants noted the use of external services to streamline and enhance their training offerings. Informant 5, for example, utilizes services like Junglemap for microtraining, which allows for integration with their IT systems and provides tailored security training across various organizational levels (I5:36). This approach is echoed by Informant 2's reliance on Nimblr to manage the continuous delivery of phishing simulations and training content (I2:7).

"We've made it simple for ourselves. There is a Swedish company called Nimblr that has developed an awareness application that sends out phishing attempts and a few other things in our organization." (I2:7)

Across the board, there is a significant emphasis on community engagement and information sharing within organizations. Informants describe various forums and platforms where security issues are discussed regularly, from Yammer groups to all-hands meetings and internal newsletters. This ongoing dialogue helps to keep security at the forefront of organizational culture and ensures that all employees remain aware and informed about best practices and emerging threats (I5:15, I2:9).

The training methods employed by these organizations reflect a sophisticated blend of traditional and innovative approaches. From interactive gamification and realistic simulations to traditional seminars and web-based modules.

4.2.2 Frequency and Length

The frequency and length of cybersecurity training across different organizations reveal a strategic focus on balancing thorough coverage with the need to keep training engaging and manageable for employees. Informant 1 and 4 mention structured, regular training schedules that include mandatory annual refreshers to ensure continuous awareness and compliance among employees. Informant 1 specifies that training groups are organized biannually, with additional yearly refreshers to keep the information fresh without overwhelming employees (I1:12, I1:14, I1:16). Similarly, Informant 4 describes an annual requirement for employees to undergo certain training programs, emphasizing the integration of these sessions into their regular workflow (I4:27).

“So our employees have to go through, for example - they should go through our training, the one we hold. They should go through it when they start at the company and then once a year. So that's the requirement we have. I think OWASP is enough to go through once. And DISA, I'm a bit unsure about, but I think it's once a year. No, I think it's just once. Then it's MSB's basic training. But I think once a year is the standard.” (I4:27)

Contrastingly, Informant 2 highlights a more dynamic approach where training frequency can vary, sometimes occurring multiple times a week depending on the structure of the Nimblr training (I2:18). Informant 5 also supports the idea of regular engagement but opts for short, monthly micro-training sessions that are mandatory yet short enough to maintain high participation rates (I5:29, I5:31).

“The micro-trainings are about 5-10 minutes per training session. We've found that to be the most effective way to get everyone to participate, there's a fairly high risk that if it's a bigger and longer training session people either don't listen or they don't take it in or they don't participate at all.” (I5:31)

Informant 5 and 2 emphasize the effectiveness of microlearning approaches. Informant 5 finds that 5-10 minute training sessions are most effective, allowing employees to engage with the content quickly and effectively without disrupting their daily tasks (I5:31). Similarly, Informant 2 implements brief, focused training segments lasting about 7 minutes each (I2:41). On the other end of the spectrum, Informant 4 mentions a comprehensive OWASP training for developers that spans 6 weeks, illustrating a commitment to deep, extensive learning for roles requiring advanced knowledge (I4:19). Informant 3 integrates flexibility into the training schedule, with annual web-based sessions complemented by continuous information learning spread across various forums within the organization (I3:22, I3:26).

Informant 5 also highlights the importance of accessibility, ensuring that training can be consumed on mobile devices during practical situations, like during short breaks at workstations (I5:33). This approach respects the work environment, integrating training seamlessly into their daily routines.

“Yes and especially that it should be consumable on the mobile or whatever

source one is from. If you're sitting in a loader loading sand out at our sand wash at Ringsjöverket then you maybe do not want to sit down at a computer and do training when you have a coffee break. Then you want to be able to consume it on the fly, bang and it's done. So it's very effective.” (I5:33)

In conclusion, these themes show a strategic focus on making cybersecurity training a regular, engaging, and manageable part of employees’ professional development. Organizations carefully balance the need for comprehensive training with the practicalities of workplace schedules and attention spans.

4.2.3 In-house or External Providers

Informants 4 and 5 describe significant in-house efforts in developing their cybersecurity training programs. Informant 4 mentions that their organization creates its own training, tailored to meet the specific needs of all employees, alongside using widely recognized platforms like OWASP and DISA (I4:8, I4:23). This approach suggests a high level of control over the content, ensuring that it aligns closely with internal policies and employee roles. Similarly, Informant 5 emphasizes the internal development of training materials, supplemented by inputs from external information services (I5:36, I5:37, I5:38).

“Then of course we take in input and information from external parties where we get the information ourselves. We subscribe to a variety of services with information about different security trends, hot trends and so on and that makes us continuously adapt our training, whatever info you go out with. The actual design is what we do ourselves, but then we use external providers just for—the services we use, Junglemap for microtraining, which is a flexible service that can be linked with various reports to Azure. I built an API that we could use. That's mainly what we use. But otherwise, it's a lot that we develop ourselves on our intranet.” (I5:37)

This hybrid approach allows them to design training that is highly specific to their organizational context while staying updated on the latest security trends through subscriptions to services like Junglemap for microtraining.

Contrastingly, Informants 1, 2 and 3 lean more towards leveraging external resources for their training needs. Informant 1 integrates externally produced tools like SecureFlag for specialized training for developers and utilizes open-source platforms like Gophish to enhance their phishing training campaigns (I1:27, I1:29, I1:39).

“SecureFlag is an external provider that offers online-based training specifically for developers. It includes important considerations like VRP management and token handling, among other things.” (I1:27)

This strategy indicates a reliance on external expertise for highly technical content and tools, enriching their in-house developed programs. Informant 2 explicitly states their preference for outsourcing training content to an external provider, Nimblr, which develops awareness applications and manages the delivery of phishing simulations. This decision is driven by the challenge of keeping pace with the dynamic nature of cybersecurity threats and the need for specialized, continuously updated content (I2:14, I2:37, I2:62). Informant 3 also points to a combination of in-house content development and external production support. Their training

is internally developed within their corporate group but relies on professional production companies to create the actual training materials (I3:8, I3:31). This approach suggests a balance between maintaining internal control over the training content and utilizing external expertise for high-quality production.

“I’m quite sure it’s the group that has developed the content themselves. Then they have had help from a production company to create the actual training, but the content itself is internal.” (I3:31)

In summary, these approaches highlight a spectrum of strategies from full outsourcing to entirely in-house development, with many organizations opting for a hybrid approach.

4.3 Theme 3: Organizational Culture

4.3.1 Fostering a Cybersecurity Culture

Across all informants, a recurring theme is the significant role of leadership in promoting cybersecurity. For instance, Informant 4 emphasizes the role of management in certifying processes like ISO 27001 and ensuring these standards are communicated and adhered to throughout the organization (I4:41). Similarly, Informant 5 details how leadership participation in management teams helps disseminate a security-first mindset throughout the organization (I5:54). This involvement ensures that cybersecurity is not just an IT issue but a central component of organization operations, supported and advocated by top management.

A strong cultural foundation that supports learning from mistakes and openly discussing cybersecurity is another key strategy. Several informants emphasize the importance of maintaining an open environment where employees feel safe to report security incidents without fear of retribution. Informant 1 discusses the significance of removing guilt and embarrassment associated with cybersecurity mistakes to encourage quick and honest reporting, which can lead to more effective learning (I1:35).

“It’s crucial that we never use this to single out people but rather to strengthen them. The goal is obviously that no one clicks on a malicious link, but it happens, so removing the guilt or embarrassment if someone does helps them feel safe reporting it to IT. Just recently, someone admitted to clicking such a link, and we were able to handle it safely by checking the link through a virtual machine, a sandbox, rather than having to reset their entire computer. We just needed to change their password. It’s more about being honest quickly, which can be a more effective learning moment than if the scenario were real.” (I1:35)

Informant 3 highlights how their organization encourages a culture of openness and continuous learning, where mistakes are used as learning opportunities rather than sources of blame (I3:42, I3:45).

“We help each other out, we give tips to each other, share information and news, and we have a very strong culture of being open, that it’s okay to make mistakes, so there’s no shame in accidentally clicking on a link, the important

thing is that it's okay if you do, but the important thing is that you report it so that we can actually handle it.” (I3:42)

This approach helps to demystify cybersecurity, making it a more integral and less intimidating part of everyday work life. Informant 5 also talks about using positive reinforcement and direct coaching to foster a security-aware culture. By encouraging and rewarding correct security behaviors, the organization reinforces the importance of security and ensures that good practices are recognized and emulated (I5:28).

Informants detail both organic structured approaches to knowledge sharing within their organizations. Informant 3 describes how knowledge sharing among developers has emerged organically, supported but not mandated by management, which has led to a more robust cybersecurity knowledge base within that team (I3:34). This grassroots level of security awareness contributes to a deeper, more sustainable organizational culture of security. Conversely, Informant 2 and 5 discuss more structured approaches, with Informant 2 developing a security framework and guidelines to standardize practices across the organization (I2:21). Informant 5 emphasizes the role of ongoing training and technical measures to guide employees towards secure behaviors automatically (I5:7).

“The strategy is still to try to incorporate training elements and information into our daily routine so to say. It should be a natural part of our operation. You should have a security mindset not only in production parts but also when working with IT tools, so it's a lot about raising awareness of external threats, creating awareness, being present, and talking to the employees to continually plant this seed.” (I5:7)

All informants agree on the necessity of integrating cybersecurity into daily routines and operational practices. Informant 1, for example, speaks to the integration of security practices through awareness campaigns and training that are part of regular internal communications (I1:47). Similarly, Informant 4 uses regular internal audits, training sessions, and simulated phishing attacks to keep security top of mind for all employees (I4:17).

Several informants mention embedding cybersecurity within the core values of the organization. Informant 4 and 1 both discuss how security is intertwined with organizational values like trust, expertise, and customer service, ensuring that it remains a priority across all business functions (I4:39, I1:51). Informant 5's strategy of identifying ambassadors within different parts of the organization to spread security awareness highlights a decentralized approach to fostering a security culture. This method helps in tailoring the security message to different operational contexts, making it more relevant and actionable for various departments (I5:45).

4.3.2 Challenges

The challenges of cultivating a robust cybersecurity organizational culture, as shared by the informants, underscore the tension between operational priorities, cultural adaptation to security practices, and generational differences in digital fluency. Informant 5 highlights the primary challenge of integrating cybersecurity training into a production-oriented and solution-focused operation. There's a natural tension between the immediate goals of production efficiency and the longer-term, often more abstract, goals of cybersecurity (I5:6).

“The difficulty with conducting this type of training, first of all, there is no real tradition of these kinds of issues, the operation is very production-oriented and very solution-oriented. A solution-oriented operation and security, they don't always mesh very well.” (I5:6)

This dichotomy can lead to resistance when attempting to implement comprehensive security measures that are perceived as slowing down or complicating production processes. The idea of implementing an “IT license”, as suggested by Informant 5, that needs regular renewal to work within an IT environment showcases an innovative approach to ensuring ongoing cybersecurity competence. However, such measures are seen as too time-consuming and invasive, reflecting a broader reluctance to adopt practices that are perceived to interfere with the core activities of the organization (I5:31). This resistance is indicative of a broader challenge where security practices must be balanced against operational efficiency and cultural acceptance.

Informant 2 discusses the challenge of digital maturity, particularly the transition from a personal to a professional digital environment where security needs are significantly more stringent (I2:25). Younger employees, accustomed to a more open and interconnected digital life through platforms like Snapchat and WhatsApp, often find it difficult to adapt to the restrictive nature of corporate IT environments. This generational gap in expectations about digital behavior poses a challenge in fostering a security-aware culture. Another challenge mentioned by Informant 2 is the resistance at higher levels of the organization, especially among older executives who may be less adaptable to changes in digital practices (I2:60).

“That's the hardest, I would say. If I go to my CEO and say that now I will take command over your iPhone, he will go completely crazy. To have Mobile Device Management, which is A and O to be fully safe, then you cannot run Apple at all. Then you have to go the Android way because there you can have dual profiles. A corporate profile and a private profile. So that's a journey that's always the hardest. The higher up you go, the harder it is, I would say. It's often people who are a bit older. And they have a change readiness like your grandfather.” (I2:60)

This resistance is not just about personal inconvenience but also reflects broader issues of control over personal devices and data privacy, which are crucial in the context of Mobile Device Management systems.

4.3.3 Training Tailored to Different Employee Groups or Individuals

Each informant discusses how they segment training based on role-specific needs, organizational structure, and the individual's level of expertise, highlighting both the advantages and challenges of creating customized cybersecurity training programs.

Informant 4 outlines a clear strategy for segmenting cybersecurity training, with specialized content such as OWASP targeted specifically at developers. This specialization ensures that the training is relevant and practical for those who need it most, enhancing its effectiveness by addressing role-specific risks and responsibilities (I4:7). Conversely, general security training like DISA is aimed at all employees, underscoring the universal aspects of cybersecurity awareness needed across the company. Informant 1 also mentions role-based customization,

with specific sessions designed for expert services and developers, indicating an ongoing effort to potentially expand this specialized training to other departments (I1:32).

“One could say that both the onboarding training and the awareness training are quite general and therefore relevant to everyone within the organization. Naturally, some will benefit from it more than others, depending on their roles. The training that is more specific or customized, for example, includes a separate session for what we call our expert services, our consultants. SecureFlag is specifically for developers. It’s not out of the question that we might develop similar sessions for other departments over time.” (I1:32)

Informant 2 discusses how training is customized not only content-wise but also in its deployment, with certain training components like management-focused modules that cater specifically to leadership roles (I2:31).

In contrast to the tailored approach, Informant 5 discusses the challenges of creating specialized training for different groups within the organization, such as production staff versus office workers. They highlight the importance of setting the training at a level accessible to the least IT-knowledgeable employees, ensuring that everyone has a baseline understanding of cybersecurity (I5:40).

“It’s a bit like that, we’re a bit divided as I talked about before, the production-close—we can call it a bit like ‘the blue collars’, more staff who primarily don’t sit in front of a computer when they work. Then we have then ‘white collars’ at the head office. We actually don’t make any distinction between people, but we do try to tailor it to the least interested, least IT-knowledgeable target group. We set it at such a level that everyone can benefit from it.” (I5:40)

This approach acknowledges the practical limitations of overly specialized training in a diverse workforce. Both Informant 5 and 3 discuss the importance of adaptability in their training programs. Informant 5 points out that while they aim to engage everyone from production staff to office workers, the actual delivery and technical depth of the training must be adjusted on individual capabilities and roles within the organization (I5:42, I5:44). Informant 3 also mentions the variability in discussion levels and types among different groups, suggesting a flexible approach to communication and education about cybersecurity across the company (I3:33).

In summary, while some organizations adopt a broad approach that standardizes cybersecurity training across all employee groups, others implement targeted strategies to address the specific needs of different roles or departments.

4.3.4 Remote Working

Informant 1 and 4 emphasize the importance of maintaining consistent security protocols, regardless of the employee’s location. Informant 1 notes that their security measures are client-based, ensuring that the security level remains constant whether employees are working from an office or remotely. This approach is supported by advising employees on secure practices while traveling, such as avoiding shoulder surfing and always locking devices (I1:41).

“No, without going too deep, our security is client-based, it shouldn’t matter where you are working from. Of course, we advise on how to think when traveling, that you should always lock your computer and not sit where someone might shoulder surf you, but we assume the same level of security on the device whether you are on our network or at an airport. We prefer that consultants connect through their mobile devices when they can, when traveling.” (I1:41)

Similarly, Informant 4 mentions that their company does not differentiate between remote and on-site work in terms of security protocols, indicating an organizational culture that supports flexibility with a consistent security posture (I4:33). Contrastingly, Informant 5 discusses the existence of specific guidelines tailored to remote work, which dictate what employees can and cannot do when working remotely. These guidelines aim to narrow down the technical possibilities and limitations for remote workers, ensuring they operate within a secure framework (I5:47).

Informant 3 and 2 highlight the use of technology to mitigate the risks associated with remote work. Informant 3 mentions the use of clients’ VPNs for secure connections to necessary systems and the avoidance of public networks, which are deemed insecure. The advice to use privacy screens when working in public places further underscores the emphasis on maintaining confidentiality and integrity of data outside the office (I3:36). Similarly, Informant 2’s approach is rooted in a Zero Trust strategy, advising against the use of unsecured public Wi-Fi networks at airports and cafes and recommending the use of mobile phones as modems to ensure secure connections (I2:50).

“That’s where our Zero Trust strategy comes into this. We want to let everyone be wherever they happen to be at the moment. The only thing we’ve said that we can’t really control is do not connect to airports and cafés wifi. Because if there’s anywhere shit happens, it’s there. Instead, use your mobile phone as a modem if you need to work in such a place where you’re not on a controlled wifi.” (I2:50)

4.3.5 Social Media

The strategies for managing social media usage within the organization, as discussed by the informants, reflect varying degrees of formalization and enforcement. These strategies can range from general guidelines and non-disclosure agreements to outright prohibition of social media usage for business purposes. Informant 4 describes a situation where the company has a guideline that advises employees not to disclose sensitive information on social media but lacks formal monitoring or specific training related to social media usage (I4:35).

“We have - the only thing I’ve seen is a guideline on how we handle social media. And it basically says not to disclose information that you’re not supposed to disclose. We don’t have any monitoring - my company doesn’t keep track of what I do on social media, I know some companies do. ” (I4:35)

This approach relies on employee discretion and managerial oversight in case of violations, suggesting a reliance on existing organizational norms and the professional judgment of employees. Informant 5 also notes the absence of specific strategies targeting social media

use, indicating that such policies are encompassed within broader IT guidelines that restrict the use of work accounts for personal activities, like signing up for social media (I5:49). This approach focuses on preventing potential breaches by limiting the use of organizational resources in personal contexts.

Informant 1 highlights that while employees are expected to adhere to non-disclosure agreements (NDAs) that cover all forms of communication, including social media, there is no active interference in employees' private social media activities (I1:43, I1:45). This suggests a trust-based approach where employees are trusted to manage their social media interactions responsibly, under the umbrella of contractual obligations.

Contrasting with the more open policies described, Informant 2 discusses a much stricter strategy where social media usage is essentially forbidden for general staff, with only three controlled accounts managed by the marketing department (I2:52).

“Generally, we have forbidden social media. We have three controlled accounts run by our marketing department. One on Instagram, one on Facebook, and one on LinkedIn. Otherwise, we do not use it in the company. Typically, we use Teams chat to chase each other. We call each other over Teams, we call each other over regular 4G. That's how we do it. And it's to have control over the dialogue. And the data that is exchanged.” (I2:52)

This approach reflects a tightly controlled communication strategy designed to minimize risks associated with unregulated social media use. Teams and other controlled communication channels are emphasized to ensure that all work-related communications are secure and monitored.

While some companies opt for a more trust-based approach that emphasizes individual responsibility within the guidelines of NDAs and IT policies, others implement stringent controls to minimize potential risks associated with social media interactions.

5 Discussion

5.1 Key Findings and Interpretation of Results

5.1.1 Frameworks, Standards, and Models

The study revealed a diverse application of frameworks, standards, and models across organizations to shape and enhance cybersecurity training strategies. Key findings include:

1. **Adoption of Specific Frameworks:** Organizations employ a variety of frameworks, standards and models to guide their cybersecurity training strategies, with ISO 27001 being notably prevalent. However, informants indicate that these frameworks do not directly shape the content or methods of security training; they simply mandate that training should occur. While frameworks like ISO 27001 influence the general security practices, such as backup management and password encryption, they do not specify training approaches. Additionally, some organizations adhere to national legislations like the Security Protection Act, which prescribes specific data handling and operational protocols but also does not dictate how training should be structured, merely that it must be conducted. This highlights that while international standards and local regulations require the implementation of training, they leave the specifics of training content and methodology to the discretion of the organization.
2. **Maintaining Training Relevance:** To ensure training remains current with the rapidly evolving cybersecurity landscape, organizations adopt multiple strategies for updating their training content. Regular monitoring of cybersecurity threats and updates, notably from national security agencies like MSB, plays an important role. This proactive approach is complemented by outsourcing update responsibilities to third-party services such as Nimblr, which helps organizations keep pace with new threats without overburdening internal resources. Additionally, internal audits and the strategic scheduling of updates during quieter operational periods help integrate the latest security practices into training programs.

This analysis seeks to compare the literature from Chapter 2, Literature Review, and the results shown from the conducted interviews. The literature robustly positions frameworks as pivotal for integrating security awareness training into organizational cybersecurity efforts (Corradini, 2020; Culot, 2019; McIntosh et al., 2024). However, this study shows that while frameworks like ISO 27001 are commonly used as starting points, they do not dictate how the training should be conducted. These frameworks generally require the inclusion of security training but do not specify how it should be implemented. This is contrasted by the more specific guidelines provided by the DISA framework from the Swedish Civil Contingencies Agency and the OWASP guidelines, which offer clearer directions for training.

While the literature highlights the significant use and impact of standards like ISO/IEC 27001 and the NIST cybersecurity framework (Culot, 2019), the findings tell a different story. None of the interviewed companies used the NIST framework, indicating a gap between the literature's perception of these frameworks' popularity and their actual use. However, it's possible that the finding is merely coincidental, reflecting that the specific companies interviewed for this study did not use the NIST framework. The literature also suggests a variety of alternative frameworks that are tailored to specific company needs or designed to tackle particular challenges (Belalcázar et al., 2017; Corradini, 2020; Hijji & Alam, 2022; Tsiodra et al., 2023). However, the findings reveal that it is quite rare for companies to use frameworks other than ISO, suggesting a lack of adoption of these niche frameworks in practice.

Ben Salamah et al. (2024) points out that the generic nature of many cybersecurity frameworks can make them difficult to adapt to specific needs, such as managing social media risks. In contrast, the companies we interviewed did not report this as an issue. They manage social media risks through policies that either restrict use or rely on employees' judgment, suggesting that the practical challenges of applying these frameworks might be less significant than the literature suggests. The literature also mentions that standard training frameworks often overlook individual learning styles, which can make training seem overwhelming or uninviting (Ben Salamah et al., 2024). The results showed that companies recognize these issues and respond by implementing micro-training sessions that help build a cybersecurity-positive culture. This approach shows that companies are moving towards training methods that better fit their culture and the needs of the employees. Moreover, the importance of tailoring training to individual needs is emphasized (Ben Salamah et al., 2023). Our findings show varied practices among companies: some aim for consistency but keep track of individual awareness scores, while others provide targeted training for specific groups. Some companies mentioned that limited resources prevent them from offering fully personalized training.

Finally, the literature by Djebbar & Nordström (2023) discusses the difficulty of choosing the most suitable frameworks due to the many available options and their overlapping features. However, this issue was not highlighted by the companies we interviewed, which may indicate that the interview questions did not fully capture this challenge. In summary, while the literature emphasizes the crucial role of frameworks in designing security training, real-world practices suggest that frameworks often function more as compliance checklists than as detailed guides for developing effective training. This analysis underscores the need for more research to close these gaps and to enhance frameworks that can truly guide organizations in creating customized and effective cybersecurity training programs.

5.1.2 Training Methods

The study revealed a diversity in training method types, frequency, length, and choice between in-house or external providers. Key findings include:

1. **Diversity in Training Method Types:** Organizations are employing a mix of innovative and traditional training methods to enhance cybersecurity awareness and skills, with many of them being online. Methods include gamification, with tools like Nimblr dynamically adjusting awareness scores, and SecureFlag integrating quiz questions within video materials for interactive learning. Realistic simulations and phishing tests are prominently used to train employees to recognize and respond to

cybersecurity threats, ensuring that training is practical and applicable to real-world scenarios. Traditional and technology-driven methods, such as instructor-led sessions and web-based modules, continue to be fundamental.

2. **Frequency and Length of Training:** The frequency and length of training sessions are strategically designed to balance thorough coverage with employee engagement and manageability. Regular training schedules are common, with mandatory annual refreshers to maintain continual awareness and compliance. Some organizations adopt a more dynamic scheduling approach, with training frequencies varying to include multiple sessions weekly depending on specific program requirements. Micro-training sessions, often lasting between 6 to 10 minutes, are used to ensure high participation rates without overwhelming employees.
3. **Choice Between In-house and External Providers:** There is a significant variation in the sourcing of cybersecurity training content. Some organizations develop their training internally to tailor content specifically to their needs and integrate it deeply with internal policies and cultural practices. For example, some use in-house developed materials supplemented by external information services to stay current with the latest security trends. Conversely, other organizations leverage external providers to enhance their training offerings. This includes outsourcing the development and management of training programs to specialists who provide up-to-date, technically sophisticated content. The use of external services like Nimblr for phishing simulations and Junglemap for microtraining allows organizations to benefit from advanced technologies and methodologies without the internal resource burden.

This analysis aims to detail the differences between the expectations set by literature and the practical implementations observed through direct feedback from companies.

Literature underscores the increasing sophistication of attackers and the resultant need for security training to encompass more than just technical components, asserting that human error is a predominant factor in cybersecurity breaches (Giriraj et al., 2022). Our findings align with this perspective, as all interviewed companies have some form of security awareness training targeting employee behaviors, not just IT skills. Even non-IT oriented companies, such as those in manufacturing, have dedicated IT security teams and training programs, indicating a broad recognition of the role human error plays in security breaches. The companies also acknowledge the prevalence of mistakes and adopt a supportive approach to errors, encouraging employees to view them as learning opportunities. This approach is integral to fostering an organizational culture that prioritizes security as a collective responsibility, which will be further discussed in the section on organizational culture (Chapter 5.1.3).

The literature also advocates for cybersecurity training that is tailored to fit the diverse roles within an organization, suggesting that training should be customized to the specific needs of different employee groups to be most effective (Ben Salamah et al., 2023; Flores et al., 2023). While companies in our study are indeed tailoring their training—especially for developers and upper management—others, particularly production-focused ones, prioritize operational efficiency over customized training. This highlights a practical constraint that may sometimes limit the implementation of ideal training strategies as suggested by the literature. Addressing the impact of social media, Evans (2022) notes that many companies underestimate the risks, with less than 50% having dedicated policies. Our findings reflect this gap; no interviewed

company mentioned specific training for social media use. However, one company has completely prohibited social media usage at work, indirectly mitigating potential risks.

In terms of training methods, literature highlights the importance of diverse approaches, from traditional instructor-led sessions to more innovative, tech-driven strategies (Corradini, 2020). Our findings reveal that while traditional methods are still employed, the predominant methods are interactive and experiential, often incorporating online elements. Coaching and mentoring, particularly with positive reinforcement, are valued for their informal yet impactful learning outcomes.

The literature underscores the importance of advanced digital technologies in transforming cybersecurity training. Notably Adams et al. (2015) discuss the Attacker-Centric Gamified Approach, which allows participants to role-play as cyber attackers to gain a deep understanding of defensive tactics. Corradini (2020) expands on this by mentioning dynamic and engaging training methods like case studies, role-playing, gamification, and simulation. Reflecting these advanced training methodologies, our findings reveal that many companies are actively incorporating these interactive and experiential approaches through various external platforms. SecureFlag, for example, is a platform that provides hands-on simulations and attacker-centric gamification tailored to a diverse range of employee roles. This method not only allows employees to understand the mindset of attackers but also helps them practice their response strategies in a controlled, high-impact environment. Nimblr specializes in micro-training, which focuses on delivering short, concentrated training sessions that include simulations such as phishing attacks and gamified learning experiences. This approach is particularly effective in maintaining high levels of engagement and ensuring that training is both manageable and integrated seamlessly into the daily routines of employees. Junglemap, another micro-training platform, also emphasizes phishing attack simulations, addressing one of the most prevalent and successful types of cyber threats today. By routinely exposing employees to these simulated attacks, companies enhance their staff's ability to recognize and deflect actual phishing attempts. Additionally, some companies opt to develop their phishing simulation campaigns using tools like Gophish. This allows organizations to tailor their training exercises more closely to their specific security co

However, while literature points to the benefits of tabletop exercises for collaborative problem-solving in simulated environments (Angafor et al., 2020), our findings indicate that such exercises are not commonly mentioned among the training methods used by the interviewed companies. This could suggest a gap in the adoption of certain simulation-based training methods. Finally, the integration of technology in training, particularly through video-based and virtual or augmented reality sessions, is touted as making learning more engaging and realistic (Qawasmeh et al., 2024). Our findings validate this, with all companies mentioning the use of technology-based training modalities, including web-based training and webinars, which are developed both internally and sourced externally.

In summary, while literature presents an idealized vision of comprehensive, tailored, and technologically advanced cybersecurity training, the actual practices in companies reflect a mix of adherence to these principles and pragmatic adaptations based on operational constraints and available resources. This analysis underscores the ongoing need to bridge the gap between theoretical best practices and the realities of implementing effective cybersecurity training in diverse organizational environments.

5.1.3 Organizational Culture

The study revealed how organizations approach the development and maintenance of a security-conscious organizational culture. Key findings include:

1. **Fostering a Cybersecurity Culture:** Leadership plays a pivotal role in cultivating a cybersecurity culture, with top management actively participating in promoting security practices throughout many of the organizations. Organizations encourage an open environment where mistakes are utilized as learning opportunities rather than penalized. This strategy removes the stigma associated with reporting security incidents, thereby enhancing the overall security posture.
2. **Challenges in Cultivating Cybersecurity Culture:** A challenge is balancing operational efficiency with the implementation of effective cybersecurity measures, particularly in production-oriented environments where security measures might be seen as impediments. Generational differences in digital fluency and resistance at higher organizational levels, particularly with adapting to new security practices and technologies, pose additional challenges.
3. **Training Tailored to Different Employee Groups:** Cybersecurity training is customized to address the specific roles and responsibilities within the organization, with distinct programs like OWASP for developers and general security awareness for all employees. Despite efforts to customize training, ensuring accessibility and relevance across a diverse workforce remains a complex task, with organizations striving to cater to the least IT-knowledgeable employees.
4. **Remote Working:** Security protocols are designed to be consistent regardless of an employee's location, with additional guidelines provided for secure practices while working remotely. This includes the use of VPNs and advice against using unsecured public Wi-Fi, ensuring that employees maintain the same level of security when outside the office.
5. **Social Media:** Strategies for managing social media use vary, ranging from general guidelines and non-disclosure agreements to more stringent prohibitions. The approach taken typically reflects the organization's broader communications and data security strategies, with some relying on professional judgment and other imposing strict controls.

This analysis seeks to juxtapose these discrepancies and offer insights on the actual practices and perceptions within organizations.

The scholarly consensus highlights that merely transferring knowledge about good security practices isn't enough; behavioral strategies are crucial for fostering positive cybersecurity habits within an organization (Bada et al., 2019). Moreover, these sources argue that training alone is insufficient to counter the rising cyber threats (Bada et al., 2019; Corradini, 2020; Daengsi et al., 2021; El-Bably, 2021; Greulich et al., 2024; Vasudevan et al., 2023). From the findings of this study, it appears that although most companies lack a specific strategy for creating a cybersecurity organizational culture, they still implement various approaches to shape security-focused behaviors among employees. Notably, while training does not specifically address issues like social media use and remote working, companies have established cultural norms and guidelines for these behaviors, such as advising against the use of unfamiliar WiFis and caution about shoulder-surfing in public. One company has even prohibited social media use at work, demonstrating a proactive approach to risk mitigation.

Research also emphasizes the need for leadership to actively promote and engage in training as a means of setting a company-wide example for cybersecurity (Corradini, 2020). The data collected indicate strong support for cybersecurity from top management across all interviewed companies. However, some challenges, such as generational differences in adapting to new security practices, persist, with older management members often showing resistance to change. Additionally, literature advocates for specialized training programs tailored to the unique needs of various departments, recognizing the diversity in knowledge levels and training requirements within an organization (Daengsi et al., 2021). Responses from companies vary, with some providing highly targeted training designed for specific departments or employee groups, while others adopt a more generalized approach.

On another note, scholars propose that fostering a positive workplace and continuously educating employees on cybersecurity can significantly boost compliance with security protocols. It is crucial to promote trust and awareness, thereby encouraging active participation in security measures (Greulich et al., 2024). The feedback from companies underscores the importance of building trust within the organization. There is a strong emphasis on openness, with a culture that encourages employees to report security mistakes as opportunities for learning rather than reasons for punishment. Nevertheless, there are differing views on the role of leadership enforcing security, with some companies supporting the idea that leaders should have the authority to reprimand employees who make security errors. Others advocate for positive reinforcement to foster a constructive workplace and enhance cybersecurity education.

Finally, it is recognized that organizational culture in cybersecurity involves both overt aspects, such as technology use, and more nuanced elements, like values and deep-seated beliefs that define an organization's core identity (Corradini, 2020). This study's findings show that although cybersecurity is not explicitly listed among the core values of the interviewed companies, many of their core principles, such as simplicity and openness, inherently support a security-focused organizational culture. This alignment helps improve security awareness and behavior across the board, underlining the importance of integrating cybersecurity strategies with the broader organizational ethos.

5.1.4 Synthesis of Findings

The synthesis of findings across the themes of frameworks, training methods, and organizational culture reveals a comprehensive view of the strategies companies currently use to enhance cybersecurity awareness among employees. This analysis ties together the diverse applications and practices observed, highlighting both adherence to theoretical recommendations and practical adaptations.

Organizations apply various frameworks like ISO 27001 to shape cybersecurity training strategies, providing flexibility without stringent specifications on execution, serving more as benchmarks or compliance requirements. Companies adopt a mix of traditional and innovative training methods such as gamification, simulations, and micro-training to make cybersecurity awareness practical and integral to daily routines, catering to diverse learning preferences. Simultaneously, a strong organizational culture led by committed leadership promotes cybersecurity awareness, creating an open environment where mistakes are learning opportunities, enhancing security posture and compliance, and often leveraging core values like openness and simplicity to support a security-focused culture.

Integrating these findings, it becomes clear that while companies are guided by the frameworks available, they tailor their training methods and cultural approaches based on specific organizational needs and challenges. This flexibility is crucial in addressing the dynamic nature of cybersecurity threats. The reliance on a mix of prescribed frameworks and innovative training solutions allows companies to maintain relevance and efficacy in their cybersecurity training programs. Ultimately, the findings indicate that companies are employing a multifaceted approach that incorporates diverse training methods, maintains training relevance, and fosters a conducive cybersecurity culture.

5.2 Limitations

Despite our efforts to conduct a comprehensive literature review, the scope was inevitably limited by time constraints, preventing an exhaustive exploration of all existing literature. While a large body of work was included to underpin the research, a more extensive review could have potentially enriched the findings by incorporating additional sources and databases (Jacobsen, 2024).

The data collection process in this study, involving interviews with five informants from various industries, faced limitations due to the small sample size. Despite the diversity in industries, the limited number of participants might restrict the generalizability of the findings and may introduce bias, as it might not fully capture the breadth of practices and perspectives in cybersecurity training across different organizational contexts (Oates, 2006). Additionally, the interview structure, based on a predefined framework focusing on frameworks, training methods, and organizational culture, might have led informants to tailor their responses to these themes. This could overshadow other vital aspects of cybersecurity training strategies. This issue was compounded by a lack of probing in the interviews; the structured nature of the questioning process limited the ability to delve deeper into unexpected or nuanced areas that could emerge during a more open-ended discussion (Oates, 2006).

The data analysis phase of this study encountered challenges that could impact the dependability and interpretation of the findings. One of the primary issues was the inconsistency in the coding process. Due to the overlapping themes, coding was not always consistently applied. For instance, initial coding captured every mention of the framework ISO 27001 by informants, but this approach was later adjusted to code only the first mention. This shift in strategy led to inconsistencies, evidenced by an 81% intercoder agreement (Cheung & Tai, 2023), indicating some discrepancy between the researchers' coding decisions. Such inconsistencies, compounded by overlapping code definitions, can lead to errors in interpreting and presenting findings, as suggested by Oates (2006), who recommends creating distinct, non-overlapping themes to enhance coding clarity.

Furthermore, the methods used for transcriptions varied across interviews, which may have affected the data's uniformity and subsequent analysis. Some interviews were transcribed using WhisperAI, others with MAXQDA, and some manually via Google Docs. Additionally, while investigator triangulation was performed (Oates, 2006), the limitations in execution, such as both researchers not independently segmenting the transcriptions, may have restricted the depth of this consistency check. More comprehensive independent analysis by each researcher could have provided a stronger validation of the coding consistency and revealed additional insights (Cheung & Tai, 2023).

Regarding transferability, the study's findings offer relevant insights that could be applicable to other settings, populations, or contexts, despite the limitations imposed by the sample size. As Oates (2006) suggests, the ability to apply findings broadly depends significantly on the clarity with which researchers describe their research setting and participants. In this study, effort was dedicated to detailing the study's methodology and the characteristics of the participant sample, which consisted of typical companies that implement security training. This thorough description aids other researchers in assessing the extent to which the findings can be generalized to similar contexts (Oates, 2006). Although the sample may not present the entire general population, the selected participants reflect typical scenarios within the field of cybersecurity training, enhancing the potential for broader applicability.

Ethical considerations were prioritized and carefully integrated throughout the duration of this study to ensure that the research adhered to the highest standards of academic integrity and respect for participants. Although a formal written consent form was not used, efforts were made to secure informed consent through other means. In retrospect, the creation of a formal written consent form would have been beneficial. It would have provided a clear record of consent and helped reinforce the transparency and professionalism of the research process. Going forward, it is recommended that future studies incorporate this practice to further enhance ethical safeguards and participant protection (Oates, 2006).

5.3 Suggestions for Future Research

Discussing the limitations identified in this thesis, future research on cybersecurity could benefit significantly by extending the literature review's scope and duration, incorporating a more diverse and larger sample size, and adopting a less structured interview format to deepen data collection. Standardizing transcription methods and ensuring consistent coding procedures, along with implementing independent coding and investigator triangulation, would enhance the dependability of data analysis. Additionally, adopting formal written consent forms would increase research transparency and bolster participant protection.

We also suggest that future research should transition towards an explanatory rather than merely descriptive study. This could involve assessing the effectiveness of cybersecurity training strategies, in addition to describing them. An investigative approach could also be adopted to explore why companies choose specific frameworks or training methods. Employing mixed methods to combine quantitative measures of training effectiveness with qualitative insights from detailed interviews or case studies would provide a richer understanding of the factors influencing cybersecurity training decisions and their impacts.

Lastly, replicating this study would be beneficial to verify its credibility and confirmability. Conducting replications in varied settings or with a broader participant pool would yield insights into the consistency of the findings across different contexts and could illuminate whether different variables or conditions affect the outcomes. This would help to strengthen the evidence base and refine the theoretical contributions of the study.

6 Conclusion

The purpose of this study was to identify and describe cybersecurity training strategies that are aimed to enhance awareness among the workforce within companies. By conducting a descriptive qualitative study using individual interviews, we have been able to answer the research question, “What training strategies are companies currently using to enhance cybersecurity awareness among employees?” The results from our study highlights a multifaceted approach employed by organizations.

Organizations utilize a diverse range of frameworks, standards and models to guide their cybersecurity training, with ISO 27001 being notably prevalent. These frameworks are applied in various ways, from dictating general security practices such as backup management to enforcing stringent requirements like encryption of passwords. Additionally, adherence to national legislation like the Security Protection Act underscores the role of both international standards and local regulations in shaping training frameworks. Although frameworks extensively dictate the technological aspects of cybersecurity within companies and mandate the implementation of cybersecurity awareness training, they appear to have little influence on the specific training methods employed.

Our findings reveal that organizations employ a blend of innovative and traditional training methods, many of which are online. These include gamification, realistic simulations, instructor-led sessions, and web-based modules. The diversity in training method types, frequency, length, and choice between in-house or external providers helps ensure that training is practical, engaging, and tailored to real-world scenarios. Regular training schedules with mandatory annual refreshers are common, alongside micro-training sessions, to maintain high participation rates without overwhelming employees.

A significant aspect of cybersecurity training strategies involves fostering a security-conscious organizational culture. Our findings underscore the notable role of leadership in fostering a proactive cybersecurity culture. Companies cultivate an environment where employees are encouraged to learn from their mistakes, with a strong emphasis on communication and the non-penalization of errors. Training is often tailored to different employee groups to ensure relevance and accessibility, with special protocols in place for remote working to maintain security consistency regardless of location.

In conclusion, companies are currently leveraging mostly the ISO 27001 framework, diverse training methods, and cultural initiatives to enhance cybersecurity awareness among employees. These strategies are intricately designed to be current, practical, and inclusive, effectively preparing employees to tackle cybersecurity challenges.

Appendix A - Interview Guide

Introduction:

- Explain the purpose of the interview.
- Ask for permission to record the conversation.
- Inform the participant about their right to confidentiality and anonymity.
- Take the full name and note the role/expertise the participant has in the company.

Questions:

1. Do you follow a specific framework, model, or standard when developing your cybersecurity training programs? If yes, could you tell us more about it?
2. In what ways does this framework, model, or standard influence the design and implementation of your cybersecurity training?
3. Do you use a single training method, or do you use a combination of several methods?
4. What types of training do you conduct to increase cybersecurity awareness among your employees?
5. Please indicate the training methods you use from the following list:
 - Instructor-led
 - Classroom
 - Seminars
 - Case study
 - Role-playing
 - Gamification
 - Simulation
 - Web-based training
 - Self-paced online training
 - Online instructor-led training
 - Webinars
 - Coaching
 - Mentorship
 - Informal learning
 - A combination of various training methods
6. How often must employees undergo training?
7. What is the typical length of the training sessions?
8. Do you develop your cybersecurity awareness training materials internally, or do you use external providers? Can you share which one?
9. If you use external providers, can you share which service or product is used?
10. Is the cybersecurity training customized to meet the diverse needs of different staff groups within your organization? If yes, please describe how.

11. Do you use specific training strategies for employees who work remotely? If yes, please describe what.
12. Are there specific strategies in place to increase cybersecurity awareness regarding risks in employees' use of social media? If yes, can you tell us more about it?
13. What strategies are in place to promote a culture of cybersecurity awareness within your organization?
14. How is awareness about cybersecurity integrated into your organization's core values?
15. What measures are in place to ensure that leadership and management actively promote a culture of cybersecurity?
16. How do you ensure that training content is continuously updated and remains relevant with the latest developments in cybersecurity practices and emerging threats?

Ending:

- Ask the participant if they have any questions for us or their own thoughts.

Appendix B - Codebook

Table B1: Main coding categories with their corresponding abbreviation

Main Category	Code Abbreviation
Frameworks, Standards and Models	FSM
Training Methods	TM
Organizational Culture	OC
Informant Background	IB

Table B2: Coding categories with their corresponding abbreviations, definitions, as well as an example taken from the transcriptions

Code Name (Abbreviation)	Code Definition	Transcription Example
FSM Definitions (FSM_FD)	Informant describes a framework, model or standard	"In some cases, if we take ISO security, or ISO 27001, which is the security certification, it sometimes places general requirements such as the company should handle backups correctly or that we should not disclose confidential information to unauthorized persons."
FSM Challenges (FSM_Chall)	Informant describes challenges with a framework, model or standard	-
Integration of Security Training (FSM_STI)	Informant describes how the employed framework, model or standard influences the security training	"And the ones we build ourselves are also influenced by, for example, the ISO certification, the requirements and controls that come from the ISO certification and OWASP."
FSM Updates and Evolution (FSM_FUE)	Informant describes how training content remains current with evolving security practices and threats	"We have a security officer who is part of that process. Then we look, for example, when we do our audits, we'll discover that 'no, this needs to be updated' and then we point that out, and then it must be updated."
Swedish Civil Contingencies	Informant describes getting	"And then all this about updated

Agency (FSM_MSB)	security information and updates from MSB	systems is also super important, so we have several people who subscribe to the updates that MSB sends out every Friday about discovered cybersecurity threats and incidents, and it also mentions if there have been vulnerabilities discovered in different systems.”
External FSM (FSM_EX)	Informant describes employing external FSM	“Yes. The most important thing is the ISO certification. It comes with a lot of requirements and controls. We have a new ISO 27001 update today.”
Internal FSM (FSM_IN)	Informant describes employing FSM that are developed in-house	“Then we have an █████ Security Framework that we have developed ourselves, and that's what then governs how a computer should look and function, how the applications should be used.”
Human Factors Integration (FSM_HFI)	Informant describes how frameworks, models and standards influence the security culture	“...and that's actually one of the requirements we have from our ISO certification. To ensure that leadership provides the support that fits.”
Social Media (FSM_SM)	Informant describes employing FSM related to Social Media	-
Remote Working (FSM_RW)	Informant describes employing FSM related to Remote Working	-
Types of FSM Employed (FSM_TE)	Informant describes what framework, model or standard the company employ	-
ISO/IEC 27001 (FSM_TE_ISO)	Informant employs the ISO/IEC 27001 framework	“We are ISO certified according to the ISO 27001 standard, which is the information security standard.”
NIST (FSM_TE_NIST)	Informant employs the NIST framework	-
Strategic Alignment Model (FSM_TE_SAM)	Informant employs the SAM framework	-
Information Security Culture Framework (FSM_TE_ISCF)	Informant employs the ISCF framework	-

Competing Security Cultures Framework (FSM_TE_CSCF)	Informant employs the CSCF framework	-
Information Security Culture Assessment (FSM_TE_ISCA)	Informant employs the ISCA framework	-
The Security Culture Toolkit (FSM_TE_SCT)	Informant employs the SCT framework	-
CAT framework (FSM_TE_CAT)	Informant employs the CAT framework	-
CyberSec Labs framework (FSM_TE_CL)	Informant employs the CyberSec Labs framework	-
CENSOR framework (FSM_TE_CEN)	Informant employs the CENSOR framework	-
The Adaptive Cybersecurity Training framework for Social Media Risks (FSM_TE_ACSTF-SMR)	Informant employs the ACSTF_SMR framework	-
Open Web Application Security Project (FSM_TE_OWASP)	Informant employs the OWASP framework	"Then we have specific cases, for example, OWASP, which is more aimed at developers."
Plan-Do-Check-Act (FSM_TE_PDCA)	Informant employs the PDCA framework	"We work with continuous improvement according to Plan-Do-Check-Act. We work with risk analyses."
Zero Trust Security Model (FSM_TE_ZT)	Informant employs the Zero Trust Security Model	"But it must be Zero Trust as it is called in all dimensions. We run multifactor authentication, all these things."
Training Frequency (TM_FR)	Informant describes the frequency of the security training	"It depends on how often they are sent out, but I would say it's one to two times a month at least."
Training Duration (TM_DU)	Informant describes the duration of the security training	"I would say it's about seven minutes."
Internal Training Material (TM_ITM)	Informant describes training material that is developed internally (in-house)	"It's our own training, for example, that we set up, and we do it at our own pace."

External Training Material (TM_ETM)	Informant describes training material that comes from external provider	“SecureFlag is an external provider that offers online-based training specifically for developers.”
Awareness Training Purpose (TM_ATP)	Informant describes the goal of the security training	-
Social Media (TM_SM)	Informant describes training aimed at heightening awareness of social media usage	“No, we don't. It's not something we discuss, however, we have gained some insights now through this phishing test, so we will probably talk about it a bit more, but it's not something we talk about today.”
Remote Working (TM_RW)	Informant describes training aimed at employees working remotely	“It also includes some good tips, like not connecting to open networks, using privacy screens when on trains or in public areas, and so on. So there are a lot of tips in it, but I would say it's quite basic.”
Description of Security Training (TM_DST)	Informant describes the employed security training	“And then we have a session specifically for information security. Then it's also mandatory, then we have a Canvas training.”
Training Results (TM_TR)	Informant describes result of training	“Yes, they did, about 23%. The standard usually lies - for non-IT companies, the standard is usually over 30%, 26% is the standard for the IT and consulting industry otherwise, so we were doing quite well.”
Types of Training Methods Employed (TM_TE)	Informant describes types of training methods employed	-
Conventional Methods (TM_TE_CM)	Informant employs instructor-led classrooms or seminars	“I would say seminars, but not everyone attends those, we send a few occasionally and those who attend take notes and then share with others what was discussed.”
Interactive and Experiential (TM_TE_IE)	Informant employs case studies, role-playing, gamification or simulation training	“We could say we do Gamification with this phishing quiz, then there's simulation through the actual test.”
Technology-Driven (TM_TE_TD)	Informant employs web-based training, self-paced online training, online instructor-led training, or webinars	“Web-based training is the one I mentioned that we do every year, and we are also putting together our own more in-depth one now, which we will finalize after we get the results from this phishing quiz.”
Informal Learning (TM_TE_IL)	Informant employs coaching, mentoring, or other types of informal training	“Coaching and mentorship, we have that but it's not formalized so that when someone needs help with something related to security, they always contact an expert in the field, so I guess that's where it belongs.”

Blended Approaches (TM_TE_BA)	Informant employs a combination of different training methods	"No, it's a combination of several. It varies."
Security Organizational Culture Strategy (OC_SOCS)	Informant describes their strategy to promote a cybersecurity culture	"The strategy is still to try to incorporate training elements and information into our daily routine so to say. It should be a natural part of our operation."
Leadership (OC_LE)	Informant describes measure in place to ensure that leadership promote a cybersecurity culture	"We have very strong support from the management team. Awareness is quite high. Our CEO is very keen that data is our biggest asset—data and our employees."
Personalization (OC_PE)	Informant describes if and how security training is personalized to individual employees or employee groups	"This generates an awareness score for each individual, which we use internally so that all employees have some sort of score."
Core Values (OC_CV)	Informant describes if and how cybersecurity is integrated into the core values of the company	"Not explicitly, but it is in a way. Simplicity is a core value that we use."
Positive Workplace Environment (OC_PWE)	Informant describes what measure are in place to promote a positive environment surrounding cybersecurity	"It's crucial that we never use this to single out people but rather to strengthen them. The goal is obviously that no one clicks on a malicious link, but it happens, so removing the guilt or embarrassment if someone does helps them feel safe reporting it to IT."
Security Culture Surrounding Remote Working (OC_RW)	Informant describes guidelines, rather than training, regarding remote working	"Of course, we advise on how to think when traveling, that you should always lock your computer and not sit where someone might shoulder surf you, but we assume the same level of security on the device whether you are on our network or at an airport."
Security Culture Surrounding Social Media (OC_SM)	Informant describes guidelines, rather than training, regarding social media	"Generally, we have forbidden social media."
Culture Challenges (OC_CC)	Informant describes challenges surrounding security culture	"The difficulty with conducting this type of training, first of all, there is no real tradition of these kinds of issues, the operation is very production-oriented and very solution-oriented."
Informant Role (IB_IR)	Informant describes their role	"My name is [REDACTED]. I'm usually a consultant. I work a lot with M365."

Informant Company (IB_IC)	Informant describes their company	“It's quite a small internal organization, we have two internal staff, but then I also work with 25 external consultants on a regular basis.”
---------------------------	-----------------------------------	---

Appendix H - AI Report

AI-based tools have been utilized for this thesis, but strictly as support regarding language, text structure, as well as transcribing interview audio recordings. The entire content in this thesis has been originally created by the authors, however, the language and structure have in some parts been enhanced by generative large language model AI.

Tools:

- ChatGPT
- Whisper

Usage:

ChatGPT has been employed primarily to enhance pre-existing text, rather than to create new content from scratch. We have utilized ChatGPT's capabilities in enhancing text across chapters 1-6, although some sections have been left completely untouched. It is important to note that we intentionally limited ChatGPT's role to minor enhancements to preserve the authenticity of the original text as much as possible. By "enhancements" we refer to correcting linguistic errors, substituting specific words with more appropriate alternatives, and restructuring poorly constructed sentences. This approach ensured that the core of our writing remained intact, while still benefiting from the clarity and precision that AI assistance can provide.

This is what we have asked ChatGPT to do for us:

- Enhance the language and sentence structure used in a specific text segment.
- Translate certain terms from Swedish to English.
- Give feedback on logical flow in text segments.

We should mention that text has never been blindly copy-pasted directly from ChatGPT into the thesis. When asking ChatGPT to enhance text, we have carefully chosen which "enhancements" from ChatGPT to implement into our original text. This approach was adopted because we prioritize our own judgment over that of the AI, ensuring that any modifications align closely with the intended meaning.

Whisper was merely utilized to transcribe two interview audio recordings, which are presented in Appendix C and D. These transcriptions have since been manually modified to fit a specific format.

References

- Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, pp.5–14.
- Alsharif, M., Mishra, S., & AlShehri, M. (2021). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, 40 (3), pp.1153–1166.
- Angafor, G.N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *SECURITY AND PRIVACY*, 3 (6), p.e126.
- Andreasson, J., & Johansson, T. (2024). Handbok för uppsatsskrivande : att genomföra en kvalitativ undersökning och presentera sina resultat. Första upplagan. Lund: Studentlitteratur.
- Bada, M., Sasse, A.M., & Nurse, J.R.C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. <http://arxiv.org/abs/1901.02672>. [Accessed 14 April 2024].
- Belalcázar, A., Ron, M., Díaz, J., & Molinari, L. (2017). Towards a Strategic Resilience of Applications through the NIST Cybersecurity Framework and the Strategic Alignment Model (SAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)*. pp.181–187.
<https://ieeexplore.ieee.org/document/8328104?arnumber=8328104>. [Accessed 6 April 2024].
- Ben Salamah, F., Palomino, M.A., Craven, M.J., Papadaki, M., & Furnell, S. (2023). An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. *Applied Sciences*, 13 (17), p.9595.
- Cambridge Dictionary. (2024a). Awareness.
<https://dictionary.cambridge.org/dictionary/english/awareness>. [Accessed 12 April 2024].
- Cambridge Dictionary. (2024b). Framework.
<https://dictionary.cambridge.org/dictionary/english/framework>. [Accessed 15 April 2024].
- Cambridge Dictionary. (2024c). Strategy.
<https://dictionary.cambridge.org/dictionary/english/strategy>. [Accessed 12 April 2024].
- Cambridge Dictionary. (2024d). Training.
<https://dictionary.cambridge.org/dictionary/english/training>. [Accessed 12 April 2024].
- Cheung, K.K.C., & Tai, K.W.H. (2023). The use of intercoder reliability in qualitative interview data analysis in science education. *Research in Science & Technological Education*, 41 (3), pp.1155–1175.
- Corradini, I. (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Cham: Springer International Publishing. <http://link.springer.com/10.1007/978-3-030-43999-6>. [Accessed 2 April 2024].
- Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*, 47 (3), pp.79–86.
- Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021). A

- Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*. pp.102–106.
<https://ieeexplore.ieee.org/document/9498208?arnumber=9498208>. [Accessed 6 April 2024].
- Djebbar, F., & Nordström, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, 11, pp.85315–85332.
- El-Bably, A.Y. (2021). Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management. *Journal of Information Security and Cybercrimes Research*, 4 (1), pp.95–102.
- Evans, A. (2022). *Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization*. London: Routledge.
- Falco, G., & Rosenbach, E. (2022). What Do I Need to Know About Cyber Frameworks, Standards, and Laws?. In G. J. Falco and E. Rosenbach (Eds.), *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, p.0. <https://doi.org/10.1093/oso/9780197526545.003.0004>. [Accessed 6 April 2024].
- Flores, C.V., Gonzalez, J., Kajtazi, M., Bugeja, J., & Vogel, B. (2023). Human Factors for Cybersecurity Awareness in a Remote Work Environment. In *International Conference on Information Systems Security and Privacy*. Science and Technology Publications, Lda, pp.608–616.
<http://lup.lub.lu.se/record/a28c8472-252d-4d3f-a697-87ff7568cccf>. [Accessed 6 April 2024].
- George, B. (2020). Introduction. In B. George and J. Paul (Eds.), *Digital Transformation in Business and Society: Theory and Cases*. Cham: Springer International Publishing, pp.1–11. https://doi.org/10.1007/978-3-030-08277-2_1. [Accessed 30 March 2024].
- Giriraj, A., Haggag, S., & Haggag, H. (2022). Human centric framework for customising and producing effective cybersecurity training materials. In pp.69–77.
<https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-206038>. [Accessed 6 April 2024].
- Google. (2024a). Google Dokument: Dokumentredigera online | Google Workspace.
<https://www.google.se/intl/sv/docs/about/>. [Accessed 26 April 2024].
- Google. (2024b). Plattform för personlig molnlagring och fildelning – Google.
<https://www.google.com/intl/sv/drive/>. [Accessed 26 April 2024].
- Greulich, M., Lins, S., Pienta, D., Thatcher, J.B., & Sunyaev, A. (2024). Exploring Contrasting Effects of Trust in Organizational Security Practices and Protective Structures on Employees' Security-Related Precaution Taking. *Information Systems Research*, p.isre.2021.0528.
- Handri, E.Y., Putro, P.A.W., & Sensuse, D.I. (2023). Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*. Bogor, Indonesia: IEEE, pp.82–87.
<https://ieeexplore.ieee.org/document/10277024/>. [Accessed 6 April 2024].
- He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21 (2), pp.203–213.
- Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees: Sensors (Basel, Switzerland). *Sensors (Basel, Switzerland)*, 22 (22).
<https://ludwig.lub.lu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cmedm&AN=36433259&site=eds-live&scope=site>. [Accessed 6 April 2024].

- Jacobsen, D.I. (2024). Hur genomför man undersökningar? : introduktion till samhällsvetenskapliga metoder. Tredje upplagan. Lund: Studentlitteratur.
- Kose, Y., Ozer, M., Bastug, M., Varlioglu, S., Basibuyuk, O., & Ponnakanti, H.P. (2021). Developing Cybersecurity Workforce: Introducing CyberSec Labs for Industry Standard Cybersecurity Training. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. pp.716–721. <https://ieeexplore.ieee.org/document/9798917?arnumber=9798917>. [Accessed 6 April 2024].
- MAXQDA. (2024). MAXQDA | QDA software package for Windows & Mac. <https://www.maxqda.com/products/maxqda>. [Accessed 25 April 2024].
- McIntosh, T.R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., & Halgamuge, M.N. (2024). From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. <http://arxiv.org/abs/2402.15770>. [Accessed 15 April 2024].
- McMullin, C. (2023). Transcription and Qualitative Methods: Implications for Third Sector Research. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, 34 (1), pp.140–153.
- Möller, D.P.F. (2020a). Introduction to Cybersecurity. In D. P. F. Möller (Ed.), *Cybersecurity in Digital Transformation: Scope and Applications*. Cham: Springer International Publishing, pp.11–27. https://doi.org/10.1007/978-3-030-60570-4_2. [Accessed 30 March 2024].
- Möller, D.P.F. (2020b). Introduction to Digital Transformation. In D. P. F. Möller (Ed.), *Cybersecurity in Digital Transformation: Scope and Applications*. Cham: Springer International Publishing, pp.1–10. https://doi.org/10.1007/978-3-030-60570-4_1. [Accessed 30 March 2024].
- Oates, B.J. (2006). Researching information systems and computing. 1. publ., Repr. Los Angeles: SAGE.
- OpenAI. (2022). Introducing Whisper. <https://openai.com/research/whisper>. [Accessed 25 April 2024].
- Qawasmeh, S.A.-D., AlQahtani, A.A.S., & Khan, M.K. (2024). Navigating Cybersecurity Training: A Comprehensive Review. <http://arxiv.org/abs/2401.11326>. [Accessed 6 April 2024].
- Tietoevry.com. (2024). UPDATE: Ransomware attack in Swedish data center. <https://www.tietoevry.com/en/newsroom/all-news-and-releases/other-news/2024/01/ransomware-attack-in-sweden-update/>. [Accessed 5 April 2024].
- Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimization: A Small Business Case Study. *IEEE Access*, 11, pp.44467–44481.
- Vasudevan, S., Piazza, A., & Carr, M. (2023). A Decade of Studies on Cyber Security Training in Organizations using Social Network Analysis: A Systematic Literature Review Through Keyword co-Occurrence Network. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*. pp.1–6. <https://ieeexplore.ieee.org/document/10111127?arnumber=10111127>. [Accessed 6 April 2024].
- Watters, P.A. (2023). Cybercrime and Cybersecurity. Boca Raton: CRC Press.