# "NOT MY RESPONSIBILITY!" - A COMPARATIVE CASE STUDY OF ORGANIZATIONAL CYBERSECURITY SUBCULTURES

CHRISTER HØILAND

SUPERVISOR
Marko Ilmari Niemimaa

**University of Agder, 2023**
Faculty of Social Sciences
Department of Information Systems

## Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

| | | |
|---|---|---|
| 1. | Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen. | Ja |
| 2. | **Vi erklærer videre at denne besvarelsen:**<br>• Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands.<br>• Ikke refererer til andres arbeid uten at det er oppgitt.<br>• Ikke refererer til eget tidligere arbeid uten at det er oppgitt.<br>• Har alle referansene oppgitt i litteraturlisten.<br>• Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse. | Ja |
| 3. | Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31. | Ja |
| 4. | Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert. | Ja |
| 5. | Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk. | Ja |
| 6. | Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider. | Ja |
| 7. | Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet. | Ja |

## Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

| | |
|---|---|
| Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering: | Ja |
| Er oppgaven båndlagt (konfidensiell)? | Nei |
| Er oppgaven unntatt offentlighet? | Nei |

# Acknowledgements

This is the final submission of my thesis for the Cybersecurity master's program at the University of Agder (UiA) in the faculty of Social Sciences. The research was conducted between January 2023 and June 2023.

I want to express my gratitude to my supervisor, Professor Marko Ilmari Niemimaa, for guiding me and providing valuable feedback throughout this project. His assistance has been essential, and this thesis would not have been possible without him.

I would also like to thank the partnering organizations and all the interview participants who generously shared their knowledge and insights with me. The data collected from these interviews has been an invaluable contribution to this research. I am grateful for their positive attitude towards me as a researcher.

Lastly, I would like to thank my family and friends for their unwavering support throughout this period.

Kristiansand, Norway
June 2$^{nd}$ 2023

Christer Høiland

Christer Høiland

# Abstract

Despite significant technological advancements and the increasing sophistication of cyberattacks in today's modern society, organizations underestimate the human link in cybersecurity. Many still overlook that human behavior and decision-making are crucial in protecting sensitive information and mitigating risks. Organizations seemingly prioritize investigating time and resources into improving their technological cybersecurity measures rather than increasing the employees' cybersecurity knowledge. These actions significantly impact the cybersecurity culture of the company.

Cybersecurity culture refers to the shared values, beliefs, and actions of the employees in an organization that emphasize the importance of safeguarding digital assets, data, and systems against cyber threats. It encompasses the organization's dedication, awareness, protocols, and ability to manage cybersecurity risks and promote a security-focused environment. Recent studies have primarily focused on discussing cybersecurity culture as a singular concept within an organization.

This qualitative research aims to investigate the impact of cybersecurity subcultures within organizations. A systematic literature review was conducted to gain an overview of the existing theoretical background on cybersecurity subcultures. This process proved that there is a research gap in the topic of subcultures, as most of the current literature encompasses cybersecurity culture as a collective concept. Data was collected through semi-structured interviews with ten employees from two IT companies. Cybersecurity leaders from each company agreed that the sales and IT subcultures had the most significant differences; hence, employees from each subculture in both companies were interviewed.

The results prove that the security leaders' suspicions were correct. The sales subcultures need to gain more knowledge about cybersecurity. Cybersecurity measures are seen more as obstacles instead of improving their cybersecurity. There is also a significant need for more responsibility. They believe that someone better qualified will take care of their mistakes if they cause a cybersecurity incident. On the other hand, the IT subculture seems to understand cybersecurity better. They have comprehensive knowledge of the topic. However, they also share this uncertainty regarding responsibilities, stating they feel pressured to share their expertise with colleagues. This leaves them with limited time to complete their actual work tasks. They point to a lack of management responsibility as one of the critical reasons for this.

This research sheds light on cybersecurity subcultures and challenges the notion that organizations have only one cybersecurity culture. Organizations need to allocate their time and resources differently and acknowledge the significance of subcultures in maintaining overall cybersecurity. The findings and insights are meant to assist organizations in enhancing their cybersecurity operations and protocols.

**Keywords: Cybersecurity culture, subcultures, organizational cybersecurity**

# Contents

**Acknowledgements** **ii**

**Abstract** **iii**

**List of Figures** **vii**

**List of Tables** **ix**

**1 Introduction** **1**

1.1 Research Problem . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
1.2 Research Motivation . . . . . . . . . . . . . . . . . . . . . . . . . . 2
1.3 Research Question . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
1.4 Research Contribution . . . . . . . . . . . . . . . . . . . . . . . . . 3
1.5 Research Approach . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
1.6 Thesis Structure . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

**2 Theoretical Background** **6**

2.1 Defining Cybersecurity Culture . . . . . . . . . . . . . . . . . . . . . 6
2.1.1 Values . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7
2.1.2 Assumptions . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
2.1.3 Beliefs . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
2.2 Understanding Cybersecurity Culture . . . . . . . . . . . . . . . . . . 9
2.2.1 Organizational Culture and Cybersecurity Culture . . . . . . . . . . 10
2.2.2 Cybersecurity Subcultures . . . . . . . . . . . . . . . . . . . . . 11
2.2.3 Subculture Awareness & Compliance . . . . . . . . . . . . . . . . 14
2.3 Theoretical Conclusions . . . . . . . . . . . . . . . . . . . . . . . . 15
2.3.1 Research Gap . . . . . . . . . . . . . . . . . . . . . . . . . . . 16

**3 Methodology** **17**

3.1 Qualitative Case Study . . . . . . . . . . . . . . . . . . . . . . . . . 17
3.2 Systematic Literature Review Methodology . . . . . . . . . . . . . . . 18
3.2.1 Formulate the Research Problem . . . . . . . . . . . . . . . . . . 19
3.2.2 Develop and Validate the Review Protocol . . . . . . . . . . . . . 19
3.2.3 Searching the Literature . . . . . . . . . . . . . . . . . . . . . . 20
3.2.4 Screen for Inclusion . . . . . . . . . . . . . . . . . . . . . . . . 20
3.2.5 Selected Literature . . . . . . . . . . . . . . . . . . . . . . . . 22
3.3 Data Collection . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23
3.3.1 Interview Participants . . . . . . . . . . . . . . . . . . . . . . . 23
3.3.2 Interviews . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
3.3.3 Ethical Considerations . . . . . . . . . . . . . . . . . . . . . . . 25
3.3.4 Data Analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . 26

**4 Findings** **28**
4.1 Management Input . . . . . 28
4.2 Empirical Findings - Employees . . . . . 30
4.2.1 Investigating the Sales Department Cybersecurity Subcultures . . . . 30
4.2.2 Investigating the IT Department Cybersecurity Subculture . . . . . . 35
4.3 Summary Tables . . . . . 39

**5 Discussion** **41**
5.1 Sales Cybersecurity Subculture . . . . . 41
5.2 IT Cybersecurity Subculture . . . . . 43
5.3 Practical Contributions . . . . . 45
5.4 Limitations . . . . . 48
5.5 Recommendations for Further Research . . . . . 48

**6 Conclusion** **49**

**A Interview Guide to Security Leaders** **53**

**B Interview Guide to Employees** **55**

**C Information Letter to Security Leaders** **57**

**D Information Letter to Employees** **58**

**E Data Management Plan (DMP) Submission** **59**

**F NSD Approval** **64**

# List of Figures

1.1 Research Process . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

2.1 Cybersecurity Culture Maturity Roadmap, inspired by Madnick et al., 2019 . 10
2.2 Organizational Cultures Illustration . . . . . . . . . . . . . . . . . . . . . . . . . 14
2.3 Conceptual Framework for Cybersecurity Subcultures. Inspired by (Keman & Pearlson, 2019). . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16

3.1 SLR process model (Xiao & Watson, 2019) . . . . . . . . . . . . . . . . . . . . 19
3.2 Final systematic literature review . . . . . . . . . . . . . . . . . . . . . . . . 21
3.3 Interview Questions Structure . . . . . . . . . . . . . . . . . . . . . . . . . . 25
3.4 Example of Transcription Coding in Company A . . . . . . . . . . . . . . . . . 27

5.1 Proposed Cybersecurity Subculture Framework . . . . . . . . . . . . . . . . . . 47

# List of Tables

3.1 Partnering Organizations . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23
3.2 Interview Participants . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24

4.1 Company A Cybersecurity Subculture Findings . . . . . . . . . . . . . . . . . . 39
4.2 Company B Cybersecurity Subculture Findings . . . . . . . . . . . . . . . . . . 40

# Chapter 1

# Introduction

## 1.1 Research Problem

Information is one of the most valuable resources in today's digitized society. It is, therefore, an ever-increasing threat that criminals are looking to steal this information. Organizations have become increasingly aware of the importance of protecting data, assets, and reputations in a constantly evolving threat landscape. One of the main ways organizations solve this is to invest large amounts of resources and money in robust digital systems to protect them against potential cyber-attacks. The purpose of this is both to prevent an attack from happening in the first place and to create fully automated solutions that can counter cyber-attacks if they should occur in the first place. Hence, many organizations erroneously assume that investing heavily in technological protection measures is the sole solution to achieving cybersecurity. However, recent findings reveal that the crucial role of humans in ensuring cybersecurity is often disregarded. According to a report by Verizon, a staggering 85% of cyber-attacks result from human error (Verizon, 2021). This underscores the pressing issue of employees' need for understanding and awareness of how to respond to digital threats. In reality, numerous attacks can be attributed to human error, with documented instances attesting to this fact:

In March 2017, Equifax, a credit company that holds significant amounts of financial information on most Americans, suffered a severe cyber-attack traced to a lack of cybersecurity culture (Fruhlinger, 2020). The attackers took advantage of well-known weaknesses that should have been addressed long ago, and the company had also failed to renew the encryption on internal cybersecurity mechanisms. This led to the leakage of sensitive information, and Equifax was accused of having a lax approach to cybersecurity (Fruhlinger, 2020). In addition, the company needed to apply the available solutions to fix the detected bug, indicating a need for cybersecurity awareness among the employees. This incident highlighted a typical weakness in cybersecurity culture and had the employees acted earlier on the detected errors, the Equifax attack could have been prevented.

How employees in the organization will behave and act in the face of cybersecurity is primarily defined by the cybersecurity culture in the organization (Uchendu et al., 2021). The cybersecurity culture is a sub-section of the organizational culture that refers to shared values, attitudes, and beliefs that direct an organization's strategy for safeguarding its digital resources and data (Schulman, 2020). This involves employees' behaviors, actions, and habits to defend the company's information assets. For example, a company that prioritizes cybersecurity culture motivates its workers to take responsibility for safeguarding their information and systems and provides necessary resources and training. Additionally, it fosters a culture of responsibility and accountability, where employees are answerable for their actions and are encouraged to report any suspicious activity or incidents (Alshaikh, 2020).

In the organization, there is more than one cybersecurity culture. Subcultures arise as subordinate parts of the overall culture. These subcultures can develop their ways and routines of dealing with cybersecurity (Da Veiga & Martins, 2017). Cybersecurity subcultures are groups of people within organizations that share a common interest in or focus on cybersecurity. These subcultures can range from small, informal groups to larger, more formal communities. They can include employees from different departments and levels of the organization. Cybersecurity subcultures can be a valuable resource for organizations, as they can help to promote a culture of cybersecurity awareness and responsibility (Da Veiga & Martins, 2017). They can also provide a forum for sharing best practices, discussing emerging threats, and collaborating on projects. It is important to note that there is a potential for various cybersecurity subcultures to develop their distinct habits and practices when it comes to managing cybersecurity. If these approaches do not align with the company's established cybersecurity protocols, the organization's cybersecurity could pose a significant risk (Da Veiga & Martins, 2017).

Maintaining a solid cybersecurity culture within an organization is crucial, and it is also the responsibility of management to ensure it (Shaikh & Siponen, 2022). The organization's management sets the tone for the organization's approach to cybersecurity by emphasizing its importance to employees, establishing clear policies for handling sensitive information, and providing training and resources to implement those policies (Shaikh & Siponen, 2022). In the case of an incident or breach, management is responsible for collaborating with cybersecurity and IT teams to investigate and contain the situation and take necessary measures to safeguard the company's data and reputation. Receiving support from management is crucial for establishing a robust cybersecurity culture. However, some managers are increasingly placing less emphasis on the human aspect of cybersecurity and instead focusing more on investing in technological protection measures. This trend has been highlighted in a recent article by Bailey et al., 2014.

Organizations must have cybersecurity subcultures as they help to establish a cybersecurity-conscious environment (Da Veiga & Martins, 2017). These subcultures play a significant role in safeguarding sensitive information and preventing data breaches. Examining these subcultures can identify potential risks or vulnerabilities within the organization. Moreover, investigating these subcultures also helps identify areas where the organization's cybersecurity practices can be enhanced. This can involve introducing new cybersecurity measures or training employees on the best methods to protect confidential information. Cybersecurity subcultures in organizations are vital to creating a cybersecurity culture and minimizing the possibility of data breaches. Hence, it is a more important topic now than ever and should be investigated Da Veiga and Martins, 2017.

## 1.2 Research Motivation

The motivation for carrying out this research is twofold. The first reason is personal interest. Throughout my course of study, the human element in cybersecurity has been an element I have become increasingly interested in. After having lectures on cybersecurity culture, I wanted to immerse myself in this topic. Then I discovered that there were several dimensions around cybersecurity cultures, including the topic of the subcultures. I saw this in practice at an IT company in the Autumn of 2022. There I got an insight into what it is like to work with cybersecurity and contribute to what may become my future work tasks. Although I saw and learned that strong technological cybersecurity measures exist, several of the employees I met in the organization needed to be made aware of certain things around cybersecurity. This made me want to dig further, and then I mainly wanted to focus on cybersecurity culture.

The second part of the motivation is to shed light on the above topic to management and employees in the organizations. Bailey et al., 2014 emphasizes that most organizations underestimate the importance of cybersecurity culture and that far too much of the focus around cybersecurity is placed on implementing technological protection methods. However, it is essential to realize that humans can be the first line of defense against cyber threats. Hence, cybersecurity cultures are crucial for how employees behave in the face of digital threats. Therefore, I wanted to examine the state of affairs around this and compare it across organizations and subcultures.

## 1.3 Research Question

To understand the research gap and establish a clear direction for the study, a research question has been formulated as the outline of this research project:

- **How do the cybersecurity subcultures influence employees' attitudes and behaviors towards cybersecurity practices and risk management?**

It is essential to answer the research question to understand how the different subcultures within an organization affect employee attitudes and actions toward cybersecurity. Various subcultures' approaches toward cybersecurity can significantly impact awareness, commitment, and adherence to cybersecurity practices. Analyzing these influences can help organizations identify subcultures that positively affect cybersecurity and use their methods to cultivate a cybersecurity-first culture across the entire organization. Conversely, dealing with subcultures hindering cybersecurity awareness and behaviors enables organizations to implement focused interventions that enhance cybersecurity posture. This topic can be further uncovered and investigated through the interviews.

By aiming to answer this research question, organizations can gain valuable insights into the relationship between cybersecurity subcultures, employee attitudes and behaviors, and overall cybersecurity resilience. Such knowledge can be used to develop targeted strategies, training programs, and initiatives to strengthen the organization's cybersecurity culture and effectively enhance its ability to respond to new and evolving cyber threats.

## 1.4 Research Contribution

This study aims to contribute valuable insights into the distinguishing features of subcultures within cybersecurity culture. By analyzing these findings, organizations can better understand how these subcultures impact cybersecurity. My study and its results will provide organizations with the necessary tools to enhance their employees' relationship with cybersecurity. This study will delve into the cybersecurity culture of both management and employees within subcultures. The insights gathered will help employees better understand their managers' attitudes and that both parties can foster mutual learning and understanding. As cybersecurity culture becomes increasingly important in the future, I encourage organizations to view this study as constructive feedback. It is worth noting that this study is not designed to criticize any individual or organization but rather to identify areas for improvement.

## 1.5 Research Approach

A qualitative research approach will be utilized to comprehensively explore and comprehend the concept of cybersecurity culture and its subcultures. This method involves obtaining non-numerical data from a group of individuals via interviews. As a first step, a Systematic Literature Review (SLR) will be conducted to gain an understanding of the existing theoretical background of the topic. The SLR model by Xiao & Watson (Xiao & Watson, 2019) will be followed, which includes predefined steps to be taken before the process starts. Finally, the outcomes of this literature review will be used to form a comprehensive picture of the existing background literature on the topic.

The interviews will be conducted in the form of semi-structured interviews with individual employees from each of the identified subcultures in both companies. Initially, the managers in each company will be interviewed. They will provide their perspective on their cybersecurity culture and highlight the two subcultures in their organization that they believe have the most significant differences in cybersecurity culture. This will guide which subcultures, and employees are to be interviewed further. Ten interviews will be conducted, including two with security managers, four with IT employees, and four with sales employees. The complete list of interviewees can be seen in the table ??. Once the interviews have been completed, they will be transcribed, coded, and analyzed. The research process will be carried out systematically throughout the entire project, as shown in the figure below:

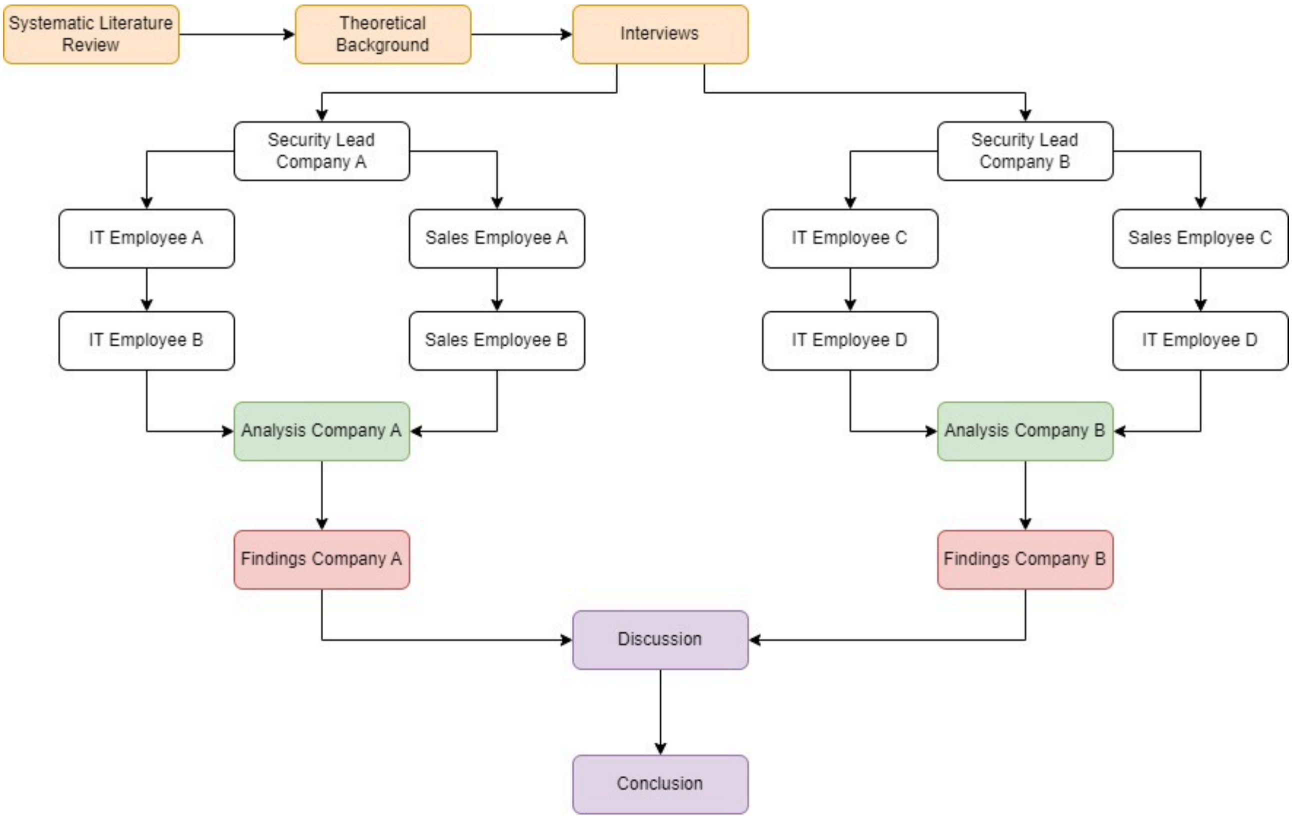


Figure 1.1: Research Process

## 1.6 Thesis Structure

This master thesis is structured into six chapters, which will be listed and shortly described in this section.

**Chapter 1: Introduction**

The first chapter overviews the study's research problem, approach, motivation, and aim. Then, a research question will be established as the fundamental basis for the study.

**Chapter 2: Theoretical Background**

In the second chapter, existing literature on the topic is described. The information was gathered through a systematic literature review. This will underline the importance of the topic and identify knowledge gaps in the existing theories that this study can investigate.

**Chapter 3: Methodology**

The third chapter will describe and justify all the methodologies used in this study. The process of carrying out the systematic literature review will be explained. The data collection methods will also be described, including the research approach, interviews, and data analysis.

**Chapter 4: Findings**

The fourth chapter will describe the findings from the interviews after the data was analyzed. Finally, the findings will be presented between the subcultures and the companies.

**Chapter 5: Discussion**

The fifth chapter will discuss the findings against the claims from the theoretical background. It will also be discussed improvements that could be implemented and what the results can contribute to the organization.

**Chapter 6: Conclusion**

In the final chapter, the research project will conclude. It will include brief reflections on the study's outcomes and a description of any limitations encountered during the research.

# Chapter 2

# Theoretical Background

This chapter will review the existing theoretical background on the topic, primarily discovered through a systematic literature review.

## 2.1 Defining Cybersecurity Culture

As organizations seek to tackle an increment in attacks that take advantage of human characteristics, cybersecurity culture has received important attention in practice and study over the last decade. (Uchendu et al., 2021). Culture refers to a group's shared norms that shape their perceptions, thoughts, feelings, and behaviors (Schein, 1996), and this definition is also incorporated into cybersecurity culture. Several definitions exist of cybersecurity culture, but the concept essentially refers to the employees' perception of values, assumptions, and beliefs around cybersecurity (Da Veiga et al., 2020). The organization's management usually sets a collective cybersecurity culture through rules and routines they encourage the employees to follow. Still, how the employees perceive and implement these in everyday work will eventually define the organization's practiced cybersecurity culture (Da Veiga et al., 2020).

Cybersecurity culture also encompasses the shared understanding of the importance of cybersecurity, the level of awareness and knowledge among employees, the degree of compliance with cybersecurity policies and procedures, and the overall commitment to protecting information and systems (Li et al., 2019). A robust cybersecurity culture promotes a proactive cybersecurity-conscious mindset, fostering a resilient and secure environment where employees are empowered to effectively recognize, prevent, and respond to cyber threats. It involves continuous education, training, and reinforcement of cybersecurity practices, as well as the establishment of a supportive organizational climate that prioritizes cybersecurity and encourages collaboration among all employees (Alshaikh, 2020).

A good cybersecurity culture begins at the top with dedication from the leadership. Individuals tend to take cybersecurity seriously when managers prioritize it and commit to adhering to best practices (Shaikh & Siponen, 2022). Employees regularly participating in cybersecurity awareness training programs learn about the value of cybersecurity, potential dangers, and recommended practices. Password cybersecurity and secure browsing practices should all be covered in training. Organizations must have clear policies and processes that are conveyed to all employees. This consists of standards for data classification, incident response plans, and allowed usage policies. A cybersecurity-conscious work environment is more easily established when employees are given clear rules to follow (Li et al., 2019). Regular network structure, application, and user activity monitoring enables early identification and a swift response to feasible cybersecurity incidents.

Understanding cybersecurity culture is essential for any organization to secure its systems and data. However, understanding the concept of cybersecurity culture can be challenging for organizations due to several factors. Firstly, cybersecurity culture is intangible and subjective, making it difficult to measure and quantify (Alshaikh, 2020). It encompasses various attitudes, beliefs, and behaviors that vary among individuals and departments within an organization (Uchendu et al., 2021). Additionally, cybersecurity culture is influenced by multiple factors such as organizational structure, leadership, employee demographics, and external influences, making it complex to grasp comprehensively.

Cybersecurity culture is not static but evolves over time, requiring continuous monitoring and adaptation. Furthermore, it demands a deep understanding of the organization's unique context and the ability to navigate the dynamic nature of cyber threats (Georgiadou et al., 2022). The multifaceted nature of cybersecurity culture and its intangible and evolving characteristics present significant challenges for organizations seeking to comprehend and effectively address it. Some of the most critical factors that define cybersecurity cultures are their perception of values, assumptions, and beliefs (Da Veiga & Martins, 2017), and they will be thoroughly investigated both in the systematic literature review and the data collection.

### 2.1.1 Values

Employees' personal values strongly influence the cybersecurity culture within an organization, impacting cybersecurity procedures in multiple ways. Employees who prioritize the personal values of accountability and honesty are more aware of cybersecurity risks and actively seek out potential cybersecurity issues, promptly reporting suspicious emails or network activities (Da Veiga & Martins, 2017). This contributes to the early detection and prevention of cyber threats. Those who value compliance and adherence to rules and regulations are likelier to follow organizational policies, use strong passwords, update software, and comply with cybersecurity standards (Uchendu et al., 2021). Their commitment to compliance helps build a robust cybersecurity culture. Moreover, personal ethics and integrity play a significant role in employees' approach to cybersecurity. Individuals with high ethical standards are less likely to engage in risky behaviors such as unauthorized data access, disclosure of sensitive information, or downloading unauthorized software (Uchendu et al., 2021). Additionally, employees who embrace responsibility and accept accountability for their actions prioritize cybersecurity measures. As a result, they understand the impact of their efforts on the organization's cybersecurity and actively contribute to maintaining a secure environment (Uchendu et al., 2021).

In addition to these values, continuous learning and adaptability are essential for improving the cybersecurity culture (Uchendu et al., 2021). Employees who value staying updated on potential threats and technological advancements are likelier to participate in training programs, follow best practices, and adapt to new cybersecurity measures (Uchendu et al., 2021). Privacy and data protection values also contribute to a more robust cybersecurity culture, as employees who prioritize these values handle sensitive information carefully and are conscious of data cybersecurity and privacy legislation (Uchendu et al., 2021). Transparency is another significant value that influences cybersecurity culture. When managers encourage openness about their activities, concerns, and potential cybersecurity incidents, a culture of awareness is fostered (Wiley et al., 2020). This enables employees to effectively identify potential risks and attacks, report instances promptly, and take necessary measures to safeguard sensitive information. Reporting incidents such as phishing emails or unauthorized access allows managers to respond swiftly, preventing further damage and implementing cybersecurity measures (Wiley et al., 2020).

### 2.1.2 Assumptions

Employee assumptions can significantly influence cybersecurity subcultures within organizations, shaping the attitudes and behaviors of employees toward cybersecurity practices (Da Veiga et al., 2020). These assumptions can profoundly impact the organization's overall cybersecurity posture if left unchecked. Employee assumptions can lead to a false sense of cybersecurity. If employees assume that the organization's cybersecurity measures are foolproof, they may become ignorant and not pay attention to best practices (Li et al., 2019). For example, they may think that their passwords are strong enough or that their devices are protected, leading them to engage in risky behaviors such as sharing credentials or accessing sensitive information on unsecured networks. This complacency can create a subculture that undermines the importance of cybersecurity, making the organization more vulnerable to attacks (Da Veiga et al., 2020).

Furthermore, assumptions about personal knowledge and skills can hinder the cybersecurity development of subcultures. For example, employees can assume that they have sufficient knowledge about cybersecurity or are not a target for cyber threats (Da Veiga et al., 2020). This can result in a subculture where employees are ignorant of potential threats and rely solely on other protective measures. Additionally, assumptions can contribute to resistance to change, making it challenging for organizations to implement new cybersecurity measures or adapt to evolving threats Da Veiga et al., 2020. To address the impact of employee assumptions on cybersecurity subcultures, organizations should prioritize awareness, education, and a culture of continuous learning. This can involve regular training programs to enhance employees' understanding of cybersecurity risks and best practices. Managers should also encourage employees to question assumptions, remain vigilant, and actively participate in strengthening the cybersecurity culture (Da Veiga & Martins, 2017). By fostering a culture of awareness, knowledge-sharing, and accountability, organizations can cultivate a cybersecurity subculture that promotes a proactive approach to risk management and helps protect valuable assets from cyber threats (Da Veiga & Martins, 2017).

### 2.1.3 Beliefs

Employees' beliefs can significantly impact the overall cybersecurity subculture within an organization, influencing attitudes, behaviors, and decision-making related to cybersecurity (Da Veiga et al., 2020). These beliefs can both positively or negatively affect the organization's cybersecurity posture. Employees' positive views about cybersecurity contribute to a strong cybersecurity subculture. Such opinions prioritize cybersecurity measures and adherence to established policies and procedures. The understanding that cybersecurity is everyone's responsibility and realizing that their actions can directly affect the organization's cybersecurity fosters a culture of accountability and vigilance (Li et al., 2019). Employees with positive beliefs actively participate in training programs, promptly report cybersecurity incidents, and adopt cybersecurity best practices, strengthening the organization's overall cybersecurity resilience (Li et al., 2019).

On the contrary, negative employee beliefs can undermine cybersecurity subcultures and weaken the organization's cybersecurity posture. If employees believe that cybersecurity is solely the IT department's responsibility or that cybersecurity measures are unnecessary and overly restrictive, they may not prioritize cybersecurity practices (Uchendu et al., 2021). Such beliefs can lead to complacency, resistance to cybersecurity measures, and a lack of awareness of potential risks and vulnerabilities. Negative beliefs can create subcultures where employees overlook cybersecurity protocols, engage in risky behaviors, and fail to report cybersecurity incidents, making the organization more susceptible to cyber threats (Li et al., 2019).

## 2.2 Understanding Cybersecurity Culture

According to Alvarez-Dionisi and Urrego-Baquero, 2019, good cybersecurity culture is essential because it helps organizations protect their systems, data, and information from cyber-attacks and unauthorized access. An influential cybersecurity culture involves employees at all levels of the organization and requires them to take responsibility for the cybersecurity and protection of information (Uchendu et al., 2021). This consists of following cybersecurity best practices, maintaining up-to-date software, using strong passwords, performing regular backups, and reporting suspicious activity. A good cybersecurity culture also helps build trust and reputation, essential for maintaining customer relationships and a healthy business (Alshaikh, 2020).

On the other hand, poor cybersecurity culture can be detrimental to organizations in several ways. Firstly, it increases the risk of cyber-attacks and data breaches, leading to data leaks, financial loss, loss of reputation, and other negative consequences (Uchendu et al., 2021). This can lead to losing customers and partners, and in the worst-case scenario, the organization may be forced to reduce its operations (Georgiadou et al., 2022). Second, a poor cybersecurity culture can lead to a loss of trust and commitment among employees. If employees feel that the organization needs to take cybersecurity seriously, it can lead to them taking it less seriously and perhaps failing to follow the necessary cybersecurity procedures (Alshaikh, 2020). This can also affect morale and the working environment, affecting productivity and profitability. Finally, organizations that do not prioritize cybersecurity culture may be at risk of breaking the law or regulation. This can lead to the organization paying fines or compensation, affecting its reputation and trust among customers and partners. (Shaikh & Siponen, 2022).

It can be challenging for organizations to decide where to start when wanting to improve their own cybersecurity culture. However, several existing frameworks can be utilized to enhance their cybersecurity culture. One example is the cybersecurity culture maturity roadmap, designed by Madnick et al., 2019. It outlines four maturity levels in the cybersecurity culture and suggests specific steps organizations can take to increase their employees' awareness and compliance (Madnick et al., 2019). Each level of the roadmap represents a state of maturity of the organization, with level one being the least mature and level four being the most mature. The roadmap is illustrated in the following model:

- **Level 1:** Employees trust that the technological measures for cybersecurity will safeguard them. Therefore they assume that their actions related to cybersecurity won't have any repercussions.
- **Level 2:** Although employees are somewhat aware of the importance of cybersecurity, they still believe that it is solely the responsibility of the IT department and not their own.
- **Level 3:** The employees acknowledge the impact of cybersecurity on their digital decisions and take somewhat responsibility for their actions. However, they also trust that their managers will act as a last resort in case of any mistakes.
- **Level 4:**The employees understand the importance of cybersecurity and protecting digital assets through collective awareness. They comply with cybersecurity routines and policies to ensure the safety of the company's digital infrastructure.

According to Madnick et al., 2019, management in all organizations should strive to reach level 4 of this maturity model. The main goal is to make every employee feel responsible

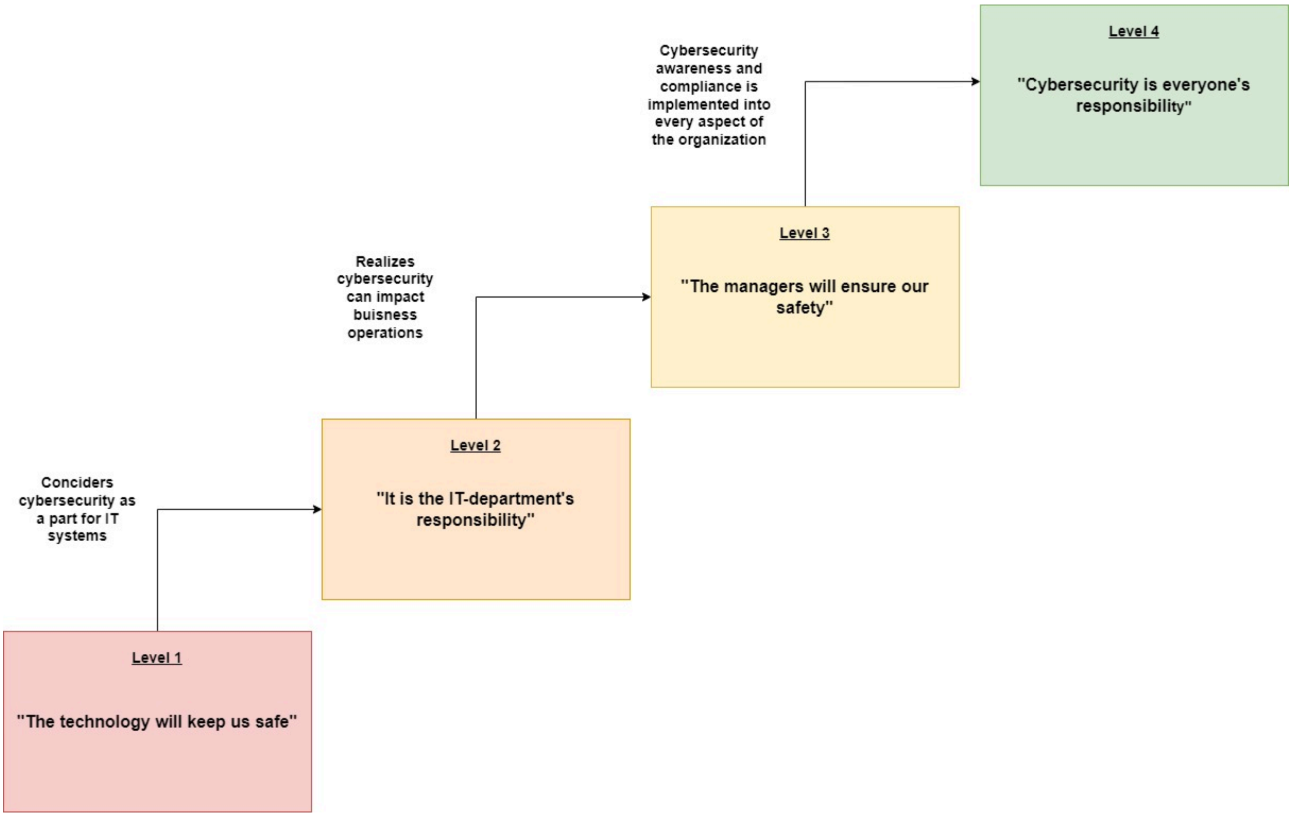

Level 4
"Cybersecurity is everyone's responsibility"
Cybersecurity awareness and compliance is implemented into every aspect of the organization
Level 3
"The managers will ensure our safety"
Realizes cybersecurity can impact buisness operations
Level 2
"It is the IT-department's responsibility"
Conciders cybersecurity as a part for IT systems
Level 1
"The technology will keep us safe"

Figure 2.1: Cybersecurity Culture Maturity Roadmap, inspired by Madnick et al., 2019

for the organization's cybersecurity and increase awareness, which will positively impact the cybersecurity culture. However, simply following this roadmap alone won't change the cybersecurity culture. The management of the organizations has to prioritize their time and resources correctly and can then utilize this roadmap as a guideline to increase resiliency (Madnick et al., 2019).

### 2.2.1 Organizational Culture and Cybersecurity Culture

The first step in understanding cybersecurity culture is understanding the difference between it and organizational culture. While both cultures are fundamental in shaping the overall character of an organization, the terms encompass different focus areas. Hence, understanding the differences between the two words could be more apparent. Every organization has a culture, regardless of its size. Organizational culture is described as “the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaption and internal integration and that has worked well enough to be considered valid, and, therefore, to be taught to new members as the correct way to perceive, think and feel concerning those problems" (Karlsson et al., 2021). In other words, organizational culture can be defined as "the way the bulk of the employees do things and see things" (Schein, 1996).

While organizational culture and cybersecurity culture are distinct, they are also interrelated. The organizational culture can significantly impact developing and maintaining a strong cybersecurity culture. For example, a positive organizational culture that values communication, collaboration, and continuous learning is more likely to foster a strong cybersecurity culture where employees are engaged and invested in cybersecurity (Karlsson et al., 2021). Hence, a hostile or toxic organizational culture can weaken efforts to develop a strong cybersecurity culture, even if policies and procedures are in place (Uchendu et al., 2021). Organizational culture refers to the broader context in which an organization operates, while cybersecurity culture relates explicitly to cybersecurity practices within that context (Schulman, 2020). Both are important for understanding an organization's approach to cybersecurity risks and its ability to mitigate them effectively.

According to (Li et al., 2019), it is a common issue that organizations struggle to see the importance of prioritizing a robust cybersecurity culture. This may be due to a need for more awareness and understanding of the importance of cybersecurity and how it can affect the organization's operations. Many see cybersecurity as a technological problem that can be solved with the right technology rather than a cultural issue that requires a holistic and continuous approach (Donalds & Osei-Bryson, 2019). Furthermore, a strong cybersecurity culture requires support from management and changes to established processes and routines, which may need to be improved by employees who are used to doing things in a certain way (Cram et al., 2020). This can create a cultural barrier to implementing effective cybersecurity practices.

### 2.2.2 Cybersecurity Subcultures

Cybersecurity subcultures refer to different groupings or communities within an overall cybersecurity culture. The subcultures may have their own norms, values, and practices that differ from the dominant cybersecurity culture (Da Veiga & Martins, 2017). These common factors are more likely adopted and internalized by employees who identify with a particular subculture. This may impact how they feel about cybersecurity procedures, risk evaluation, conformity, and the general worth of cybersecurity (Da Veiga & Martins, 2017).

For employees who have similar interests and viewpoints, subcultures foster a sense of identification and belonging. Creating a supportive network where employees may reinforce and promote cybersecurity-conscious behaviors can result from this feeling of identity (Da Veiga & Martins, 2017). Employees who aspire to belong to a specific subculture might adopt the attitudes, practices, and behaviors that that group supports. This could have negative effects if the subculture encourages unethical or counterproductive conduct. On the contrary, motivating personnel to strive for excellence in cybersecurity practices will affect the organizations positively (Wiley et al., 2020). Different cybersecurity subcultures may place a stronger emphasis on specific skill sets, methods, or safety measures. Hence, the employees who fit into these subcultures may develop into experts in certain areas, increasing their self-assurance, knowledge levels, and professional development (Da Veiga & Martins, 2017).

The cybersecurity subcultures can significantly impact how individuals behave and make organizational decisions (Da Veiga & Martins, 2017). For instance, a subculture that emphasizes the importance of proactive defense and staying ahead of new dangers may encourage its members to adopt a mindset of ongoing learning and invention. On the other hand, a subculture that prioritizes awareness and compliance might promote a more traditional and rule-based strategy (Da Veiga & Martins, 2017).

Similarly, the cybersecurity subcultures may also encourage collaboration and knowledge exchange among employees. Employees identifying with a particular cybersecurity subculture are inclined to participate in discussions, share their views, and ask fellow subculture members for help (Da Veiga & Martins, 2017). As a result, the organization could establish a greater level of shared expertise and cybersecurity posture. There may be a variety of best practices and techniques for cybersecurity. Employees who fit into a specific subculture may use and encourage these techniques at work (Da Veiga & Martins, 2017). This might result in the spread of effective cybersecurity procedures throughout the company and contribute to developing a more robust and uniform cybersecurity strategy (Li et al., 2019). Some subcultures could prioritize prudence and conservative decision-making over risk-taking to avoid potential cybersecurity problems. Others might choose a plan that prioritizes creativity and adaptability while being more risk-tolerant. The subculture an employee belongs to can affect how they perceive risk and make cybersecurity-related decisions (Alshaikh, 2020). People frequently feel a feeling of expert identity and belonging in cybersecurity subcultures. If they identify with it, employees may feel inclined to support the subculture's beliefs and objectives. This may result in more extraordinary dedication, involvement, and commitment to cybersecurity duties and obligations (Da Veiga & Martins, 2017).

Subcultures might influence employees' ethical frameworks and opinions on cybersecurity. These ethical stances may impact how employees decide and respond to moral problems. Cybersecurity culture can help people become skilled and knowledgeable in particular facets of cybersecurity (Zwilling et al., 2022). For instance, a subculture emphasizing offensive cybersecurity methods would push its members to gain proficiency in penetration testing and vulnerability analysis. The types of cybersecurity tasks that employees carry out for the organization and their future as professionals may both be impacted by this specialization (Li et al., 2019). Subcultures can help personnel improve their expertise and expertise in particular facets of cybersecurity. For example, a subculture that emphasizes offensive cybersecurity methods might encourage its members to become knowledgeable in penetration testing and vulnerability assessment. This area of expertise may affect employees' paths to employment and their cybersecurity work for the company (Da Veiga & Martins, 2017).

How employees communicate about cybersecurity, internally and externally, might be influenced by subcultures. In turn, this can define how the subcultures perceive the importance of cybersecurity. Subcultures may resist change and impede the enactment of new cybersecurity procedures or technologies (Cram et al., 2020). Employees may be reluctant to adopt different methods or innovations if how employees communicate about cybersecurity, both internally and externally, organization's capacity to respond to new threats while implementing more effective cybersecurity measures may need to be improved by this aversion to change (Cram et al., 2020).

The professional development of cybersecurity employees might be affected by subcultures. Some subcultures could prioritize cybersecurity* as a vital component of corporate operations and push for more funding and resources. Others might take a more lenient approach, viewing cybersecurity as less critical for the organizations (Alshaikh, 2020). Furthermore, this can affect employee attitudes toward cybersecurity in their personal life. Some subcultures might prioritize long workdays and extreme devotion to cybersecurity tasks, while others may emphasize striking an appropriate time balance between work and life (Alshaikh, 2020). Employees who identify with a particular subculture may align their attitudes and behaviors with that subculture, affecting their general well-being and job happiness (Alshaikh, 2020).

Cybersecurity subcultures are essential because they influence how employees feel and act toward safety measures (Da Veiga & Martins, 2017). Employees are more likely to prioritize and adhere to cybersecurity procedures when subcultures promote a strong cybersecurity mindset, increasing defenses against digital assaults. Additionally, subcultures can promote a supportive and cooperative work atmosphere where employees actively share knowledge, report events, and keep abreast of new hazards. By working together, we can improve the organization's overall cybersecurity posture and lessen the possibility of successful cyberattacks (Da Veiga & Martins, 2017). To avoid any unfavorable impact on employee behavior or possible company conflicts, managers must ensure that employees adhere to ethical and legal requirements (Shaikh & Siponen, 2022).

According to Da Veiga and Martins, 2017, common factors that forms subcultures are:

**Departments:** Within an organization, different departments may have varying priorities and approaches toward cybersecurity. Such differences can result in the development of unique subcultures, where each group adheres to its own set of beliefs and practices related to cybersecurity (Da Veiga & Martins, 2017). For instance, a marketing department may prioritize safeguarding the company's brand image and reputation. In contrast, an engineering department may be more concerned about maintaining the confidentiality and integrity of the company's systems and data. To ensure adequate protection against cyber threats, the IT department must collaborate with the different subcultures within the organization. This collaboration may involve educating the other departments on the significance of cybersecurity, providing them with resources and training to implement adequate cybersecurity measures, and establishing clear policies and procedures that all must follow. By working together, the different departments can create a strong culture of cybersecurity that protects the organization from a wide range of cyber threats.

**Locations:** Having multiple office locations can create subcultures of cybersecurity within an organization due to variations in cybersecurity practices, policies, and procedures across different sites (Da Veiga & Martins, 2017). For instance, one office might have rigorous cybersecurity protocols, while another may not prioritize protecting sensitive information. These discrepancies can cause differences in attitudes and behaviors toward cybersecurity, which could affect the overall efficiency of the organization's cybersecurity measures. Furthermore, these subcultures may pose challenges in implementing and enforcing consistent cybersecurity policies throughout the organization.

**Identities:** Differences in employee identities such as age, gender, race, ethnicity, sexual orientation, and cultural background can lead to developing cybersecurity subcultures in organizations (Da Veiga & Martins, 2017). In addition, these differences can influence perspectives and priorities on cybersecurity, resulting in distinct subcultures within the organization. For instance, younger employees may be more familiar with new technologies, while older employees may prefer traditional working methods. Similarly, women may be more likely to report cybersecurity concerns, while men may prioritize completing tasks over cybersecurity. As organizations strive to promote a culture of cybersecurity, they must address these challenges to meet the needs of all employees.

In most organizations, the dominant cybersecurity culture coexists with various subcultures that have branched out from it, as discussed in (Da Veiga & Martins, 2017). The cybersecurity culture embodies the shared values, attitudes, and beliefs of cybersecurity, forming the basis for cybersecurity strategies (Uchendu et al., 2021). In addition, subcultures arise to address the unique needs of different departments or teams, developing their own cybersecurity practices and knowledge (Da Veiga & Martins, 2017). Despite having distinct approaches, subcultures are still interconnected with and influenced by the overarching cybersecurity culture. Recognizing and understanding these subcultures is crucial for effective cybersecurity management, as it enables tailored strategies while fostering collaboration and alignment with the organization's cybersecurity objectives (Da Veiga & Martins, 2017). This structure is illustrated in the following figure, model 2.2:

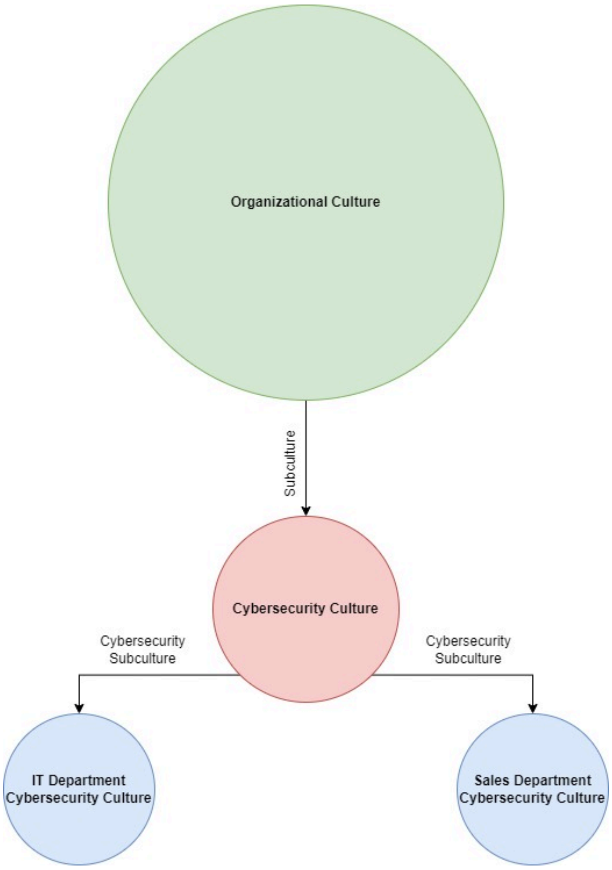


Figure 2.2: Organizational Cultures Illustration

### 2.2.3 Subculture Awareness & Compliance

To reduce cybersecurity concerns, it is crucial to understand the subcultures and their potential cybersecurity risks. In addition, the subculture tends to form its own views on awareness and compliance (Zwilling et al., 2022). Hence, it is essential to understand these concepts and how these perceptions can form among the employees.

Cybersecurity awareness refers to the degree to which personnel is aware of the importance of their organization's cybersecurity policies, rules, and guidelines and the degree to which they comply with these policies, regulations, and procedures (Uchendu et al., 2021). In an ideal cybersecurity subculture, awareness is prioritized, and people are actively involved in training. They are following best practices and remaining vigilant against potential threats. These subcultures understand the significance of safeguarding sensitive data for the organization and its customers. They regularly hold discussions, forums, and dedicated resources to share information, report incidents, and address cybersecurity concerns (Li et al., 2019). On the other hand, some subcultures need more proper knowledge and interest in cybersecurity practices, resulting in low cybersecurity awareness Wiley et al., 2020. This could lead to them underestimating the risks and consequences of cyber threats, making the organization vulnerable to attacks.

When employees in cybersecurity subcultures within organizations choose to handle compliance on their own, it can result in significant consequences (Donalds & Osei-Bryson, 2019). This decentralized approach can cause inconsistencies and gaps in cybersecurity practices across the organization Cram et al., 2020. Without a unified and standardized approach, employees may adopt varying levels of adherence to cybersecurity policies and procedures, leading to a fragmented cybersecurity posture (Da Veiga & Martins, 2017). This can create vulnerabilities and increase the risk of cybersecurity breaches, as certain employees may unknowingly engage in risky behaviors or neglect essential cybersecurity measures.

Furthermore, employees taking their own approach to compliance can hinder effective risk management and oversight. For example, when individuals decide how to comply with cybersecurity requirements, it becomes challenging for organizations to assess and monitor their overall cybersecurity posture accurately (Wiley et al., 2020). This lack of visibility can impede the identification of potential weaknesses or non-compliance issues, making it easier to implement appropriate controls and mitigate risks effectively. It also complicates conducting audits or demonstrating regulatory compliance, as there may be a need for more documentation or evidence of consistent cybersecurity practices (Cram et al., 2020).

## 2.3 Theoretical Conclusions

The theoretical conclusions drawn from investigating cybersecurity culture and its subcultures through a systematic literature review suggest that subcultures within organizations play a significant role in shaping cybersecurity practices and awareness. Furthermore, these subcultures can influence how individuals perceive, prioritize, and engage with cybersecurity measures, ultimately impacting the organization's cybersecurity posture.

Based on theoretical research, organizations must establish a solid and pervasive cybersecurity culture to practice cybersecurity effectively. This culture involves individuals' collective beliefs, attitudes, and behaviors toward cyber security, emphasizing the shared responsibility of safeguarding digital assets. Organizations can enhance awareness, encourage proactive cybersecurity measures, and create a strong defense against cyber threats by promoting a culture that values cybersecurity. This emphasizes creating a cybersecurity-conscious environment integrating cybersecurity into all operations, decision-making processes, and employee behavior.

Cybersecurity subcultures can both facilitate and hinder cybersecurity awareness. When subcultures promote a strong cybersecurity mindset, foster information sharing, and encourage proactive cybersecurity practices, individuals are more likely to prioritize and actively engage in cybersecurity measures. On the other hand, subcultures that lack awareness or downplay the importance of cybersecurity may create a complacent attitude, leaving the organization vulnerable to cyber threats. Furthermore, if cybersecurity awareness is high in certain subcultures, it can act as a catalyst for spreading best practices and raising awareness in other subcultures. Conversely, if there is a need for cybersecurity awareness in influential subcultures, it can impede the adoption of cybersecurity measures throughout the organization.

Overall, the theoretical conclusions from cybersecurity subculture literature emphasize the importance of understanding and addressing subcultures within organizations to enhance cybersecurity awareness and practices effectively. By recognizing the role of subcultures and implementing strategies to foster a culture of cybersecurity, organizations can better protect themselves against cyber threats.

Once the theoretical investigations were completed, a model was developed to demonstrate the formation and functionality of cybersecurity cultures. This framework is derived from an illustration presented by Keman and Pearlson, 2019. This framework explains how cybersecurity is influenced by and can influence other factors, including the overall cybersecurity culture. It also explores how the subculture's perception of the cybersecurity culture can shape employees' behavior and practices toward cybersecurity. The framework that was produced as a result of the systematic literature review is illustrated in figure 2.3:

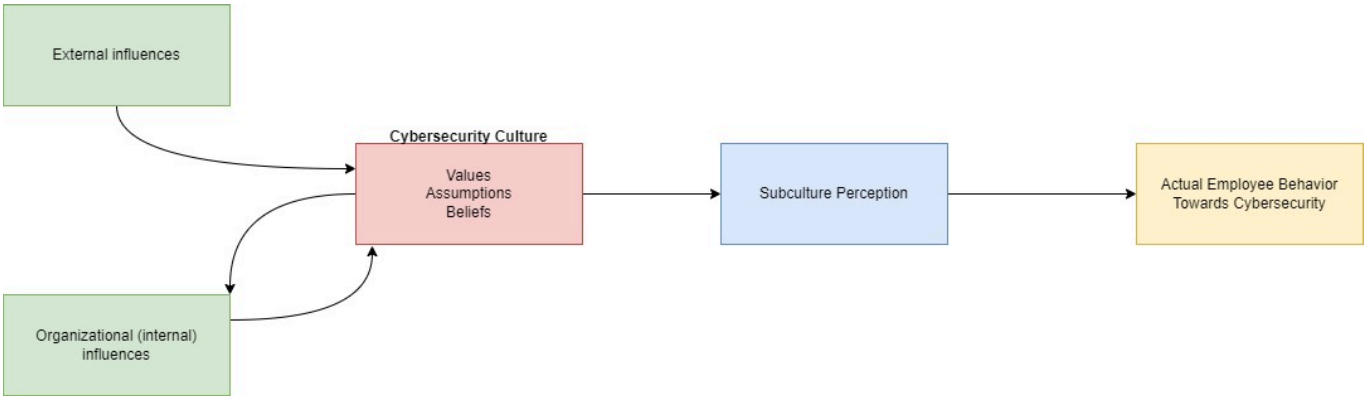


Figure 2.3: Conceptual Framework for Cybersecurity Subcultures. Inspired by (Keman & Pearlson, 2019).

### 2.3.1 Research Gap

A gap in research exists regarding the subcultures within the field of cybersecurity. While there is a considerable amount of research on cybersecurity culture as a whole, there needs to be more exploration of the potential cybersecurity subcultures that may exist within organizations. Current data on cybersecurity culture typically focuses on broad themes such as awareness, training, policies, and organizational practices. However, there needs to be more investigation into the unique subcultures that may exist within various departments, teams, or locations. When doing this systematic literature review, it was only Da Veiga and Martins, 2017 that specifically investigated the subcultures, which points to a significant lack of existing theory around the topic. This lack of information is concerning, as the subcultures can significantly impact shaping individuals' attitudes, behaviors, and motivations toward cybersecurity.

Understanding the nuances of cybersecurity subcultures is crucial to develop targeted interventions, strategies, and policies that align with the specific cultural dynamics within organizations or communities. By examining subcultures, variations in beliefs, norms, and values related to cybersecurity can be uncovered, providing insights into how different groups approach and perceive cybersecurity practices. Closing this research gap would allow for a more comprehensive understanding of the intricate social dynamics within cybersecurity domains, enabling the development of more effective and tailored approaches to enhance cybersecurity. Therefore, this research aims to investigate the meaning and impact of cybersecurity subcultures thoroughly.

# Chapter 3

# Methodology

This chapter will justify the methodical decisions and approaches taken in the research project. It will also present the details of the data-gathering process.

## 3.1 Qualitative Case Study

Research has established that quantitative studies are a reliable research approach when investigating cybersecurity culture. Given the complexity of this research topic, selecting an appropriate methodology was crucial. To supplement and expand on this research, a qualitative approach to a comparative case study was deemed necessary. Case studies are utilized to research a specific area within its context (McCombes, 2019). The research will explore and evaluate the level of cybersecurity awareness among various subcultures, and this approach combination has hence been considered appropriate. Qualitative case studies enable the use of multiple data collection methods, and interviews will be conducted with cybersecurity leaders and employees from the subcultures. (Fossey et al., 2002). It is worth noting that qualitative case studies require me to possess complex personal skills such as asking good questions, being a good listener, and staying adaptive, all within an ethical framework.

Initially, there was a consideration to use quantitative analysis as the main research method. This involved gathering data through quantity rather than quality (McLeod, 2023). An alternative plan could have been to reach out to more employees from various organizations in the holding company to investigate cybersecurity subcultures on a wider scale. Surveys would have been sent out to all participants to collect data. This research approach would have provided a surface-level impression of how employees view cybersecurity subcultures. The collected data could have been used to create statistical models that highlight general opinions throughout the holding company. However, this approach was dismissed early on in the process, as a qualitative analysis would provide a deeper understanding of the topic. Semi-structured interviews with employees in the cybersecurity subcultures will facilitate open conversations about the topic and allow me, as a researcher, to delve deeper into their perceptions of cybersecurity compared to a quantitative approach (McLeod, 2023).

## 3.2 Systematic Literature Review Methodology

A literature review seeks to understand and examine existing theoretical perspectives on a specific topic, with the research question as a guideline for the process. It involves thoroughly searching for and evaluating academic articles, books, journals, conference papers, and other relevant literature sources to identify the topic's current theoretical state. The literature review also aims to uncover knowledge gaps and areas that could be subject to further research (Fund, 2023). As a result, it helps support claims that the thesis topic is relevant and underlines that it will provide new knowledge to the area. There are several possible ways to conduct a literature review, but a systematic literature review will be conducted for this specific instance, if you don't mind. The steps taken to conduct the systematic literature review are based on the "Process of the systematic literature review" (Xiao & Watson, 2019), which can be seen in section 3.2.

As previously explained, a literature review process can involve a wide range of theoretical sources. However, only journals were used in this instance. Journals are more likely to be peer-reviewed, which helps increase the overall quality and reliability. Furthermore, due to the rapidly evolving nature of this topic, the search area was limited to a 10-year period (i.e., 2013-2023) to avoid outdated and irrelevant sources of information. Both of these criteria are measures taken to uphold the literature review's overall quality and relevance. Further inclusion and exclusion criteria will be explained in section 3.2.2.

For this particular project, a systematic literature review was conducted. The systematic literature review aims to provide an objective and comprehensive summary of the existing evidence on a particular topic (Xiao & Watson, 2019). The model found in "Guidance on Conducting a Systematic Literature Review" by Xiao and Watson, 2019 will be used to conduct the systematic literature review. The article describes a systematic literature review as a research method that involves a rigorous and comprehensive search for relevant studies, followed by a critical appraisal and synthesis of their findings.

A systematic literature review aims to provide an objective and comprehensive summary of the existing evidence on a particular topic. The model found in "Guidance on Conducting a Systematic Literature Review" (Xiao & Watson, 2019) will be utilized to conduct the systematic literature review. The article describes a systematic literature review as a research method that involves a rigorous and comprehensive search for relevant studies, followed by a critical appraisal and synthesis of their findings.

Xiao & Watson (Xiao & Watson, 2019) describe that a successful systematic literature review consists of several phases and steps that must be planned and followed. The three phases that the process is made up of are: planning the review, conducting the review, and reporting the review. These three stages involve eight steps: (1) formulating the problem, (2) developing and validating the review protocol, (3) searching the literature, (4) screening for inclusion, (5) assessing quality, (6) extracting data, (7) analyzing and synthesizing data and (8) reporting findings. Figure 3.2 illustrates the steps and phases that the methodology consists of:

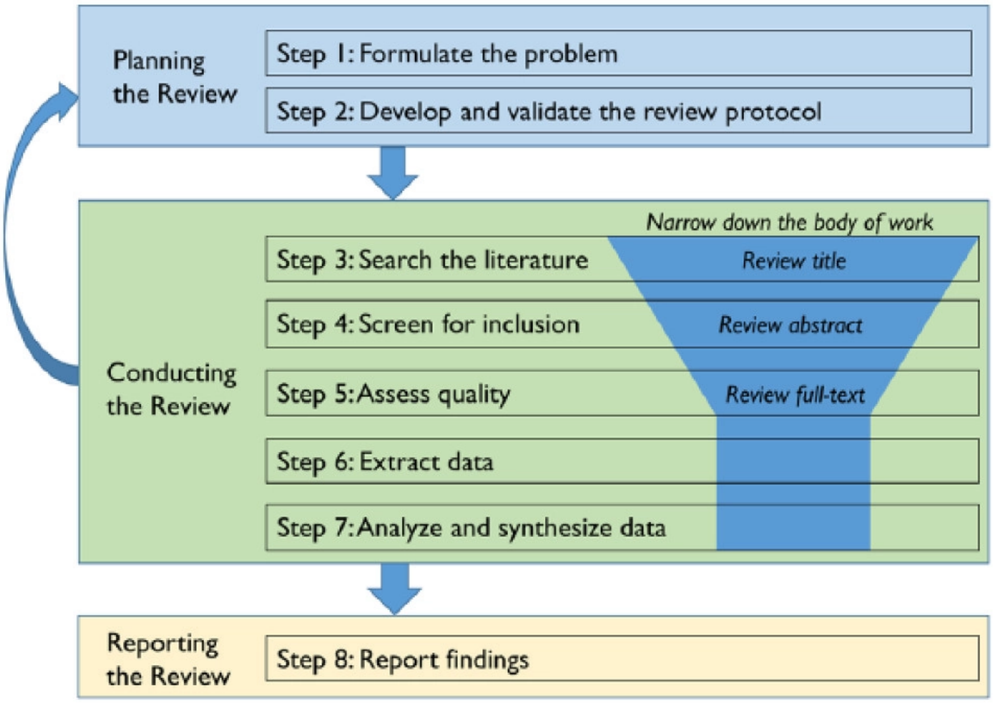

Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Conducting the Review
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings

Figure 3.1: SLR process model (Xiao & Watson, 2019)

### 3.2.1 Formulate the Research Problem

The full extent of the research problem and the research questions has already been presented in chapter 1.1. In short, this qualitative case study seeks to identify the differences in awareness and compliance between subcultures within the partner organizations and measure the state of their overall cybersecurity culture.

### 3.2.2 Develop and Validate the Review Protocol

According to Xiao and Watson, 2019, the review protocol should "describe all the elements of the review, including the purpose of the study, research questions, inclusion criteria, search strategies, quality assessment criteria, screening procedures, strategies for data extraction, synthesis, and reporting" (Xiao & Watson, 2019). Following each step of a clearly validated review protocol is essential for maintaining the overall quality of the literature review. In this case, the review protocol that will be utilized is the systematic literature review model described in section 3.2.

#### Inclusion and Exclusion Criteria

Having clearly defined inclusion and exclusion criteria when searching and reviewing the literature is crucial for maintaining the overall quality of the literature review (Xiao & Watson, 2019). It also helps narrow the search area, meaning more time can be spent reviewing relevant literature. Below are lists describing the inclusion and exclusion criteria I decided to implement for the systematic literature review:

**Inclusion Criteria:**

- Research material: Journal
- Publication year: After 2013
- Language: English

- Content: Relevant to the research questions
- Availability: Open or accessible through the institution

**Exclusion Criteria:**

- Research material: Other material than journals, e.g., conference papers or blogs
- Content: Irrelevant to the research questions
- Availability: Locked behind a paywall or other access restrictions
- Publication year: Before 2013
- Language: Other languages than English

As previously mentioned, it was decided to only fully review journals in this research as they have a higher chance of being peer-reviewed. This usually results in a higher overall quality of the literature, as it is more likely that the information it provides is recognized and correct. As cybersecurity culture is a relatively quickly evolving topic, it was also decided to use data from the last ten years to get the most relevant information out of the literature. A lot of literature did not fulfill these criteria and was hence left out from further processing.

### 3.2.3 Searching the Literature

The digital databases searched during the literature review were Google Scholar and Research Gate. To find literature related to the topic of cybersecurity subcultures in organizations, I first conducted a broad search. Then, I used the following steps of the model to narrow down the results. The specific search keywords I used were "cybersecurity subcultures in organizations" and "employee behavior and awareness in cybersecurity subcultures."

### 3.2.4 Screen for Inclusion

Once the literature search was conducted and the exclusion and inclusion criteria were applied, the screening process could begin. The systematic literature review screening process consists of multiple stages to identify relevant studies for inclusion in the review (Xiao & Watson, 2019). It is a crucial step in the systematic literature review as it determines which studies should be thoroughly read and examined for inclusion in the final list of articles (Xiao & Watson, 2019). The screening process began by collecting records from preliminary research, removing duplicates, and applying inclusion and exclusion criteria. I was left with 102 records that needed to be screened. The following step was to begin eliminating irrelevant articles by following this procedure:

- Reading the title and the abstract, and additional chapters if necessary (i.e conclusion)
- Briefly checking the relevancy of content
- Checking if the author(s) are credible and reliable

Through the screening process, the original 102 articles were narrowed down to a selection of 21 articles to be further processed. The next stage involves conducting a full-text reading to determine the articles' relevancy and eligibility. The purpose of this final step in the screening process is to systematically identify and choose studies that align with the review's objectives, ensuring that the final selected studies are suitable for analysis and synthesis (Xiao & Watson, 2019). In model 3.2, the illustration demonstrates the complete process of conducting the screening procedure:

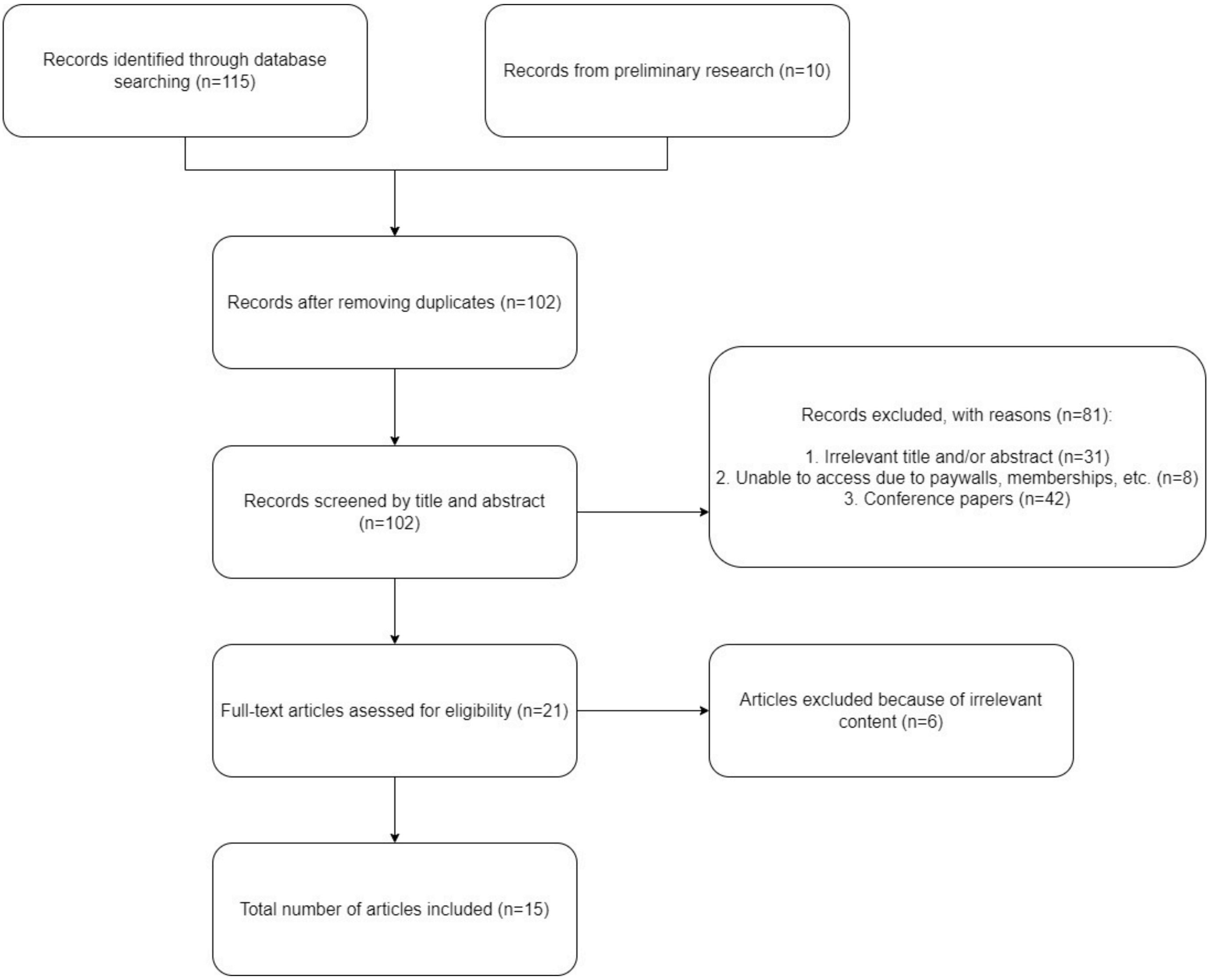

Records identified through database searching (n=115)
Records from preliminary research (n=10)
Records after removing duplicates (n=102)
Records screened by title and abstract (n=102)
Records excluded, with reasons (n=81):
1. Irrelevant title and/or abstract (n=31)
2. Unable to access due to paywalls, memberships, etc. (n=8)
3. Conference papers (n=42)
Full-text articles asessed for eligibility (n=21)
Articles excluded because of irrelevant content (n=6)
Total number of articles included (n=15)

Figure 3.2: Final systematic literature review

### 3.2.5 Selected Literature

The articles 15 articles listed in the table below are the result of the search and evaluation conducted through the systematic literature review:

| No. | Title | Journal | Research Method | Year | In-Text Citation |
|---|---|---|---|---|---|
| 1. | Developing a cybersecurity culture: Current practices and future needs. | Computers & Security | Qualitative | 2021 | (Uchendu et al., 2021) |
| 2. | Developing cybersecurity culture to influence employee behavior: A practice perspective | Computers & Security | Interpretive | 2020 | (Alshaikh, 2020) |
| 3. | More than the individual: Examining the relationship between culture and cybersecurity Awareness. | Computers & Security | Quantitative | 2020 | (Wiley et al., 2020) |
| 4. | Defining and identifying dominant cybersecurity cultures and subcultures | Computers & Security | Quantitative | 2017 | (Da Veiga & Martins, 2017) |
| 5. | The effect of perceived organizational culture on employees' cybersecurity compliance | Information and Computer Security | Quantitative | 2021 | (Karlsson et al., 2021) |
| 6. | Maximizing Employee Compliance with Cybersecurity Policies | MIS Quarterly Executive Vol 19. Iss.3 | Quantitative | 2020 | (Cram et al., 2020) |
| 7. | Neutralization: New Insights Into the Problem of Information Systems Security Policy Violations | MIS Quarterly Vol. 34, No. 3 | Qualitative and Quantitative | 2010 | (Siponen & Vance, 2010) |
| 8. | Defining organisational information security culture — Perspectives from academia and industry | Computers & Security | Qualitative and Quantitative | 2020 | (Da Veiga et al., 2020) |
| 9. | Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behaviour | International Journal of Information Management | Quantitative | 2019 | (Li et al., 2019) |
| 10. | Cybersecurity risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity | Computers & Security Journal | Quantitative | 2022 | (Shaikh & Siponen, 2022) |
| 11. | Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents | International Journal of Information Management | Quantitative | 2019 | (Donalds & Osei-Bryson, 2019) |
| 12. | Implementing a Cybersecurity Culture | CA Journal Vol.2 | Qualitative | 2019 | (Alvarez-Dionisi & Urrego-Baquero, 2019) |
| 13. | A Cyber-Security Culture Framework for Assessing Organization Readiness | Journal of Computer Information Systems | Qualitative | 2022 | (Georgiadou et al., 2022) |
| 14. | Organizational structure and safety culture: Conceptual and practical challenges | Safety Science 126 | Qualitative | 2020 | (Schulman, 2020) |
| 15. | Cybersecurity Awareness, Knowledge and Behavior: A Comparative Study | Journal of Computer Information Systems | Quantitative | 2022 | (Zwilling et al., 2022) |

## 3.3 Data Collection

This section will describe how the data collection was done for the project after the finished literature review. This study utilized semi-structured interviews with 10 participants as the primary data collection method. Semi-structured interviews are particularly advantageous in qualitative research (Baxter & Jack, 2010), as they perfectly balance structure and flexibility. Unlike structured interviews, which rely on predetermined questions, semi-structured interviews allow for open-ended questions and follow-up probes, allowing for a more in-depth exploration of participants' responses (Baxter & Jack, 2010). This flexibility also enables interviewers to pursue unexpected lines of inquiry and obtain rich and nuanced data, as participants can express their thoughts and experiences in their own words.

Semi-structured interviews prioritize participants' voices, taking a participant-centered approach that recognizes their perspectives and experiences (Medelyan, 2023b). Participants have the freedom to steer the conversation based on their views, which creates a more collaborative and reciprocal relationship between the interviewer and the participant. This approach fosters trust and discussion, involving a dialogue rather than a one-sided interrogation. Moreover, semi-structured interviews are beneficial for exploring complex and sensitive topics. They provide a safe space for participants to share their thoughts, beliefs, and experiences at their own pace and comfort level, ensuring ethical considerations and respecting participants' boundaries (Baxter & Jack, 2010). With this method, interview participants can provide sensitive or personal information that they may not have shared otherwise. The following parts of the report will describe the data collection process in detail and tell the interviewed companies and employee participants.

### 3.3.1 Interview Participants

The interview participants were obtained from two different organizations. These organizations agreed with me to collaborate through the research project and intend to use the results to improve their operations. To ensure that these investigations cannot be linked to individuals, the companies will be anonymized and referred to as Company A and Company B throughout the thesis. Both organizations are IT companies that want to implement a significant investment in cybersecurity, and both are part of the same holding company. Below is a table with brief descriptions of each of the companies:

| Company | Size | Description |
|---|---|---|
| Company A | Medium: >100 employees | Company A has offices throughout Norway, with tasks distributed across departments, such as customer service, sales, and IT. The company specializes in developing IT systems for the public sector, and their most used systems are utilized for public document management. |
| Company B | Medium: >70 employees | Company B operates from its Bergen and Oslo offices. Their core expertise lies in designing IT systems for both public and private sectors. Their most prevalent system is utilized for storing and administering property documents. |

Table 3.1: Partnering Organizations

Both companies work in the IT sector and utilize digital systems in most operations. Although they have slightly different focus areas, both deal with much information in their work. Therefore, the initial interviews were conducted with cybersecurity leaders from both companies. The aim was to gain their perspective on cybersecurity and identify the subcultures with the most notable differences in knowledge and awareness. During the research process, both leaders agreed that the differences between the sales and IT cybersecurity subcultures were the most significant. This led to eight employees from the subcultures agreeing to participate in the interviews, in addition to the two previously mentioned security leaders.

| Employee Pseudonym | Company | Role | Years in role |
|---|---|---|---|
| Security Lead A | Company A | Chief Information Security Officer | 1 year |
| Security Lead B | Company B | Cybersecurity Leader | 5 years |
| IT Employee A | Company A | Senior Developer | 5 years |
| IT Employee B | Company A | Cloud Engineer | 3 years |
| IT Employee C | Company B | Senior Developer | 4 years |
| IT Employee D | Company B | Senior Developer | 5 years |
| Sales Employee A | Company A | Key Account Manager | 4 years |
| Sales Employee B | Company A | Customer Relations | 1 year |
| Sales Employee C | Company B | Sales Consultant | 3 years |
| Sales Employee D | Company B | Customer Relations | 3 years |

Table 3.2: Interview Participants

As shown in the table, it is clear that the interview participants possess distinct experiences and backgrounds. Nevertheless, their valuable feedback will aid in the research study and enable a comparison of both companies and subcultures, providing insight into the perceived cybersecurity within these subcultures.

### 3.3.2 Interviews

Qualitative case studies benefit significantly from semi-structured interviews, offering a flexible and comprehensive approach to gathering detailed and nuanced data. Semi-structured interviews allow me to maintain a certain level of the structure by using an interview guide with pre-determined questions while allowing participants to elaborate on their experiences and perspectives freely. In addition, this approach ensures consistency across interviews, making it easier to compare responses and identify common themes while providing an open-ended platform for participants to express their thoughts and provide unique insights.

As part of the initial research project, I interviewed Security Lead A and Security B. Towards the end of the interview, I asked them about the subcultures they believed had the most significant disparity in cybersecurity knowledge and awareness. They both individually identified the sales and IT cybersecurity subcultures as the most different. In addition, they connected me with two employees from these subcultures in their respective companies to further explore this.

The purpose of the interviews is to understand how different subcultures view cybersecurity. To accomplish this, the interview must be well-structured to gather valuable information and contribute to discussions during the semi-structured interviews. Therefore, the questions were designed to explore the subcultures' values, assumptions, and beliefs. The model below outlines the interview structure and the questions developed to obtain answers to specific areas of focus:

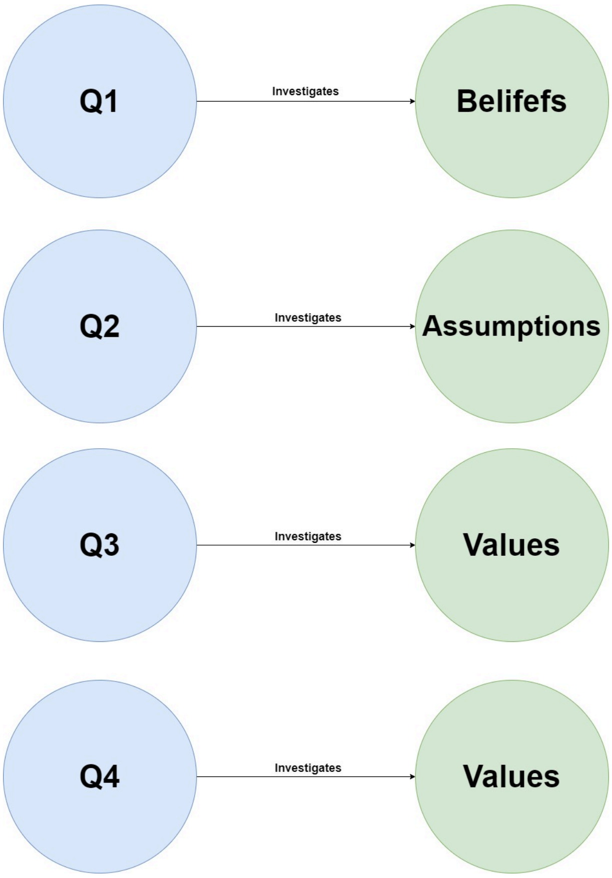


Figure 3.3: Interview Questions Structure

An important fact to note is that both companies belong to the same holding company. To strengthen their defenses against cyber threats, the partner companies can collaborate by adopting standard policies, procedures, and guidelines that align with industry best practices and regulatory requirements. They can also share threat intelligence and conduct joint risk assessments. In addition, regular training and awareness programs can be organized to educate employees from both companies on cybersecurity best practices and foster a culture ofcybersecurity awareness. This may result in similar cybersecurity practices among employees and potentially similar interview answers. However, employee perceptions can also differentiate even though they may share many standard procedures.

### 3.3.3 Ethical Considerations

When conducting a study that involves gathering data from people, it is crucial to prioritize ethical considerations during the data collection. In addition, the participants will be sharing a significant amount of personal information during the interviews, making it even more critical for me as a researcher to treat them with respect and dignity throughout the process. To incorporate established data processing practices into my research, I've opted to utilize Oates, 2006 ethical guidelines:

**Right to withdraw:** The interview participants were informed that they could withdraw from the research project at any time, even after the interview has been completed, if they change their minds.

**Right to give informed consent:** At the start of the interviews, the interview participants are asked if they have read through the information letter they have received in advance. The interview can start if they give verbal consent that they have understood this information.

**Right to anonymity:** The interview participants will remain anonymous and given a pseudonym. The companies they work for will also be anonymized.

**Right to confidentiality:**: The interview participants were informed that the data collected would be kept confidentially and securely stored.

After getting the contact information of the employees who had agreed to be interviewed, I sent out an information letter which can be seen in Appendix B. Here they received information about the interview and how their answers will be used further in the research. Before the discussions started, I submitted my Data Management Plan (DMP) to the Norwegian Centre for Research Data (NSD). In the DMP, I stated how the data was to be processed, where it was to be stored, and which guidelines the data collection was to follow. This plan was approved by NSD and sent out as an attachment with the information letter so that the interview participants could feel confident that their data was being processed securely. The DMP submission form and the subsequent approval from NSD can be found respectively in Appendix E and Appendix D.

### 3.3.4 Data Analysis

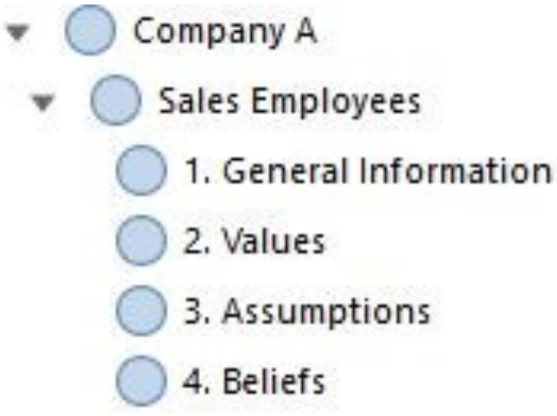
In a qualitative case study, analyzing data typically involves reviewing transcripts created from audio recordings of interviews (Fossey et al., 2002). In-depth and detailed information is gathered from the interviews and recorded in transcripts, providing valuable insights into the subcultures' perspectives and experiences on cybersecurity. By analyzing these transcripts systematically, patterns, themes, and connections within the data can be identified. This will lead to a more contextual and meaningful understanding of the research topic. The transcripts also help to give me an idea of divergent or contradictory viewpoints, contributing to a more comprehensive exploration of the data. Finally, this rigorous approach ensures the reliability and validity of the findings.

This study aims to compare the cybersecurity subcultures in different organizations through a comparative case study. The analysis process will utilize a thematic analysis to enhance the research process. This involves selecting and analyzing multiple cases or organizations to identify common themes or patterns within a specific research topic. This study focuses on comparing and contrasting the findings from various points to gain a deeper understanding of cybersecurity subcultures within organizations. I conducted semi-structured interviews with employees from Company A and Company B. The interviews provided valuable insights into the cybersecurity subcultures within the sales and IT departments of both companies. The data collected from these interviews were analyzed using thematic analysis to identify recurring themes or patterns within the qualitative data.

Thematic analysis helps to identify and categorize critical factors that influence the cybersecurity subcultures in each organization. By comparing the findings from the two companies, similarities and differences in the subcultures could be identified. This comparative approach provides a comprehensive understanding of the cybersecurity practices, knowledge, attitudes, and responsibilities within both organizations' sales and IT departments The thematic analysis also helps highlight areas where improvements can be made to strengthen the overall cybersecurity culture within each company (Crosley, 2021). This study provides valuable insights into the cybersecurity subcultures and contributes to the existing knowledge in the field.

The first step in the process is transcribing the interviews, which involves transforming spoken content into written form. To achieve this, each interview was audio recorded with consent from the interview participants. As the interviews were conducted digitally, I utilized software that automatically transcribed the conversation as the discussions progressed. However, to ensure the quality and readability of the transcripts, I manually went through generated transcripts by listening to the audio from the interviews. I corrected any mistakes or added missing information. Going through the transcripts and listening to the audio also helped me familiarize myself with the content of the interviews.

Once the transcripts are completed, the next step is coding. This involves manually categorizing and organizing the transcripted data to identify themes and sub-themes. The goal is to uncover commonalities, differences, and significant insights within the data. During the coding process, I reviewed each of the individual transcripts and assigned codes to data segments representing meaningful concepts or ideas. These codes could be descriptive, interpretive, or conceptual, capturing the content's essence. I compared and contrasted codes as coding progressed, looking for connections and relationships between different transcripts. This helped identify overarching themes, sub-themes, or patterns from the data. This is especially advantageous in comparative analyses, as it enables easy comparison of transcriptions through code navigation. During the process, I utilized a software called Nvivo 12. This is a widely recognized and extensively used program for conducting qualitative studies and was ideal for my data analysis process. The example illustrated in figure 3.4 demonstrates how a typical set of nodes were set up, in this case, for the Sales Employees of Company A.



- Company A
  - Sales Employees
    - 1. General Information
    - 2. Values
    - 3. Assumptions
    - 4. Beliefs

Figure 3.4: Example of Transcription Coding in Company A

I will synthesize and interpret the coded data in the final analysis phase to develop meaningful insights and draw conclusions. I will examine the relationships between codes and themes, looking for explanations, interpretations, and theoretical implications. The findings will often be supported by relevant quotes or examples from the transcripts, providing evidence to support the interpretations. This data analysis process in a qualitative case study allows for a deep exploration of the interviews, providing comprehensive and detailed insights into cybersecurity subcultures.

# Chapter 4

# Findings

This chapter will describe the main findings from the interviews. These interviews were recorded and subsequently transcribed. For more accessible analysis, the transcriptions were then coded into themes and sub-themes. The purpose is to present the employees' perceptions of their attitude to cybersecurity and to find out what kind of differences among the employees regarding knowledge, assumptions, and knowledge. In conclusion, the findings will be compared in separate tables for a more accessible overview of the findings between the companies and the subcultures. The interview guides for the management and employees are in Appendix A and B.

## 4.1 Management Input

The first round of interviews was done with managers from each company. Emphasis was also placed on both managers having cybersecurity as their area of responsibility. The leaders were not interviewed to be compared as a subculture but rather to get their perspective on what they think their company's cybersecurity culture is like, which actions they are taking to improve their company's cybersecurity, and most importantly, to get them to identify which subcultures differ the most so that these can be interviewed further. The leaders were also beneficial in putting me in contact with the interviewees from the identified subcultures. This sub-chapter will describe the findings from the interviews with both security managers.

### Company A

The first interview was conducted with the Chief Information Security Officer (CISO) of Company A. This person will be referred to by the pseudonym Security Lead A throughout the chapter. The CISO has vast experience in both the organization and the IT industry. However, the company has recently appointed Security Lead A to this role to prioritize cybersecurity. The new responsibility of Security Lead A extends beyond Company A and encompasses the entire holding company, including Company B. This means that Security Lead A is accountable for overseeing the cybersecurity practices of several companies, despite being located in Company A.

Company A recognizes that its employees' human error and lack of cybersecurity beliefs are crucial factors that must be addressed to enhance the organization's cybersecurity. When asked about the most common risks, Security Lead A identifies phishing as a severe problem and highlights that employees often use work-related and private services interchangeably:

> *"We will spend a lot of time sending out test phishing emails to the employees and trying to teach them not to click on them in the future. We have a service that is good at filtering out*

*phishing, but it always appears in some cases and especially because people use their private e-mails and services on the same PC or mobile phone as they carry out their work tasks".*

According to Security Lead A, efforts have been made to enhance cybersecurity awareness and beliefs among employees across different departments. This is achieved through nano learning, which involves distributing short and focused learning materials throughout the year to allow employees to integrate them into their daily work. The company recognizes the significance of raising awareness and fostering a solid attitude toward cybersecurity among its employees. Furthermore, Security Lead A emphasized that transparency is a core value in their cybersecurity culture:

> *"We must run a very open and blameless policy around mistakes. I always encourage this in my communication with the employees. If you are in doubt about handling something or whether you have made a mistake, we want to hear about it as soon as possible, especially in relation to cybersecurity. Everyone makes mistakes, so if they report it, it's much better because we can find the cause and deal with it immediately."*

During the interview's conclusion, Security Lead A was asked which subcultures exhibit the most significant divergence in beliefs and attitudes toward cybersecurity. In response, the manager specified that the sales and IT departments have the most substantial differences. Convincing sales personnel of the significance of cybersecurity is often more challenging than it is for the IT employees. Furthermore, the IT employees has more extensive knowledge and awareness of potential threats that may harm them.

**Company B**

The other manager interviewed is Cybersecurity Leader in Company B and will be referred to by the pseudonym Security Lead B. The person has five years of experience in this role and is responsible for cybersecurity in the company. In addition to this responsibility, Security Lead B is also head of development. In contrast to Company A, which tries to emphasize transparency through dialogue with management, Company B instead encourages an organized platform where employees can share cybersecurity concerns:

> *"We have implemented a measure called the "Security Council" in our organization. At least one representative from each development team meets regularly to exchange knowledge and challenges regarding cybersecurity [...]. This is an important measure to ensure transparency among the teams in our organization."*

According to Security Lead B, Company B faces a significant challenge in raising cybersecurity awareness among its employees. Unfortunately, the resources allocated to this task are limited due to time constraints and differing priorities. Recognizing that employees are focused on generating profits and that their work takes precedence, the Security Lead acknowledges that cybersecurity education is not a top priority. However, they are committed to changing this and have implemented a solution. Fixed course days have been set aside throughout the year to provide all employees with insights into the significance of cybersecurity. In addition, the Security Lead actively participates in these events:

> *"I often give lessons in cybersecurity at the course days we hold for our employees. I emphasize the importance of cybersecurity and getting the right mindset. Why should we think about cybersecurity in what we do? Why should we not click on a suspicious e-mail that arrives in the inbox? I ask the employees these questions and try to explain to make them think that their actions may have consequences for cybersecurity."*

When concluding the interview, Security Lead B was asked to identify subcultures that showed the most significant differences so that they could be further investigated. They must know Security Lead A's response to the same question. However, Security Lead B also emphasized that the cybersecurity subcultures of the sales and IT departments differ significantly regarding beliefs and assumptions toward cybersecurity. The leader highlighted that this is mainly due to the sales department's inclination towards simplicity:

> *"They want to deal with simple tools and have as quick access as possible. They don't want to be confused by password changes and don't quite see why connecting to hotel or airport internet can be dangerous when traveling. Simplicity is prioritized over cybersecurity, which can pose a major risk."*

Lastly, Security Lead at Company B emphasizes the efforts made to enhance their cybersecurity culture. They want to work towards implementing cybersecurity awareness and compliance in all company areas and hope this mindset is reflected in other departments. However, the leader acknowledges that although they try to share knowledge, they have other responsibilities besides cybersecurity that require attention. Therefore, ensuring everyone remains informed and aware of cybersecurity can pose a significant challenge.

## 4.2 Empirical Findings - Employees

During the initial round of interviews, leaders from both organizations agreed that the Sales and IT departments' cybersecurity subcultures differ significantly in their beliefs about cybersecurity. Therefore, interviews were conducted with employees from both subcultures in both companies. The security managers were accommodating in quickly putting me in contact with the interviewees and expressed an eager interest in having this topic investigated. The interviews also took place digitally, as many participants are located in different cities across Norway.

The upcoming chapter will unveil noteworthy and sometimes unexpected discoveries that were made. Investigating the employee cybersecurity subcultures is the main objective of the research, and these interviews will provide valuable insights and analyze whether the cybersecurity measures described by Security Leads A and B are influential among the employees or not. I found the interviewees very honest and open, as they were told they would remain anonymous throughout the project. However, they needed to be bold in highlighting both positive and negative aspects of their respective organizations and wanted to help their organizations improve their cybersecurity culture.

### 4.2.1 Investigating the Sales Department Cybersecurity Subcultures

The first subculture examined was the cybersecurity culture of the sales departments. With the unwavering support and guidance of Security Leads A and B, I could contact employees from their companies and plan interviews with each of them. As previously mentioned, both Security Leads agreed that the sales department is one of the weaker subcultures regarding cybersecurity. Therefore, this part of the report will describe the findings from the Sales Employee interviews in Company A and Company B.

**Company A**

From Company A, Sales Employee A and Sales Employee B were interviewed. Sales Employee A works as a Key Account Manager at Company A, with four years of experience in this role. Sales Employee B is a Customer Relations representative within the same company and has been in the position for one year. The differing roles and experiences of the interviewees may result in interesting and diverse outcomes.

One of the topics discussed was the employees' perception of their organizational cybersecurity culture. Sales Employee A, who had previously worked in a larger organization with 12,000 employees, shared that working in a smaller company can positively impact cybersecurity culture. The employee expressed that it's easier to communicate openly and honestly with fewer people, resulting in a more conducive environment for discussing cybersecurity issues. They also noted that since everyone is usually in the office, it's more convenient to talk to colleagues, which makes them feel more secure and comfortable. Comparing it to their previous job, they highlighted that reporting errors were a much more complicated and lengthy process due to the organization's size and structure.

It is evident that Sales Employee A prefers a more open and flat cybersecurity culture, where reporting errors and problems is more straightforward and less complicated. The structure utilized at their previous workplace made it more challenging to come forward with critical messages in their previous job, which required going through several stages. Sales Employee A now appreciates Company A's more open and accessible structure. However, Sales Employee B does not share this perception of openness within the company:

*"I want to say that where I come from, which was a debt collection company, it was easier to get answers to things I wondered about. It seems that we have a culture of "companies within companies" here, which makes it harder to connect with other teams who are too focused on their tasks. In particular, I believe that the IT department could benefit from sharing their expertise with the rest of us and being more accessible for questions".*

When discussing cybersecurity, it becomes evident that Company A needs to make more effort to hold its employees updated on cybersecurity and needs to do more to maintain a strong cybersecurity culture of awareness and compliance. Both employees agreed there were concerns about cybersecurity and a lack of commitment to the topic in the past. However, Sales Employee A states things have changed since Security Lead A was promoted to Chief Security Officer. They emphasize that having a dedicated manager focused on cybersecurity has dramatically improved the organization's overall cybersecurity measures:

*"Security Lead A, a manager who previously was head of development, has now been given a dedicated position for cybersecurity. After this happened, I feel that awareness increased quite a bit. They have initiated several measures to make learning about cybersecurity easier, such as nano learning, which they started giving us last week."*

When discussing training and knowledge regarding cybersecurity, this area is slightly basic among sales employees. As they indicated earlier in the interview, the focus on this could have been better. It has also been uncertainty around the topic. Both state that they have no specific training in cybersecurity, but the situation is improving now, and they are eager to learn more on the topic as they understand the increasing importance of the topic. Sales Employee A comments that:

*"I haven't received any training on cybersecurity before, no. At least not very clearly. There have always been a couple of routines and some guidelines we should follow, but beyond that, we haven't gained any more knowledge. Fortunately, that has changed now."*

Sales Employee A expresses contentment with the improved level of support provided and values the regular updates on potential threats received via email from Security Lead A. They state that this helps them to easier recognize threats in their everyday work and to avoid common dangers like phishing and social engineering. In contrast, Sales Employee B acknowledges progress towards improvement in the organization but notes a concern that profit may take precedence over cybersecurity. This is possibly due to time constraints, according to Sales Employee B:

> *"While we have established routines for cybersecurity and are told to prioritize them, the demands of customers can often become overwhelming. With sales assignments and follow-ups to attend to, it can be challenging to balance our focus on making profits and prioritizing cybersecurity. Unfortunately, this can lead to neglecting cybersecurity measures due to time constraints".*

Both of the sales employees have basic knowledge of some cybersecurity measures. For example, Sales Employee A describes that they grade the sensitivity of all the documents they write and that this is a feasible cybersecurity measure they are satisfied with. In addition, Sales Employee A expresses openness to new standards now being introduced by Security Lead A. Sales Employee B, on the other hand, is not completely satisfied with the latest cybersecurity measures being implemented:

> *"I've noticed that many individuals utilize two-factor authentication for their email accounts. I haven't been interested in it as I find it a hassle. However, I do hear a lot of people say it's great. I suggest using bio-metric identification, like facial recognition or fingerprint scanning, as an alternative to relying solely on that (2FA). It would make things much more convenient for me"*

The Sales Employees expressed their efforts to adapt to the new guidelines provided by the management. Although they need more time for additional learning, they ensure that they try to follow the necessary cybersecurity guidelines. Both also emphasize that Security Lead A's new role and the implementation of nano-learning are helping to improve the situation. They think that their colleagues in the department share the same belief. However, there is a sense of avoiding responsibility. Sales Employee B says that:

> *"I do my best to adhere to the routines provided, but I lack expertise in cybersecurity and distinguishing between safe and unsafe practices. As a salesperson, my primary focus is on fulfilling my assigned job duties, and I view cybersecurity as the responsibility of the IT department. They possess more knowledge than I do, and I believe they are better equipped to safeguard all employees."*

Both employees understand the significance of cybersecurity and want to gain new information about the topic. However, they also state that following the rapidly evolving threat landscape can be difficult. They both acknowledge that cybersecurity is now more crucial than ever and that staying informed is essential due to the growing threat of cyber attacks. Sales Employee A even cites cyber warfare as a prime example:

> *"Cybersecurity is crucial, especially with the constantly evolving and dangerous threat landscape. The news is filled with reports on cyber warfare and hack attacks between countries like Russia, China, and Ukraine. These incidents make me realize the significance of safeguarding our information since there are individuals out there with malicious intent to steal it".*

When discussing the ability and desire to adjust to new changes in cybersecurity routines, the employees show different perspectives on this topic. Sales Employee A expresses dedication towards adapting to recent changes in cybersecurity, recognizing its significance in presenting a professional and secure image to customers. They also acknowledge that several customers have strict cybersecurity requirements, so it is essential for Sales Employee A to be up-to-date for better collaborations. In contrast, Sales Employee B reiterates their earlier opinion and finds it hard to adapt to such drastic changes:

> *"To simply view my payslip, I must go through a two-factor authentication process. It seems like a lot of effort for something so routine. I understand the need to protect sensitive information, but it's too excessive to authenticate my access to a personal document.*

Lastly, Employee B in Sales expressed that cybersecurity measures hinder their effectiveness. They feel the actions are intrusive and have made multiple processes more cumbersome. In addition, the numerous extra steps that need to be taken and the short implementation time make it difficult for them to learn and adapt to everything new. While they understand the potential threats of cybersecurity, they believe that more straightforward and less intrusive measures could also improve the effectiveness of their work.

**Company B**

Company B, Sales Employee C, and Sales Employee D were interviewed. Sales Employee C works as a Sales Accountant at Company B, with three years of experience in this role. Sales Employee B is a Customer Relations representative within the same company and has been in the position for three years.

Both employees from Company B report a positive and transparent cybersecurity culture in their own company and feel well-supported by their managers. They value the collaborative atmosphere among their colleagues and the ease of addressing concerns. Although they receive plenty of pertinent and current information on cybersecurity, Sales Employee C notes that it can be challenging to comprehend at times fully:

> *"I have received some video clips regarding cybersecurity, which I admit to falling behind on. Although I understand the importance of gaining knowledge on the subject, it's been challenging to keep up with amidst my other responsibilities."*

They both expressed satisfaction with the organization's commitment to cybersecurity. The sales employees feel proud and safe to work in an organization that takes cybersecurity seriously and recognizes the importance of protecting their digital assets. The feedback on the implementation of new measures for individuals to contribute to enhancing cybersecurity was mixed. Sales Employee D expressed high levels of contentment with these measures:

> *"The company has implemented new cybersecurity measures requiring a Microsoft automation app or a one-time SMS password for logging in. Many of our systems now also require a password and a security question. These measures are important for cybersecurity, and we must follow them to protect ourselves."*

On the other hand, Sales Employee C is rather critical of many of the cybersecurity measures introduced. Although they admit that they are not good at keeping up with new information about cybersecurity, they state that they think it is unnecessary that the management of cybersecurity measures discourages them from connecting to public networks with work PCs:

*"As per company policy, accessing public networks is prohibited. Consequently, I am unable to utilize my work computer during my travels. I have been advised to share my mobile data from my work phone to my PC as an alternative, but I find this method burdensome and challenging."*

When discussing cybersecurity training, both employees state that they need more support from the management on this in the past. As a result, the employees are concerned that they may not have enough cybersecurity knowledge and that efforts to increase awareness should have been implemented earlier. However, the company's introduction of nano-learning has alleviated their worries. Sales Employee C finds this method effective in developing their cybersecurity knowledge. On the other hand, Sales Employee D prefers an alternative learning approach.

*"It can be challenging to watch the short videos we receive during a busy workday. It would be helpful to have dedicated days or hours for cybersecurity courses, allowing us to receive comprehensive information rather than small pieces. Time is my biggest challenge, and this solution would be more efficient."*

When discussing awareness and compliance with cybersecurity measures, the employees acknowledged that they could have been more proactive in increasing their knowledge. They felt they needed to be more informed about the current threat landscape. Time constraints were cited as the main contributing factor. In addition, their understanding of cybersecurity is basic. However, they recognize the concept of a phishing email and the importance of periodically changing their password. Despite this, both employees expressed a strong sense of responsibility towards the information they handle. Sales Employee C specifically stated that:

*"Our organization handles highly sensitive documents for public organizations, including child protection-related documents. We must prioritize privacy and adhere to the latest GDPR regulations. I recognize my responsibility to uphold strong cybersecurity practices to benefit myself, our organization, and our customers."*

However, it is evident that it is challenging for everyone to adapt to these changes in cybersecurity, which is proven by Sales Employee D, who holds a slightly different point of view. Although they acknowledge a sense of responsibility, they believe that the entire weight of cybersecurity should not solely fall on their shoulders:

*"As someone from the older generation, I often struggle with keeping up with all the latest technology. Though I try to follow cybersecurity protocols, I sometimes rely on others to fix any mistakes I may make. I trust that there are experts within the organization who are better equipped to handle these situations than I am."*

When discussing the importance of staying protected when handling information systems, both employees expressed that cybersecurity is of utmost importance, particularly in today's digital age. They also emphasized that they feel obligated to uphold cybersecurity measures to the best of their abilities. Furthermore, they complimented their organization for prioritizing cybersecurity even more rigorously now than before and credited their leaders for bringing attention to the topic. They find it easy to ask colleagues about cybersecurity matters and are confident in receiving further help if needed.

Both employees expressed their willingness to adapt to any changes that management brings, although it can be a challenging task. They mentioned two-factor authentication as an example of a cybersecurity measure that they find difficult to implement. Sales Employee D even stated that it's more of an obstacle than a cybersecurity measure and that they're not fond of it. However, they understand the importance of securing the data of their customers and are eager to contribute to this cause. They would however like the cybersecurity measures implemented by the management to be less intrusive, and simpler to use.

### 4.2.2 Investigating the IT Department Cybersecurity Subculture

Once the sales subculture was interviewed successfully, attention was turned toward the IT subculture and its employees. I had the opportunity to interact with four individuals, two from each company, who were willing to participate in the interview process. Their responses provided valuable insights into their subculture's perspectives on cybersecurity.

**Company A**

From Company A, IT Employee A and IT Employee B were interviewed. IT Employee A is a senior developer with five years of experience. IT Employee B is a cloud engineer who has worked in their position for five years. These two employees have comparable lengths of experience in the company, but their job roles distinguish their fields of work.

Both employees state that Company A's cybersecurity culture is generally strong, with a certain level of autonomy and decision-making authority for developers. IT Employee A describes that there is a bit of hierarchy in the organization and that the developers generally have more freedom to shape their own working day:

> *"I have to admit that there is a kind of unofficial hierarchy within the organization here. Being a developer, I feel that I have more flexibility compared to a seller, for instance. That allows me more productivity and control over my tasks and workdays. With this freedom, I have the opportunity to delve into other areas of interest, like cybersecurity".*

While IT Employee A perceives hierarchy as a contributing factor to Company A's cybersecurity culture, IT Employee B highlights their organization's culture of transparency and openness towards cybersecurity. They emphasize that employees can freely admit their mistakes without fear of punishment or humiliation. According to IT Employee B, this openness is critical in fostering a strong cybersecurity culture, and they are eager to share their expertise and assist those who may encounter challenges.

When discussing which steps Company A takes in order to improve cybersecurity, IT Employee A highlighted that there is an important focus on physical cybersecurity measures. This includes utilizing keycard access and visitor control procedures, as no unauthorized people should get access to the company's physical assets. The employees stress the importance of restricting access to the organization's hardware to prevent unauthorized individuals from accessing digital information and carrying out cybersecurity attacks. They are pleased that the organization places a high value on physical, cybersecurity. Confidentiality agreements are signed, and regular information and reminders about cybersecurity practices are provided. Lastly, both employees state that two-factor authentication has been enforced for all employees, which they see as an essential cybersecurity measure.

When discussing cybersecurity education and training, it was clear that the knowledge level of cybersecurity among the interviewees is high. IT Employee A stated that they had received comprehensive training in cybersecurity and had the option to pursue additional courses and certifications. Similar to the sales team, the IT Employees also observed a boost in their cybersecurity measures after Security Lead A was promoted to the position of Chief Security Officer:

> *"Lately, the CISO has been placing more emphasis on cybersecurity. I have been regularly informed about the potential threats we should be vigilant of and the necessary precautions that we, as developers, should take. Furthermore, they have introduced nano learning to provide further education on the subject."*

The IT employees showcased their extensive knowledge and expertise in cybersecurity. They emphasized the critical importance of ensuring secure systems in their roles as developers. IT Employee A recognized the ever-evolving threat landscape and stressed the need to stay updated to prevent emerging attacks. They emphasized the responsibility of creating secure and reliable systems that protect sensitive information from malicious actors. IT Employee B echoed these sentiments, placing great significance on cybersecurity and emphasizing its relevance to their work. Both employees stress the importance of ongoing education and training to stay up-to-date with the latest cybersecurity trends and best practices. They also highlighted the importance of taking a proactive approach to cybersecurity rather than simply reacting to threats as they arise, which Sales Employee B emphasizes in the interview:

> *"Ensuring cybersecurity is of utmost importance to us, as we have customers who entrust us with highly sensitive information stored in our documents and databases. It's imperative that we take this matter seriously to avoid any potential consequences. My impression is that the developer team is fully aware of the significance of cybersecurity and is committed to maintaining a safe and secure cybersecurity culture".*

During the interviews conducted with Company A's IT employees, another topic that was discussed was their attitude toward adapting to changes in cybersecurity. Both employees expressed their willingness to modify their routines as a vital aspect of improving cybersecurity. They also encouraged their fellow employees to embrace this approach. It was evident from the interviews that Company A's IT employees take cybersecurity very seriously and are proactive in improving it. The willingness to adapt to changes is a crucial aspect of cybersecurity, especially in today's rapidly evolving digital landscape, where cyber threats continue to grow and become more sophisticated. By embracing change, Company A's IT employees are safeguarding their organization's digital assets and ensuring they are always one step ahead of potential risks. IT Employee B holds the belief that change is beneficial and should be welcomed:

> *"Through my personal experience, I have come to realize that change can be a positive force. Embracing change enables an organization to progress and become better equipped to tackle future challenges. As someone who is over 50 years old, I strive to motivate my fellow colleagues to adopt a positive attitude toward change. Having managed change*

*myself, I have witnessed firsthand the benefits it can bring, and I believe that others can also embrace change successfully."*

In conclusion, the interviews with Company A's IT employees were a testament to their dedication to cybersecurity. The willingness to adapt to changes and embrace new approaches is a hallmark of their commitment to ensuring that their organization's digital assets are always secure. The interviews conducted with the IT-Employees in Company A generally show that they understand the importance of cybersecurity and want to contribute with their knowledge to maintain a strong cybersecurity culture. They want to share their expertise but also realize that they are privileged with more time on their hands as developers to focus on cybersecurity than their colleagues in other departments.

#### Company B

From Company B, IT Employee C, and IT Employee D were interviewed. IT Employee C is a senior developer and has worked in this role for four years. Similarly, IT Employee D is also a senior developer with slightly longer experience, with five years in the role. Although they share similarities in their roles, comparing their responses and seeing if they align will be intriguing.

During discussions about their organization's cybersecurity culture, both employees expressed satisfaction with some of the measures implemented by the company. One such step is the internal Security Council plays a significant role in promoting a robust cybersecurity culture, as previously mentioned by Security Lead B. This was implemented as a cybersecurity measure to discuss cybersecurity concerns across teams within Company B. However, both IT employees reveal that this measure relies significantly on their participation as they are seen as the "security experts" and feel partly pressured by the management to take care of cybersecurity discussions in the Security Council. On the positive side, IT Employee D highlights that it enhances transparency across various departments:

*"As members of the Security Council, we can address cybersecurity incidents that have affected all teams within the company. Additionally, as IT Employees, we can bring attention to potential threats that other departments may not have considered. This proactive approach is crucial in promoting a culture of cybersecurity awareness within our organization. However, I do not believe the responsibility should fall solely on us. It would benefit the management to also educate all teams about cybersecurity."*

The IT Employees feel that they have sufficient control and awareness of cybersecurity and emphasize that it is essential for them to stay up-to-date on new threats. This is important to protect their organization and, most importantly, the customers and their sensitive data. It is also clear that the employees feel a responsibility to spread knowledge to the other employees in the information, but believe that there needs to be more management support to convey this attitude. This is evident in this statement from IT Employee D:

*"As an IT Employee, I believe the Security Council relies heavily on our cybersecurity knowledge. However, all employees must understand that cybersecurity is the responsibility of the entire organization, not just the IT department. We need to work together and collectively increase cybersecurity awareness to ensure the safety and cybersecurity of our company's digital assets. I hope that our management also realizes this."*

According to the IT employees in Company B, they feel burdened by the responsibility of sharing their cybersecurity knowledge. This task takes up much of their time and prevents them from focusing on other essential tasks. The employees also noted a great expectation placed on them to prioritize their time to educate others on cybersecurity, mainly through the Security Council. However, they feel that this expectation causes the Security Council to become a one-way exchange, with IT employees sharing their knowledge with other teams but receiving different input from other groups. In addition, IT employee C felt labeled as the "cybersecurity expert," leading to expectations from employees in other subcultures regarding their contributions to the organization. The IT employees would appreciate more support from management in distributing cybersecurity knowledge, allowing them to focus on maintaining and developing their respective systems.

When discussing willingness and desire to adjust to changes in cybersecurity culture, both expressed their openness to adaptation, recognizing that difference is crucial for ensuring progress in cybersecurity. While they acknowledged that some employees in other departments are hesitant about change, they strive to encourage them by sharing knowledge with the Security Council. IT-Employee D highlighted that the threat landscape constantly evolves, underscoring the importance of Company B constantly assessing and changing its practices to keep pace:

> *"As employees and managers within the organization, we are all aware of the rapidly evolving threat landscape. Almost every day, new threats emerge that require our careful attention. Unfortunately, it seems unlikely that this trend will slow down anytime soon. I have been following news reports of cyber attacks on companies with increasing concern, and I sincerely hope that our organization does not become a victim. Given the current number of threats, it is important that we prioritize cybersecurity and promote knowledge sharing across all departments".*

The employees working in IT have expressed their appreciation for Company B's approach to cybersecurity. They have noticed that the organization takes the matter of cybersecurity seriously, and appreciate that cybersecurity incidents are dealt with accordingly. They believe that the establishment of the Security Council is a positive step towards creating awareness among all employees and are hopeful that more such measures will be taken in the future. However, they feel that more managerial support is needed. While the CISO has offered assistance, being physically located at Company A limits their availability. The IT employees note that Security Lead B has other responsibilities that occasionally prevent them from fully addressing cybersecurity concerns. It has been recommended. The IT Employees, therefore, suggests hiring a fully dedicated cybersecurity expert to be physically present at Company B to aid in cybersecurity incidents and promote knowledge, awareness, and compliance.

## 4.3 Summary Tables

Understanding the values, assumptions, and beliefs that shape cybersecurity subcultures within organizations is crucial for developing effective cybersecurity strategies and fostering a strong cybersecurity culture. The table presented below provides a comparative summary of the critical aspects uncovered in interviews, highlighting employees' diverse values, beliefs, and assumptions regarding cybersecurity practices. By analyzing these factors collectively, organizations can gain a deeper understanding of the underlying principles that guide employee attitudes and behaviors toward cybersecurity, allowing them to implement targeted measures that confidently enhance cybersecurity awareness and resilience. The summary tables for each company are listed below:

| Subculture | Values | Assumptions | Beliefs |
|---|---|---|---|
| IT Employees | Feels more freedom in their role, which also entails a certain grade of responsibility to acquire new knowledge. They also emphasize that they want to contribute to fostering a secure and transparent cybersecurity culture in their organization. They embrace changes within cybersecurity and motivate others to do the same. | Assumes that the responsibility of sharing cybersecurity knowledge is shared between the developer team and the management. Furthermore, they expect employees in other subcultures to take a certain responsibility for cybersecurity. | Believes that cybersecurity should be of utmost importance to everything they do. They want to develop safe and secure systems to keep their customers' data safe and believe it is important always to be aware of potential threats. However, they believe that the rest of the employees in the organization need to share this attitude. |
| Sales Employees | Strives to be transparent about their cybersecurity actions. Feels a specific responsibility in appearing knowledgeable in cybersecurity towards the customers. Expresses a desire and willingness to learn more about the topic, but time doesn't allow it. They find it easy to be open about cybersecurity to their colleagues. | Assumes that basic cybersecurity measures like 2FA will keep them protected, but still struggle to see the importance of it. They trust that the company and the CISO will keep them safe and updated on new threats and risks through cybersecurity measures, such as nano-learning. | Realizes that they have a responsibility to know the most important routines, but still feel that it is the IT department's responsibility to focus on cybersecurity. Realizes there is an evolving threat landscape but trusts that the organization's cybersecurity is in good hands. |

Table 4.1: Company A Cybersecurity Subculture Findings

| Subculture | Values | Assumptions | Beliefs |
|---|---|---|---|
| IT Employees | value the promotion of cybersecurity subcultures as they have significant knowledge in the field and can bring attention to potential threats. However, they feel like there needs to be more responsibility throughout the company, both from the employee and management aspects. | In agreement with company A, they also assume that the responsibility of cybersecurity is shared between them and the rest of the company's employees. However, they feel that they are pressured to contribute with their knowledge in the cybersecurity council with little management support | Think that although they can help the company with their expertise in cybersecurity and can troubleshoot their problems, the other departments should be instructed in this matter since they believe it's not only their responsibility but from all employees of the said company |
| Sales Employees | Feel a special responsibility towards their customers to protect their data, especially when the information they process is sensitive and mostly on behalf of the public sector. They also feel a sense of commitment to update themselves on cybersecurity threats to appear professional in front of their customers. | Assumes that the management is taking steps to ensure their cybersecurity and are particularly satisfied with the introduction of nano learning. However, they state that some steps the management takes are intrusive and appear to be seen as obstacles rather than protective measures, such as 2FA. | Believe in the importance of cybersecurity measures, although it can bring some intrusive difficulties that make their work less effective than they would have wanted. However, they also believe that cybersecurity threats are emerging rapidly, which results in wanting to stay updated and educated on cybersecurity. |

Table 4.2: Company B Cybersecurity Subculture Findings

# Chapter 5

# Discussion

This chapter will discuss the empirical findings from the interviews. It will also highlight the practical contributions this study brings to the topic.

The systematic literature review revealed a lack of previous research on the topic of cybersecurity subcultures. While existing data emphasize the overall importance of cybersecurity culture within organizations, little attention has been paid to subcultures. Even after presenting the findings, it is evident that investigating and prioritizing this area is crucial. The research shows that subcultures are emerging, each with its own cybersecurity routines. The employees' knowledge, motivation, and awareness levels vary greatly, which can affect the organization's cybersecurity. Previous studies have overlooked this aspect of cybersecurity culture, and this study has highlighted several key factors that organizations must address.

The results from the qualitative approach to a comparative case study have now been obtained through semi-structured interviews and the systematic literature review. The findings have proven to be very distinct and highly interesting and have addressed the knowledge gaps that were previously identified. In the next part of the report, the cybersecurity subcultures will be discussed differently from the previous findings chapter. Although the sales and IT cybersecurity cultures will be addressed independently, they will be examined across both organizations. If any significant differences between the subcultures being discussed together are found, they will be highlighted.

## 5.1 Sales Cybersecurity Subculture

Four sellers were interviewed in total in the sales cybersecurity subcultures. The interviewees were of varying roles, ages, and work experience. Although they worked across companies, many answers and perceptions were similar. Both security managers pointed to the sales cybersecurity subculture as the one with weaker cybersecurity knowledge and awareness. Subsequently, the interviews also show that this is the truth. In this subsection, the interview findings will be presented, and the most critical factors will be highlighted.

The transparency of the cybersecurity culture in both organizations has made the sales employees very content. This is a positive development because it encourages employees to report mistakes without fear of negative repercussions. By reporting errors, they can be addressed and corrected swiftly, and it is commendable that both organizations foster such openness. Furthermore, prompt reporting of cybersecurity issues enables quicker resolution and prevention of potential threats. Conversely, a culture of fear where employees hesitate to report cybersecurity incidents can be detrimental, allowing threats to grow unchecked. Therefore, it is reassuring that the organizations promote an open cybersecurity culture, as emphasized by the sales employees during their interviews.

Another positive aspect of the sales cybersecurity culture is their desire to learn more about cybersecurity. It is clear that it is a topic that they understand is becoming more critical in today's society, and they feel a particular responsibility towards their customers to keep their knowledge of the topic up to date. It can almost seem that this responsibility is felt more strongly towards the customers than the organization itself, which shows that the employees feel a lot of respect and care for the data they store for their customers. The employees seem to be aware that their data is very sensitive and valuable, and therefore do not want it to fall into the wrong hands.

However, it seems that the organizations are not taking advantage of their sales employee's desire to learn more about cybersecurity. Some employees report that they simply don't have the time to learn, despite efforts by management to facilitate learning through nano learning. Others point to a prioritization error on the part of management, where profit is given precedence over cybersecurity. This has led to a need for more knowledge and awareness among sales employees, despite management's recent efforts to improve cybersecurity measures. Sales employee B also describes difficulties obtaining knowledge from the departments that are more competent in cybersecurity, such as the IT department. This is described as "company within a company," and the possibility of communication and learning between the departments seems to be very limited, at least in Company A. Company B seems to have tried to combat this problem with the help of the Security Council. It's clear that the managements need to prioritize and arrange for the sales employees to acquire knowledge about cybersecurity, whether in the form of learning or communication with more competent departments.

The feedback from the sales employee varies greatly regarding the implemented cybersecurity measures. The interviews show that both companies are taking steps to improve their cybersecurity, despite some past reluctance to do so. Some sales employees view measures intended to strengthen cybersecurity as a personal inconvenience complicating their daily routine. Sales Employee B even goes as far as describing it as "burdensome and challenging." The majority of the sales employee prioritize efficiency and simplicity and often need help understanding how these measures contribute to enhancing cybersecurity. Consequently, they may not comply with or attempt to bypass the standards. There is a risk that the negative outlook towards these measures could spread within subcultures, resulting in more individuals disregarding them. The organization's management needs to adequately communicate the purpose of these cybersecurity measures and their intended function in preventing cyber threats. This information is necessary for employees to view these measures as obstructive rather than protective for their knowledge and personal safety.

In addition to a lack of understanding of the cybersecurity measures, a lack of responsibility is one of the biggest problems for the sales cybersecurity culture. As previously mentioned, most people feel a responsibility toward their customers and want robust cybersecurity to safeguard their data. But the vast majority believe that all responsibility for cybersecurity lies with others, such as the IT department and the leadership. This can lead to the belief that there will always be someone to clean up if a mistake should happen and that they can become a little too dependent on the combination of a lack of responsibility and a transparent culture. As a result, the employees are less attentive and aware of their mistakes because they trust that they can go and report it to someone who will clean it up for them. Thus, they feel they need to feel a more personal responsibility for the organization's cybersecurity and mindlessly trust that other, more competent employees can fix the problems the sales employees create. Unfortunately, this can be a dangerous attitude, as more frequent threats can occur when employees do not feel responsible for acting carefully in the face of digital threats.

The findings above suggest that the cybersecurity culture maturity model, depicted in figure 2.1, is relevant in this case. This model outlines four maturity levels, with level one being the least mature and level four being the most mature. The sales subculture's findings show a lack of maturity in this cybersecurity subculture, but there are also positive aspects. The sales employees have surpassed level one in maturity by acknowledging that technology alone cannot ensure their safety. However, they still seem to rely on someone else to clean up after them, thus relinquishing much responsibility. It appears that they struggle to recognize the significance of their actions and are oblivious to the consequences that may arise because they believe that others with more expertise are better equipped to manage their cybersecurity. As a result, it is reasonable to categorize the sales cybersecurity culture at level 2 maturity. They recognize the importance of the human aspect of cybersecurity but try to avoid taking responsibility for their actions.

In summary, both organizations have fostered a sales cybersecurity culture that values transparency and encourages employees to report mistakes without fear of consequences. This positive environment has led to prompt resolution and prevention of potential threats. The sales team also demonstrates a strong interest in enhancing their cybersecurity knowledge and feels accountable for safeguarding their customers' data, reflecting their respect for the sensitive information they handle. Despite these positive developments, there needs to be more personal responsibility within the sales cybersecurity culture. Many employees believe cybersecurity is the IT department's and leadership's responsibility, which diminishes their sense of accountability and may result in carelessness when facing digital threats. To address this issue, organizations should prioritize cultivating a culture emphasizing individual responsibility and providing sales employees opportunities to acquire cybersecurity skills and knowledge.

## 5.2 IT Cybersecurity Subculture

Four IT employees were interviewed in total in the IT cybersecurity subcultures. The interviewees were of varying roles, ages, and work experience. Although they worked across companies, many answers and perceptions were similar. Both security managers pointed to the sales cybersecurity subculture as the one with the most substantial knowledge, and the interviews also show that this is the truth. The interview findings will be presented in this subsection, highlighting the most critical factors.

Companies have differing opinions regarding the cybersecurity culture among IT employees. Company A has a hierarchy where IT employees have a higher status than sales employees. This hierarchy grants IT employees more freedom to allocate their time, allowing them to spend more on cybersecurity. They do not seem to experience the same profit-driven pressures as sales employees. This has positive and negative implications. On the positive side, IT employees in Company A have more time to improve their cybersecurity skills and acquire new knowledge to develop and maintain information systems safely. On the negative side, the hierarchical structure is unfair to sales employees. Although IT employees work with information systems more vulnerable to cyber attacks, sales employees should also have the opportunity to learn about cybersecurity. If management can facilitate this for IT employees, they should also provide sales employees a chance to learn about cybersecurity and allocate time. On the other hand, the IT employees in Company B boast of the transparent and flat cybersecurity culture there, just like the sales employees explained earlier. These also appreciate the previously described Security Council and feel that there is good communication among the employees.

The IT employees demonstrate a high level of knowledge when it comes to cybersecurity. They emphasize the importance of staying informed about new threats and prioritizing the development of secure systems for customers. They also feel a sense of responsibility to share their knowledge with colleagues. The organizations provide opportunities for certifications and further education in cybersecurity, which is commendable. However, it is unfortunate that sales employees do not receive the same opportunities, but it is understandable that IT employees interact more with digital systems. The IT employees' focus on knowledge will undoubtedly positively impact the company's overall cybersecurity.

During interviews, it was evident that Company A and Company B share similarities and differences in their focus on cybersecurity. After employing a joint Chief Security Officer for all companies in the holding group, both companies have shown an increased focus on cybersecurity. However, the CISO is physically located at Company A but oversees the cybersecurity of all companies. Company A places more emphasis on physical cybersecurity, such as the use of key cards and preventing unauthorized access to the building. This is an often overlooked aspect of cybersecurity, but Company A takes this threat seriously and actively works to incorporate it into its cybersecurity culture. Unauthorized individuals gaining access to physical devices can cause significant damage to digital systems, making it critical for companies to recognize this threat.

The IT employees in Company B did not mention the implementation of physical cybersecurity in their cybersecurity subculture. However, they prioritize promoting communication, as evident from the sales employees' feedback. The employees expressed satisfaction with the company's transparency. The IT and sales subcultures credit the Security Council for facilitating knowledge and sharing concerns across the different departments. This open communication among employees is a valuable quality that Company B should maintain. Encouraging interaction and exchanging knowledge among colleagues can enhance the flow of information, raise cybersecurity awareness, and foster a more robust cybersecurity culture.

The employees in the IT department at Company B have expressed concerns about the Security Council's weakness regarding cybersecurity. They feel that the responsibility for distributing knowledge and increasing awareness falls solely on them, without adequate support from the management. They believe that cybersecurity should be a collective responsibility among all employees. However, there needs to be more clarity regarding the distribution of responsibilities, particularly regarding who is responsible for ensuring that employees across all departments gain increased awareness. The IT employees understand they have a special responsibility for cybersecurity, as it is their primary duty to secure, develop, and operate IT systems. If they are left to handle the burden alone, balancing their work tasks with staying current on cybersecurity threats can become challenging. The management needs to prioritize cybersecurity awareness across all departments, including sales.

In summary, the companies differ in their approach toward cybersecurity culture among IT employees. Company A adopts a hierarchical structure that gives IT employees more time and freedom to focus on cybersecurity, while sales employees do not receive the same privilege. This approach ensures increased knowledge to the IT department but may seem unfair to the sales employees. In comparison, Company B has a transparent and flat cybersecurity culture, with open communication facilitated by the Security Council. In addition, company A emphasizes physical cybersecurity measures, while Company B prioritizes communication. However, Company B's IT employees believe they need more management support to bear the sole responsibility for cybersecurity awareness. They believe cybersecurity should be a collective responsibility among all employees, and management should prioritize increasing awareness across all departments.

The differences in cybersecurity are more significant between the subcultures of the same company than of the same type of department across the companies. The fact that these cybersecurity subcultures in the same company have such large differences is very significant for the overall cybersecurity in the companies. Different departments' varying priorities regarding cybersecurity measures can lead to inconsistent cybersecurity practices. This creates vulnerabilities that weaken the company's overall cybersecurity posture. Communication gaps can also hinder effective collaboration and information sharing between departments. Addressing cybersecurity threats becomes challenging with cohesive efforts, and the organization may need help to respond promptly and effectively to potential incidents. Additionally, some departments may have unequal protection of sensitive data due to differences in their understanding and implementation of cybersecurity measures. This increases the risk of data breaches and unauthorized access. Therefore, organizations must prioritize individual responsibility, provide learning opportunities, and improve communication to enhance their cybersecurity culture and mitigate potential risks. It is crucial to address these issues to maintain a secure and protected organization.

The findings highlight the importance of the management structure and their cybersecurity behavior. Managers must set a high standard by leading the way in following cybersecurity rules and best practices. This includes adhering to password policies, using multi-factor authentication, and practicing safe browsing procedures to demonstrate a solid commitment to cybersecurity. The rest of the organization should follow their lead, and management should effectively inform everyone about the value of cyber safety. This involves outlining the risks and potential consequences of cyber threats, stressing the importance of protecting confidential data, and emphasizing every employee's role in maintaining a secure environment.

To create a strong cybersecurity culture, CISOs must provide strong leadership and work closely with executives to establish cybersecurity-focused policies, practices, and governance frameworks. They should educate employees on the value of cybersecurity and the risks and consequences of cybersecurity breaches through regular training and awareness campaigns. CISOs should ensure clear communication between IT departments and other organizational departments to encourage collaboration to incorporate cybersecurity considerations into various business processes and initiatives.

## 5.3 Practical Contributions

The research findings challenge the current idea that there only exists a single cybersecurity culture within organizations. Existing studies examined earlier in the research project mainly focused on cybersecurity culture as a collective concept, with few considering the possibility of emerging cybersecurity subcultures. However, this research has revealed that cybersecurity subcultures do indeed arise, and their behavior can significantly affect the organization's overall cybersecurity. Therefore, organizations should acknowledge and understand their cybersecurity subcultures and get an overview of perceptions regarding their cybersecurity policies and procedures effectively. Furthermore, the research contributes to significant differences in perceptions among subcultures, emphasizing the need for organizations to shift from a single cybersecurity culture approach to addressing the cybersecurity subcultures individually.

The differences in cybersecurity are more significant between the subcultures of the same company than of the same type of department across the companies. The fact that these cybersecurity subcultures in the same company have such large differences is very significant for the overall cybersecurity in the companies. Different departments' varying priorities regard-

ing cybersecurity measures can lead to inconsistent cybersecurity practices. This creates vulnerabilities that weaken the company's overall cybersecurity posture. Communication gaps can also hinder effective collaboration and information sharing between departments. Addressing cybersecurity threats becomes challenging with cohesive efforts, and the organization may need help to respond promptly and effectively to potential incidents. Additionally, some departments may have unequal protection of sensitive data due to differences in their understanding and implementation of cybersecurity measures. This increases the risk of data breaches and unauthorized access. Therefore, organizations must prioritize individual responsibility, provide learning opportunities, and improve communication to enhance their cybersecurity culture and mitigate potential risks. It is crucial to address these issues to maintain a secure and protected organization.

One of the biggest obstacles hindering the development of cybersecurity awareness among the sales cybersecurity subculture is the need for more time. Due to their already heavy workloads, employees need help finding dedicated time for cybersecurity training, often perceiving it as an additional burden rather than a priority. To address this issue, management should prioritize their employees' time and allocate more resources to cybersecurity training. This will enable employees to acquire cybersecurity knowledge and comprehend the measures' importance. By doing so, employees will understand the importance of their digital decisions and awareness and no longer view cybersecurity measures as obstacles. Ultimately, this knowledge will improve overall cybersecurity within the organization.

Another crucial aspect that the management should address is the delegation of responsibilities. This issue is evident in all the subcultures that have been examined. For example, sales employees tend to evade accountability for their cybersecurity decisions and rely on the IT department or someone with more knowledge and responsibility to rectify errors. Managers must provide clear information regarding the consequences of cybersecurity mistakes and emphasize the importance of being cautious enough to prevent cybersecurity incidents from happening rather than relying on someone else to clean up. Moreover, employees should act more responsibly when handling digital systems, and the management should allocate resources to train them on this matter.

The interviewed IT departments believe that they need to be more responsible when it comes to cybersecurity. As a result, they think that dedicated managers should share this responsibility. While having a separate CISO is a good start, IT employees feel that management should play a more active role and increase awareness among all employees instead of relying solely on the IT department. One solution could be hiring more dedicated employees to handle cybersecurity, as the CISO alone may need more resources. In addition, allocating more resources to cybersecurity will allow IT employees to focus on other tasks and make the organization safer and more efficient.

This research project has made it evident that, in most cases, the root causes of discovered issues can be traced back to two main themes: priorities and distribution of responsibilities. These are common and persistent problems. However, both organizations seem to excel in fostering a transparent cybersecurity culture with effective communication, except for a few areas where they need to improve communications between the different departments. If the management of the organizations aims to strengthen cybersecurity further, they must prioritize and distribute responsibilities differently to enhance the overall cybersecurity culture, including subcultures.

From the management's perspective, it is essential to note that they have taken steps toward improving the organization's cybersecurity measures. All employees are now undergoing nano learning, and two-factor authentication is mandatory. However, the feedback on these implementations has been mixed during interviews. Despite this, the leaders have acknowledged their shortcomings in cybersecurity and recognize it as a significant reason for employee concerns. Prioritizing cybersecurity subcultures will take time and require substantial organizational changes. It is evident that the management is making efforts to improve, but there is still a long way to go in fostering a cybersecurity culture, especially among sales employees.

Upon thorough analysis and discussion of the findings, I have created a framework that depicts the connections highlighted by the interviews. The management aims to establish a cybersecurity culture that they expect all employees to adhere to. However, each subculture may interpret this culture differently, forming distinct values, assumptions, and beliefs that may differ from the management's expectations. Ultimately, an employee's perception of cybersecurity is influenced by their subculture, which affects their behavior, level of awareness, and compliance with cybersecurity policies. These three steps influence each other, and it has been tried and illustrated in the model below, figure 5.1:

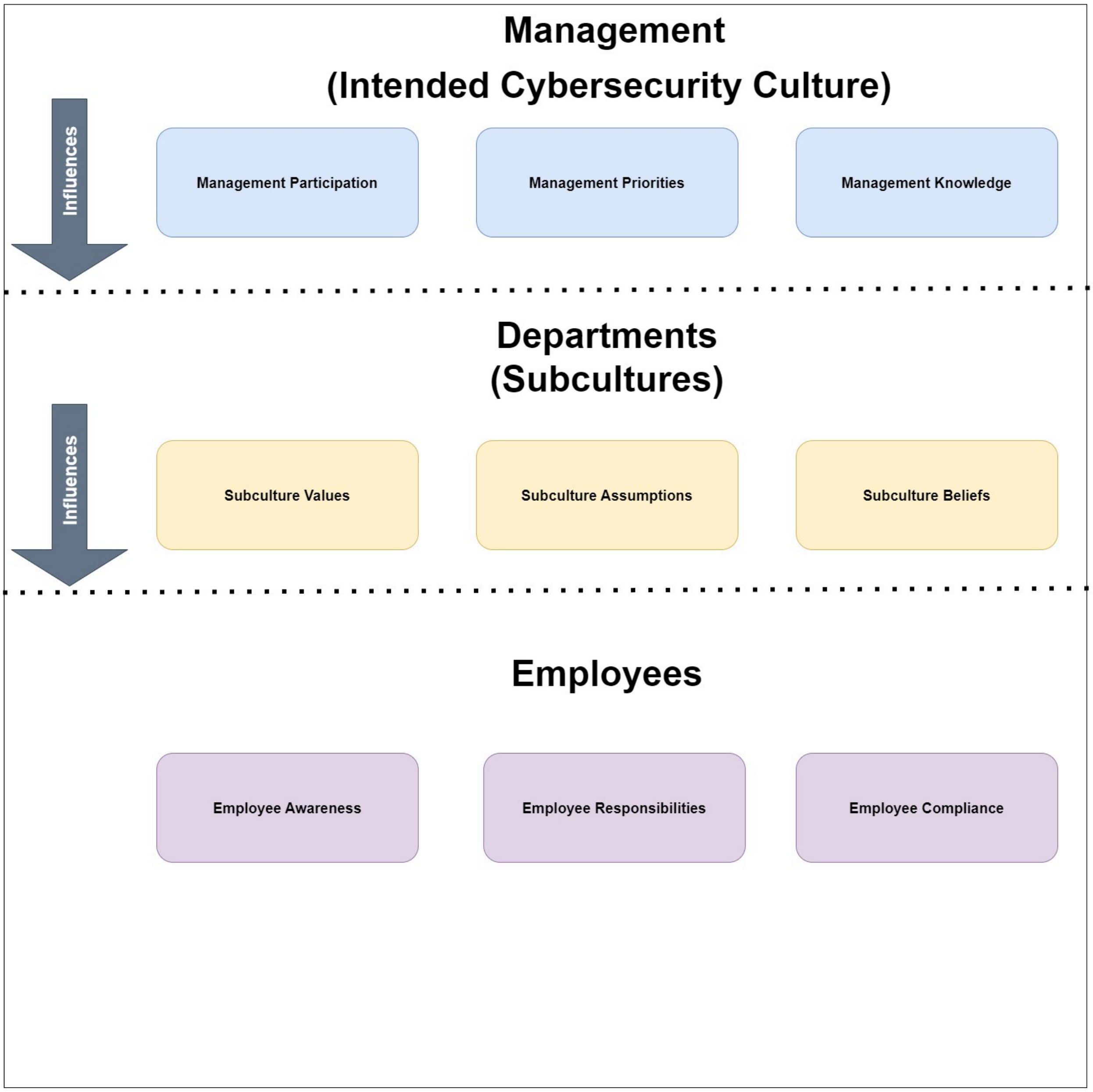


Figure 5.1: Proposed Cybersecurity Subculture Framework

## 5.4 Limitations

When researching cybersecurity subcultures within organizations, I faced several limitations that impacted the overall quality and scope of the findings. Insights into subcultures were obtained through qualitative interviews with four individuals from the two companies. However, it's essential to acknowledge that these interviews have limitations as they must provide a complete understanding of the cybersecurity subcultures. The small sample size restricts the representation of diverse perspectives and complexities within the subcultures. Besides, individual biases and subjectivity can influence the interviews, potentially skewing the overall understanding. Subcultures within organizations can be multifaceted, varied across departments, and influenced by contextual factors. A broader research approach is necessary to gain a more comprehensive insight, including a more extensive and more diverse participant pool, additional research methods like observations and surveys, and considering a more comprehensive range of contextual factors shaping the subcultures. Such an approach would provide a more nuanced understanding of subcultures beyond the limited perceptions gathered from the qualitative interviews.

Accessing relevant literature was a significant challenge during my research project, as payment walls hindered my progress. Furthermore, numerous academic journals and research publications required subscriptions or individual article purchases, which made it challenging to acquire a diverse range of literature. Despite this, I found a solution by utilizing the eduVPN provided by Universitetet I Agder, granting me access to additional databases. However, many databases remained inaccessible, containing valuable literature that would have significantly benefited my research project. Nevertheless, I am confident that the literature I did find was relevant and sufficient to complete my research successfully.

## 5.5 Recommendations for Further Research

Researchers could explore various topics to understand cybersecurity subcultures within organizations better. One area of investigation could be how organizational structure and hierarchy influence cybersecurity subcultures. This was something that IT Employee A also briefly mentioned in the interview. By examining how different decision-making structures impact the development and diffusion of cybersecurity practices, valuable insights can be gained. Leadership styles could also be studied to determine how they align with cybersecurity subcultures and their effectiveness in fostering a strong cybersecurity culture. Finally, cultural values, beliefs, and norms could be considered to examine cross-cultural variations in cybersecurity subcultures.

Researchers could also further investigate external factors such as industry regulations, legal frameworks, and overall threat landscapes that can significantly impact employee attitudes and behaviors toward cybersecurity. By examining the interactions between these external factors and internal organizational dynamics, it is possible to identify strategies that align cybersecurity practices with industry standards and improve overall cyber resilience. In-depth research in these areas can provide organizations with a better understanding of the factors that shape cybersecurity subcultures. This knowledge can inform the development of targeted interventions, policies, and training programs to strengthen cybersecurity cultures and enhance overall cybersecurity posture within organizations. Building a robust cybersecurity subculture mitigates cyber threats and safeguards essential assets and information.

# Chapter 6

# Conclusion

This study aimed to delve into the topic of cybersecurity subcultures and emphasize the significance of recognizing that the cybersecurity culture is not a uniform concept. Hence, the conclusion is based on the analysis of the research above question:

- How do the cybersecurity subcultures impact organizational cybersecurity, and why is it significant?

Despite the limited number of participants in the study, the findings reveal concerning data regarding the distribution of responsibilities and uncertainty among employees regarding their role in maintaining cybersecurity. Differences in subcultures have a significant impact on overall cybersecurity in organizations. Nonetheless, it is worth noting that participants understand the importance of cybersecurity and are eager to expand their knowledge on the topic. They feel responsible for keeping sensitive data safe for their customers and acknowledge that enhancing cybersecurity is crucial. The organizations have motivated employees whose potential remains untapped, and the management must take action to improve knowledge and awareness at all levels of the organization. Although management needs to prioritize time and resources to address these issues, implementing expertise and understanding can effectively solve the problems uncovered in the study.

The significance of cybersecurity subcultures lies in their direct impact on an organization's cybersecurity awareness and resilience. A robust cybersecurity subculture fosters a collective sense of responsibility and ownership for cybersecurity across the organization. When employees share a common understanding of the importance of cybersecurity and are motivated to act by cybersecurity best practices, the organization becomes more resilient against cyber threats. In addition, a robust cybersecurity subculture promotes a proactive cybersecurity mindset, encourages timely reporting of incidents or vulnerabilities, and facilitates effective collaboration between different departments. Subsequently, this enhances the organization's overall cybersecurity awareness and preparedness.

In conclusion, cybersecurity subcultures shape employees' attitudes and behaviors, which are pivotal in an organization's overall cybersecurity posture and resilience. Developing and sustaining a solid cybersecurity culture relies on leadership commitment, effective communication and training programs, robust cybersecurity policies and procedures, a positive work environment, and ongoing monitoring and evaluation. By cultivating a strong cybersecurity culture, organizations can enhance their ability to protect sensitive information, mitigate risks, and effectively respond to cyber threats, ultimately safeguarding their digital assets and maintaining customers' trust. The research emphasizes the significance of cybersecurity subcultures and proves that organizations have many dominant cybersecurity cultures.

# References

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

Alvarez-Dionisi, L. E., & Urrego-Baquero, N. (2019). Implementing a Cybersecurity Culture. *ISACA JOURNAL VOL 2*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture

Andronache, A. (2021). *Increasing security awareness through lenses of cybersecurity culture*. https://go.gale.com/ps/i.do?id=GALE%5C%7CA675866955&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=18434711&p=AONE&sw=w&userGroupName=anon%5C%7Ec9b39eb7&aty=open+web+entry

Arkvik, I. (2021). *How to establish a strong security culture in your organisation*. https://www.visma.com/blog/establishing-security-culture-organisation/

Bailey, T., Kaplan, J., & Rezek, C. (2014). *Why senior leaders are the front line against cyberattacks*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks#/ (accessed: 10.02.2023).

Baxter, P., & Jack, S. (2010). Qualitative case study methodology: Study design and implementation for novice researchers. https://doi.org/10.46743/2160-3715/2008.1573

BDC. (2023). *Organizational culture*. https://www.bdc.ca/en/articles-tools/entrepreneur-toolkit/templates-business-guides/glossary/organizational-culture (accessed: 15.02.2023).

Busetto, L., Wick, W., & Gumbinger, C. (2020). *How to use and assess qualitative research methods*. https://neurolrespract.biomedcentral.com/articles/10.1186/s42466-020-00059-z (accessed: 11.02.2023).

Corradini, I. (2020). Building a Cybersecurity Culture in Organizations. https://link.springer.com/book/10.1007/978-3-030-43999-6

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. *MIS Quarterly Executive Vol 19. Iss.3*. https://doi.org/https://doi.org/10.17705/2msqe.00032

Crosley, J. (2021). *What (exactly) is thematic analysis?* https://gradcoach.com/what-is-thematic-analysis/ (accessed: 01.03.2023).

Da Veiga, A. (2019). Achieving a security culture. https://uir.unisa.ac.za/bitstream/handle/10500/26783/Chapter%5C%205%5C%20-%5C%20da%5C%20Veiga.pdf?sequence=3&isAllowed=y

Da Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—perspectives from academia and industry. *Computers & Security*. https://doi.org/https://doi.org/10.1016/j.cose.2020.101713

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*. https://doi.org/https://doi.org/10.1016/j.cose.2017.05.002

Denison, G. (2023). *Ethical considerations in research: Best practices and examples*. https://www.prolific.co/blog/ethical-considerations-in-research-best-practices-and-examples (accessed: 15.04.2023).

Donalds, C., & Osei-Bryson, K.-M. (2019). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2019.102056

Dutta, A., & Mccrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*. https://doi.org/10.2307/41166154

Dutton, P., & McLaughlin, J. (2023). *Organizational subculture: Definition & examples*. https://study.com/academy/lesson/organizational-subculture-definition-examples.html (accessed: 10.02.2023).

Elvin, G., & Johansson, E. (2017). *The impact of organizational culture on information security during development and management of it systems*. https://www.diva-portal.org/smash/get/diva2:1112265/FULLTEXT01.pdf

ENISA. (2017). *Cyber security culture in organisations*. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations (accessed: 16.03.2023).

Failla, R. J. (2020). The Influence of Organizational Culture on Cybersecurity Governance in Breached Organizations. https://www.proquest.com/openview/d8e034823b995190f39b4ef464282de7/1?pq-origsite=gscholar&cbl=18750&diss=y

Flynn, L. (2013). *International considerations for cybersecurity best practices*. https://insights.sei.cmu.edu/blog/international-considerations-for-cybersecurity-best-practices/

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research*.

Fruhlinger, J. (2020). *Equifax data breach faq: What happened, who was affected, what was the impact?* https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (accessed: 10.02.2023).

Fund, R. L. (2023). *What is a literature review?* https://www.rlf.org.uk/resources/what-is-a-literature-review/ (accessed: 10.03.2023).

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*. https://doi.org/https://doi.org/10.1080/08874417.2020.1845583

Hoover, L. (2021). *Qualitative vs quantitative research methods data analysis*. https://www.gcu.edu/blog/doctoral-journey/what-qualitative-vs-quantitative-study (accessed: 03.03.2023).

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2021). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*. https://doi.org/https://doi.org/10.1108/ICS-06-2021-0073

Keman, H., & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture.

Kolkowska, E. (2011). *Security subcultures in an organization - exploring value conflicts*. https://www.semanticscholar.org/paper/Security-subcultures-in-an-organization-exploring-Kolkowska/17e14d9b1599478142011ad9a56b2142932e3831

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

Madnick, S., Siegel, M., & Pearlson, K. (2019). Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)3.

Malmedal, B., & Røislien, H. E. (2016). *The norwegian cyber security culture*. https://norsis.no/content/uploads/2022/05/The-Norwegian-Cybersecurity-culture-web.pdf

Mazumdar, M. (2022). *Ethical considerations in research every author should know*. https://researcher.life/blog/article/ethical-guidelines-for-researchers/ (accessed: 11.02.2023).

McCombes, S. (2019). *What is a case study? | definition, examples methods*. https://www.scribbr.com/methodology/case-study/ (accessed: 10.02.2023).

McLeod, P. (2023). *Qualitative vs quantitative research methods data analysis*. https://www.simplypsychology.org/qualitative-quantitative.html (accessed: 03.03.2023).

Medelyan, A. (2023a). *Coding qualitative data: How to code qualitative research*. https://getthematic.com/insights/coding-qualitative-data/

Medelyan, A. (2023b). *Coding qualitative data: How to code qualitative research*. https://getthematic.com/insights/coding-qualitative-data/

Mitchell, A. (2021). *How to get cybersecurity, compliance productivity to co-exist*. https://www.insightful.io/blog/cybersecurity-compliance-productivity

Oates, J. (2006). Ethical frameworks for research with human participants.

Robertson, T. (2022). *Levels of culture subculture for managing organizations.* https://smallbusiness.chron.com/introduction-organizational-structure-2774.html (accessed: 11.03.2023).

Schein, E. H. (1996). Three Cultures of Management: The Key to Organizational Learning.

Schulman, P. R. (2020). Organizational structure and safety culture: Conceptual and practical challenges. *Safety Science 126*. https://doi.org/https://doi.org/10.1016/j.ssci.2020.104669

Shaikh, F. A., & Siponen, M. (2022). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security Journal*. https://doi.org/https://doi.org/10.1016/j.cose.2022.102974

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of information systems security policy violations. *MIS Quarterly Vol. 34, No. 3*. https://doi.org/https://doi.org/10.2307/25750688

Sullivan, P. (2019). *How can organizations build cybersecurity awareness among employees?* https://www.techtarget.com/searchsecurity/tip/How-can-organizations-build-cybersecurity-awareness-among-employees

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

University, C. S. (2023). *Literature review: Systematic literature reviews.* https://libguides.csu.edu.au/review/Systematic (accessed: 16.03.2023).

Verizon. (2021). *Cybercrime thrives during pandemic: Verizon 2021 data breach investigations report.* https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report (accessed: 16.03.2023).

Walk, K. (1998). *What (exactly) is thematic analysis?* https://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis (accessed: 02.03.2023).

Watkins, M. D. (2013). *What is organizational culture? and why should we care?* https://hbr.org/2013/05/what-is-organizational-culture (accessed: 15.02.2023).

Watson, J. (2017). *When are subcultures in your organization a problem?* https://talentvanguard.com/2017/10/29/when-are-subcultures-in-your-organization-a-problem/ (accessed: 11.03.2023).

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

Winkler, I., & Brown, T. C. (2021). Security culture and behavior. https://doi.org/10.1002/9781119623946.ch9

Wong, K. (2020). *Organizational culture: Definition, importance, and development.* https://www.achievers.com/blog/organizational-culture-definition/

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2022.102520

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*. https://doi.org/https://doi.org/10.1177/0739456X17723971

Zwilling, M., Kilen, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*. https://doi.org/https://doi.org/10.1080/08874417.2020.1712269

# Appendix A

# Interview Guide to Security Leaders

**Introduction:**

- Do you consent to the data collection described in the information letter?
- Job Position?
- How long have you had this role?
- Can you describe a little more about your responsibilities?

**Interview:**

**Q1:** How do you work to ensure a secure cybersecurity culture in your organization?

- Are routines around cyber security something that is practiced and focused on regularly?
- Do you have any cybersecurity training or education measures for the employees?
- Is it a problem that people do not follow the safety rules and routines you implement?

**Q2:** Often, a lack of compliance with safety routines can result from the employees not having the competence to adapt to the changes the management makes. This results in the employees not adapting to changes because they do not want to but lack the competence to do so.

- What do you do to ensure that everyone works with something they want, are satisfied with, and simultaneously master?
- Is there a low margin for notifying the management if the employees are working with something they do not master or are unable to complete?

**Q3:** Which groups of employees/departments do you feel are more willing to adapt to changes and messages from management related to cyber security? How do you work to identify the factors that contribute to this being an adaptive cybersecurity culture?

- How does it become visible?
- Why do you think this particular subculture is more adaptable to changes and messages from management?
- How do you work to implement rules and routine reductions in this subculture?

- How do you work to identify the factors that contribute to this being an adaptive cyber security culture?

**Q4:** Which groups of employees/departments do you feel are less willing to adapt to changes and messages from management related to cyber security?

- How does it become visible?
- Why do you think this particular subculture is less adaptable to changes and messages from management?
- How do you work to implement rules and routine reductions in this subculture?
- How do you work to make this subculture more adaptable to changes in cybersecurity culture?

**Q5:** Lack of adaptability and routine changes can also result from psychology. Do you agree with this statement?

- If so, what do you do to ensure the employees know that each employee is informed about and understands the importance of maintaining collective safety routines?
- If not, are there other psychological reasons why employees do not adapt to collective safety routines?
- Do you follow up the subcultures equally should problems arise?

# Appendix B

# Interview Guide to Employees

**Introduction:**

- Do you consent to the data collection described in the information letter?
- Job Position?
- Can you describe a little more about your responsibilities?

**Q1:** How do you feel that your organizational culture is?

- If it is good, which factors do you think are decisive for you to maintain a good organizational culture?
- If it is not good, which factors do you think are decisive for you not maintaining a good organizational culture?

**Q2:** How do you work to safeguard cyber security in your organisation?

- Are routines around cyber security something that is practiced and focused on regularly?
- Have you received any cyber security training or education? (courses, guidance, training materials, etc.)
- Do you feel that management is helping to focus on and raise awareness of cyber security?
- Do you think you are getting enough follow-up regarding cyber security?

**Q3:** How do you feel your own awareness and knowledge of cyber security is?

- Do you know the most important measures you can take to increase your own awareness?
- Do you take the initiative to learn more about cyber security yourself, or only if you are told about it?
- Do you feel that lack of awareness is a problem in your department?
- Why do you think it is important/not important to adapt to changes in cyber security culture?

**Q4:** Do you think it is easy to adapt to new routines and changes in the cyber security culture?

- If so, what personal and organizational factors do you think contribute to the ease of adapting to these changes?
- If no, what prevents you from adapting to changes in the cybersecurity culture?

# Appendix C

# Information Letter to Security Leaders

Hello, and thank you for taking the time to do this interview. My name is Christer Høiland, and I am studying for a master's degree in cybersecurity at the University of Agder. I am now in the data collection period of my master's thesis. I have chosen to conduct this by interviewing employees and managers in my two partner companies.

The master's thesis aims to investigate patterns and connections related to behavior and compliance with safety routines. It is a growing problem that certain subcultures in organizations do not maintain good enough routines for cybersecurity, or do not adapt to changes in the cybersecurity landscape. This means that several of today's cyber attacks can be traced back to human error, which is often the result of a lack of information or a lack of compliance with given routines. An organizational culture consists of several subcultures, which may be distributed across departments, offices, positions, or divisions.

The interview you take part in will try to identify your relationship with, and how you, as a manager, experience the different employees in the subcultures in your company adopting new rules or changes from the management. Combined with further interviews with employees in the subcultures identified in the interviews, this will help to provide insight into similarities and differences related to competence, behavior, and compliance with safety routines across the subcultures in each partner company.

The interview will be transcribed so that I can use that content and the answers from the interview material further. You will receive a copy of the transcript after the interview, so you can gain insight into your data and, if desired, make changes.

If you don't want to answer the questions, please don't hesitate to deny. All the interviewees will be anonymized so that they cannot be linked to individuals, and all the information collected will be deleted after the completed project. If you would like your answers not to be included in the project even after the interview has been completed, you can send an e-mail to chriho18@uia.no.

Thanks for your help!

With kind regards,

Christer Høiland

# Appendix D

# Information Letter to Employees

Hello, and thank you for taking the time to do this interview. My name is Christer Høiland, and I am studying for a master's degree in cybersecurity at the University of Agder. I am now in the data collection period of my master's thesis. I have chosen to conduct this by interviewing employees and managers in my two partner companies.

The master's thesis aims to investigate patterns and connections related to behavior and compliance with safety routines. It is a growing problem that certain subcultures in organizations do not maintain good enough routines for cybersecurity, or do not adapt to changes in the cybersecurity landscape. This means that several of today's cyber attacks can be traced back to human error, which is often the result of a lack of information or a lack of compliance with given routines. At the same time, there are also many subcultures that are good at maintaining routines, and these are an equally important part of the project. An organizational culture consists of several subcultures, which may be distributed across departments, offices, positions, or divisions.

The interview you take part in will try to identify your relationship with cybersecurity culture, and how you, as an employee, experience whether cybersecurity routines are followed and adapted in their subculture. It must also be investigated whether the employees feel that the management is involved in supporting and facilitating this. Combined with further interviews with managers, this will help to provide insight into similarities and differences related to competence, behavior, and compliance with safety routines across the subcultures in each partner company.

The interview will be transcribed so that I can use that content and the answers from the interview material further. You will receive a copy of the transcript after the interview so that you can gain insight into your data and, if desired, make changes.

If you don't want to answer the questions, please don't hesitate to deny. All the interviewees will be anonymized so that they cannot be linked to individuals, and all the information collected will be deleted after the completed project. If you would like your answers not to be included in the project even after the interview has been completed, you can send an e-mail to chriho18@uia.no.

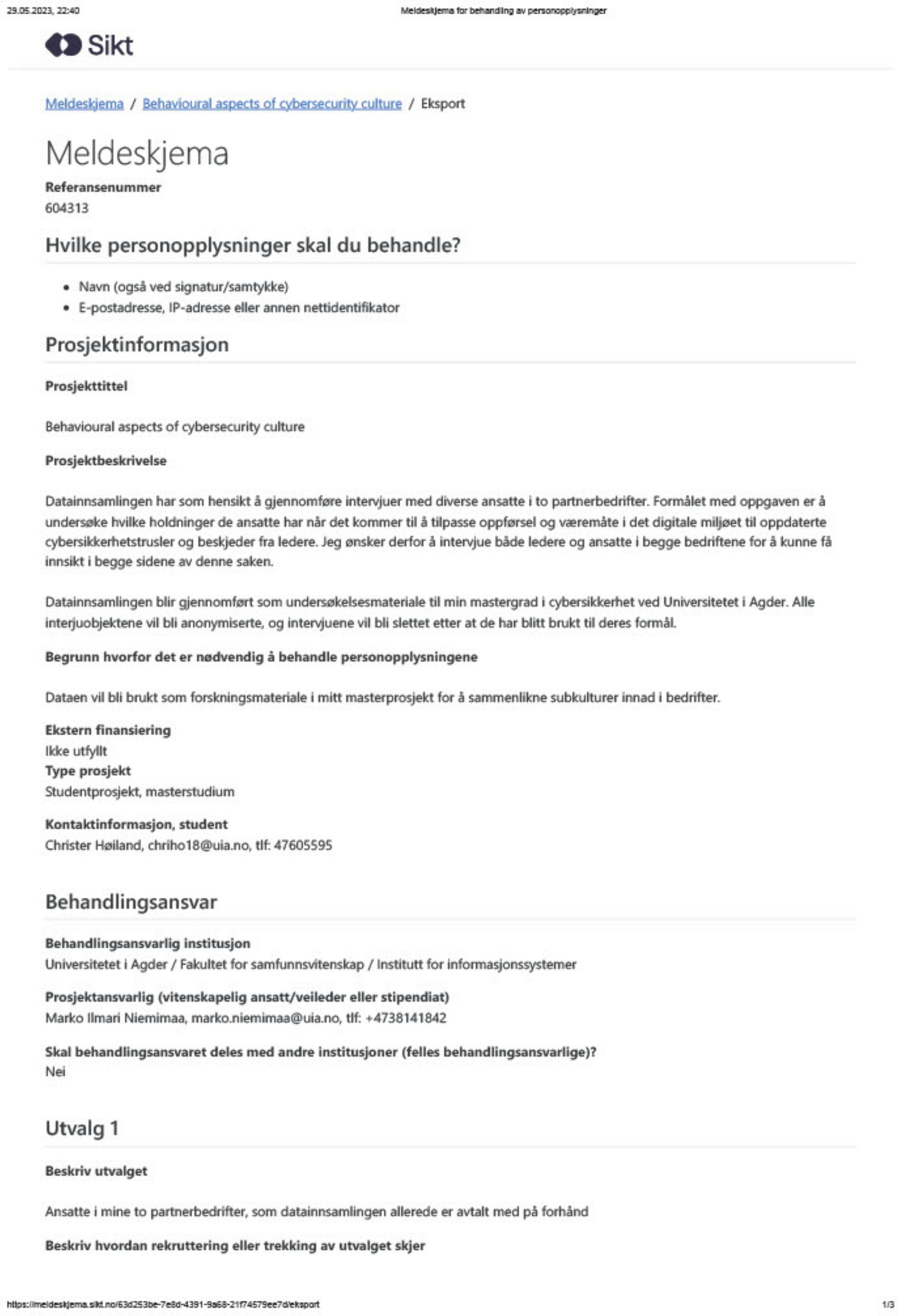
Thanks for your help!

With kind regards,

Christer Høiland

# Appendix E

# Data Management Plan (DMP) Submission



29.05.2023, 22:40 Meldeskjema for behandling av personopplysninger

Sikt

Meldeskjema / Behavioural aspects of cybersecurity culture / Eksport

## Meldeskjema

**Referansenummer**

604313

### Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator

### Prosjektinformasjon

**Prosjekttittel**

Behavioural aspects of cybersecurity culture

**Prosjektbeskrivelse**

Datainnsamlingen har som hensikt å gjennomføre intervjuer med diverse ansatte i to partnerbedrifter. Formålet med oppgaven er å undersøke hvilke holdninger de ansatte har når det kommer til å tilpasse oppførsel og væremåte i det digitale miljøet til oppdaterte cybersikkerhetstrusler og beskjeder fra ledere. Jeg ønsker derfor å intervjue både ledere og ansatte i begge bedriftene for å kunne få innsikt i begge sidene av denne saken.

Datainnsamlingen blir gjennomført som undersøkelsesmateriale til min mastergrad i cybersikkerhet ved Universitetet i Agder. Alle interjuobjektene vil bli anonymiserte, og intervjuene vil bli slettet etter at de har blitt brukt til deres formål.

**Begrunn hvorfor det er nødvendig å behandle personopplysningene**

Dataen vil bli brukt som forskningsmateriale i mitt masterprosjekt for å sammenlikne subkulturer innad i bedrifter.

**Ekstern finansiering**

Ikke utfyllt

**Type prosjekt**

Studentprosjekt, masterstudium

**Kontaktinformasjon, student**

Christer Høiland, chriho18@uia.no, tlf: 47605595

### Behandlingsansvar

**Behandlingsansvarlig institusjon**

Universitetet i Agder / Fakultet for samfunnsvitenskap / Institutt for informasjonssystemer

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**

Marko Ilmari Niemimaa, marko.niemimaa@uia.no, tlf: +4738141842

**Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?**

Nei

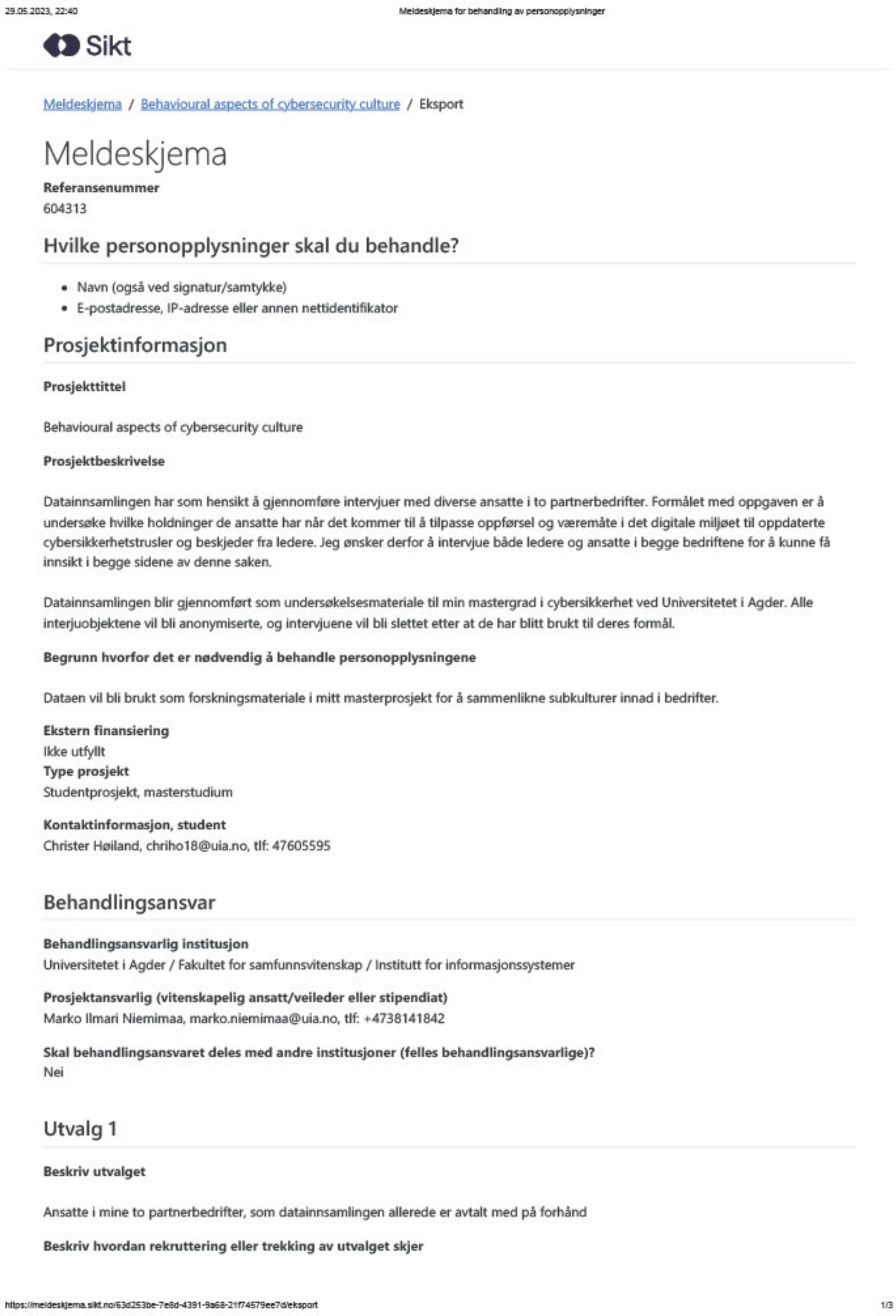
### Utvalg 1

**Beskriv utvalget**

Ansatte i mine to partnerbedrifter, som datainnsamlingen allerede er avtalt med på forhånd

**Beskriv hvordan rekruttering eller trekking av utvalget skjer**

https://meldeskjema.sikt.no/63d253be-7e8d-4391-9a68-21f74579ee7d/eksport 1/3



Sikt

Meldeskjema / Behavioural aspects of cybersecurity culture / Eksport

# Meldeskjema

**Referansenummer**
604313

## Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator

## Prosjektinformasjon

**Prosjekttittel**

Behavioural aspects of cybersecurity culture

**Prosjektbeskrivelse**

Datainnsamlingen har som hensikt å gjennomføre intervjuer med diverse ansatte i to partnerbedrifter. Formålet med oppgaven er å undersøke hvilke holdninger de ansatte har når det kommer til å tilpasse oppførsel og væremåte i det digitale miljøet til oppdaterte cybersikkerhetstrusler og beskjeder fra ledere. Jeg ønsker derfor å intervjue både ledere og ansatte i begge bedriftene for å kunne få innsikt i begge sidene av denne saken.

Datainnsamlingen blir gjennomført som undersøkelsesmateriale til min mastergrad i cybersikkerhet ved Universitetet i Agder. Alle interjuobjektene vil bli anonymiserte, og intervjuene vil bli slettet etter at de har blitt brukt til deres formål.

**Begrunn hvorfor det er nødvendig å behandle personopplysningene**

Dataen vil bli brukt som forskningsmateriale i mitt masterprosjekt for å sammenlikne subkulturer innad i bedrifter.

**Ekstern finansiering**
Ikke utfyllt
**Type prosjekt**
Studentprosjekt, masterstudium

**Kontaktinformasjon, student**
Christer Høiland, chriho18@uia.no, tlf: 47605595

## Behandlingsansvar

**Behandlingsansvarlig institusjon**
Universitetet i Agder / Fakultet for samfunnsvitenskap / Institutt for informasjonssystemer

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**
Marko Ilmari Niemimaa, marko.niemimaa@uia.no, tlf: +4738141842

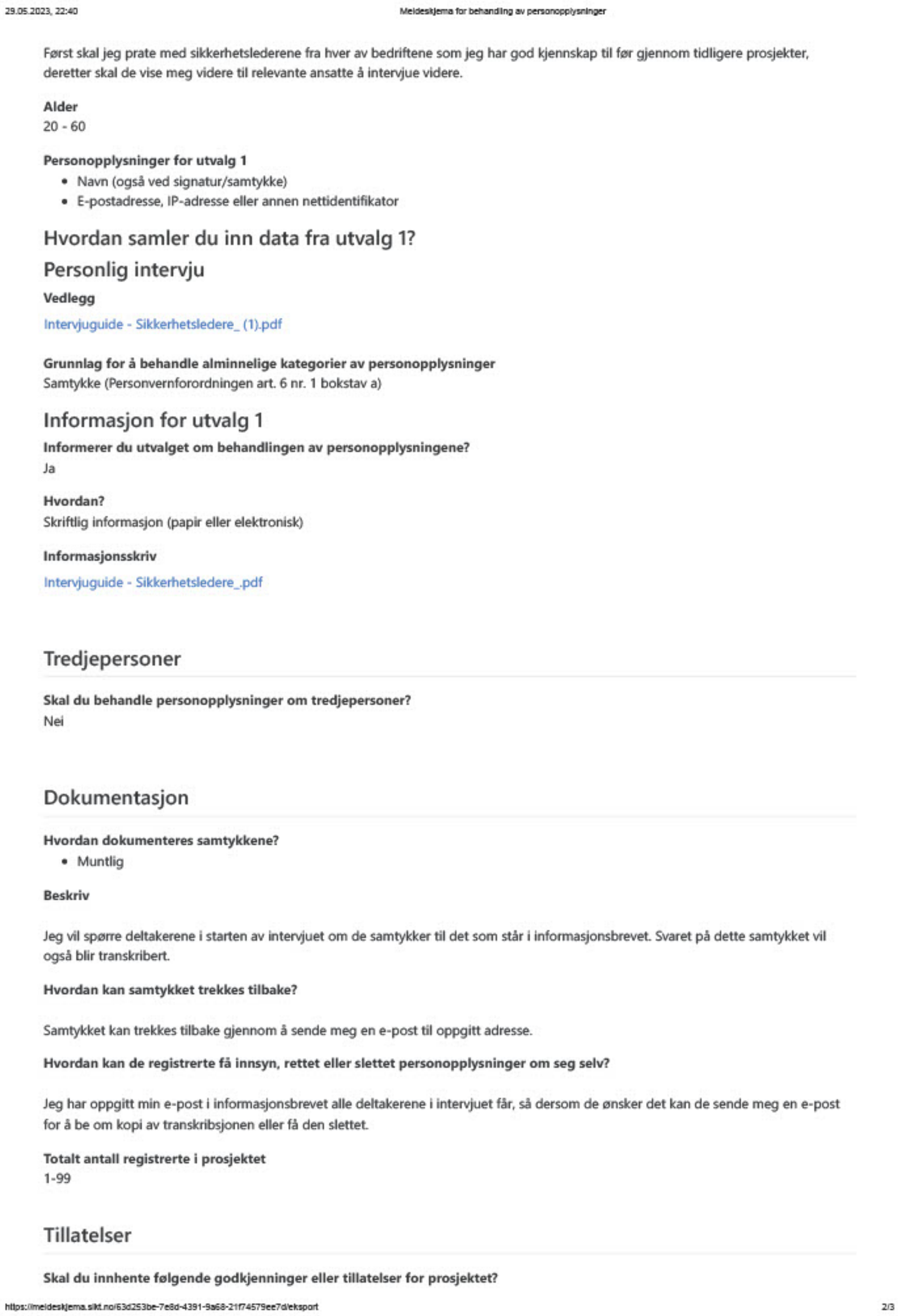
**Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?**
Nei

## Utvalg 1

**Beskriv utvalget**

Ansatte i mine to partnerbedrifter, som datainnsamlingen allerede er avtalt med på forhånd

**Beskriv hvordan rekruttering eller trekking av utvalget skjer**



Først skal jeg prate med sikkerhetslederene fra hver av bedriftene som jeg har god kjennskap til før gjennom tidligere prosjekter, deretter skal de vise meg videre til relevante ansatte å intervjue videre.

**Alder**

20 - 60

**Personopplysninger for utvalg 1**

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator

### Hvordan samler du inn data fra utvalg 1?

### Personlig intervju

**Vedlegg**

Intervjuguide - Sikkerhetsledere_ (1).pdf

**Grunnlag for å behandle alminnelige kategorier av personopplysninger**

Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

### Informasjon for utvalg 1

**Informerer du utvalget om behandlingen av personopplysningene?**

Ja

**Hvordan?**

Skriftlig informasjon (papir eller elektronisk)

**Informasjonsskriv**

Intervjuguide - Sikkerhetsledere_.pdf

## Tredjepersoner

**Skal du behandle personopplysninger om tredjepersoner?**

Nei

## Dokumentasjon

**Hvordan dokumenteres samtykkene?**

- Muntlig

**Beskriv**

Jeg vil spørre deltakerene i starten av intervjuet om de samtykker til det som står i informasjonsbrevet. Svaret på dette samtykket vil også blir transkribert.

**Hvordan kan samtykket trekkes tilbake?**

Samtykket kan trekkes tilbake gjennom å sende meg en e-post til oppgitt adresse.

**Hvordan kan de registrerte få innsyn, rettet eller slettet personopplysninger om seg selv?**

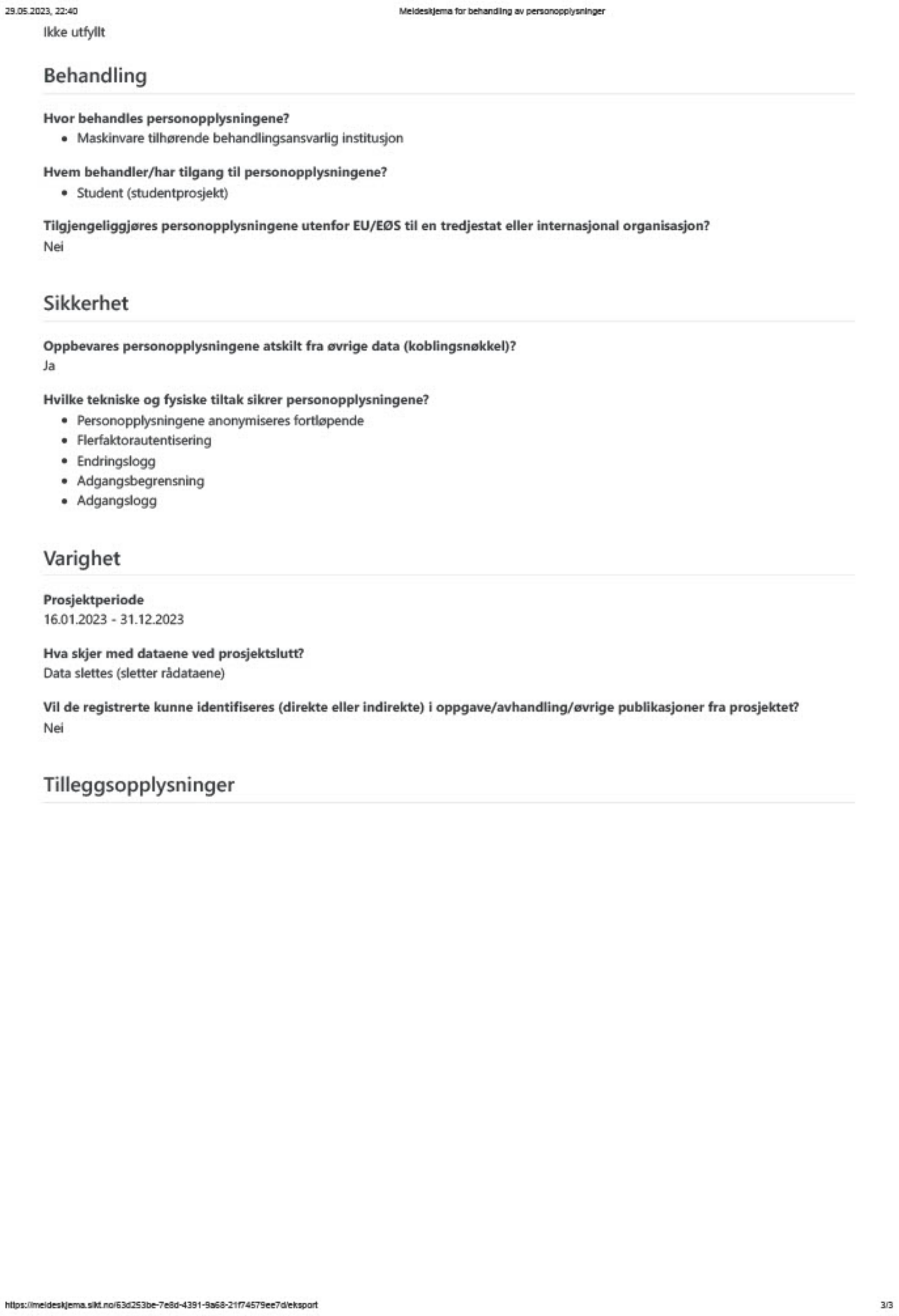
Jeg har oppgitt min e-post i informasjonsbrevet alle deltakerene i intervjuet får, så dersom de ønsker det kan de sende meg en e-post for å be om kopi av transkribsjonen eller få den slettet.

**Totalt antall registrerte i prosjektet**

1-99

## Tillatelser

**Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?**



29.05.2023, 22:40 Meldeskjema for behandling av personopplysninger

Ikke utfyllt

## Behandling

**Hvor behandles personopplysningene?**

- Maskinvare tilhørende behandlingsansvarlig institusjon

**Hvem behandler/har tilgang til personopplysningene?**

- Student (studentprosjekt)

**Tilgjengeliggjøres personopplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?**

Nei

## Sikkerhet

**Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?**

Ja

**Hvilke tekniske og fysiske tiltak sikrer personopplysningene?**

- Personopplysningene anonymiseres fortløpende
- Flerfaktorautentisering
- Endringslogg
- Adgangsbegrensning
- Adgangslogg

## Varighet

**Prosjektperiode**

16.01.2023 - 31.12.2023

**Hva skjer med dataene ved prosjektslutt?**

Data slettes (sletter rådataene)

**Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?**

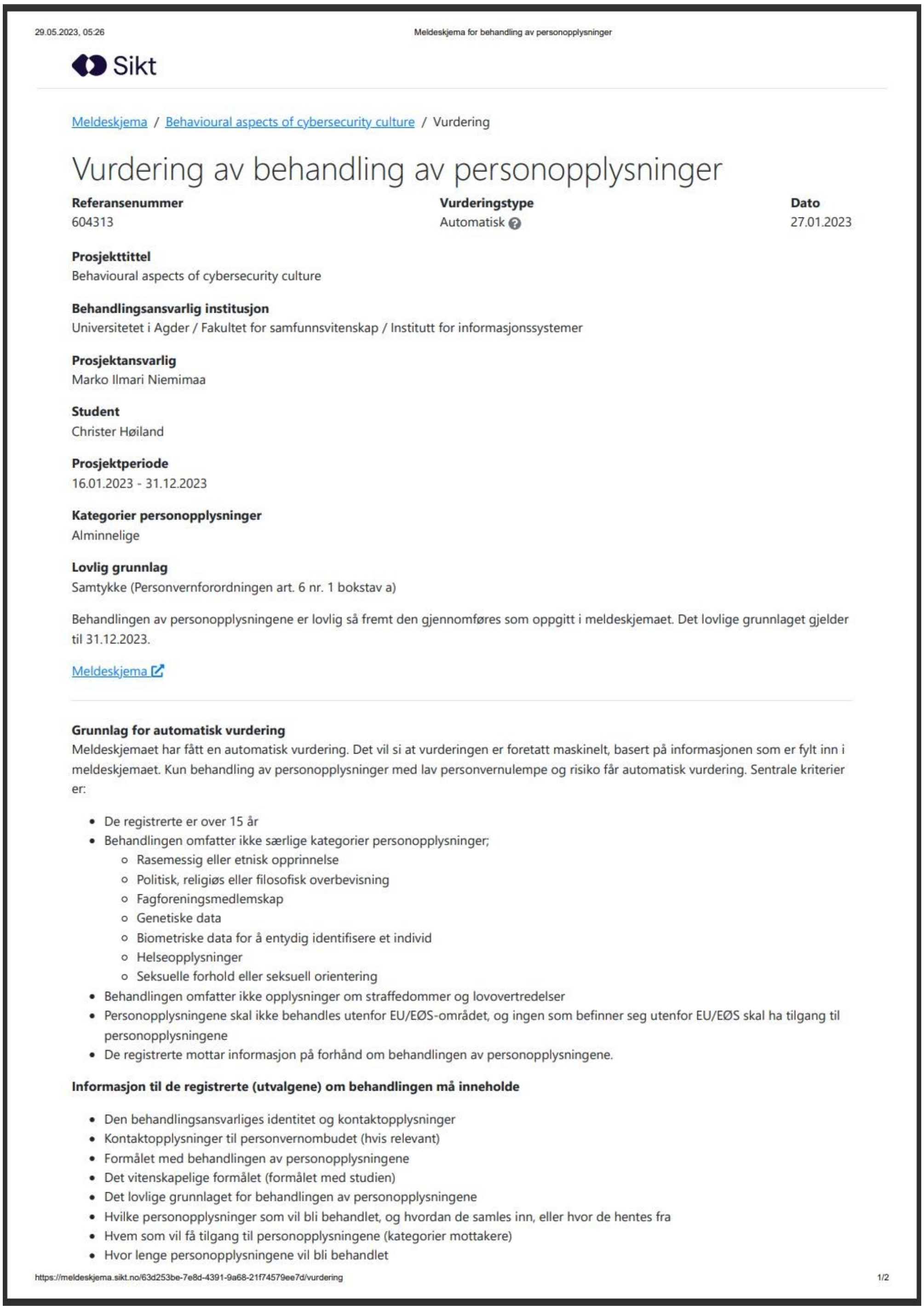
Nei

## Tilleggsopplysninger

https://meldeskjema.sikt.no/63d253be-7e8d-4391-9a68-21f74579ee7d/eksport 3/3

# Appendix F

# NSD Approval



29.05.2023, 05:26 Meldeskjema for behandling av personopplysninger

Sikt

Meldeskjema / Behavioural aspects of cybersecurity culture / Vurdering

## Vurdering av behandling av personopplysninger

| Referansenummer | Vurderingstype | Dato |
|---|---|---|
| 604313 | Automatisk | 27.01.2023 |

**Prosjekttittel**
Behavioural aspects of cybersecurity culture

**Behandlingsansvarlig institusjon**
Universitetet i Agder / Fakultet for samfunnsvitenskap / Institutt for informasjonssystemer

**Prosjektansvarlig**
Marko Ilmari Niemimaa

**Student**
Christer Høiland

**Prosjektperiode**
16.01.2023 - 31.12.2023

**Kategorier personopplysninger**
Alminnelige

**Lovlig grunnlag**
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 31.12.2023.

Meldeskjema

**Grunnlag for automatisk vurdering**
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

**Informasjon til de registrerte (utvalgene) om behandlingen må inneholde**

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)
- Hvor lenge personopplysningene vil bli behandlet

https://meldeskjema.sikt.no/63d253be-7e8d-4391-9a68-21f74579ee7d/vurdering 1/2