UMEÅ UNIVERSITY

SECURING THE FUTURE:

Exploring Barriers to Sustainable Cybersecurity Practices

Andrea Egelrud and Johanna Holmgren

Department of informatics
Master thesis, 15 hp
IT Management
SPM 2024.01

Abstract

Organizations are embracing technological solutions to improve efficiency; however, this also opens organizations to new threats. The rapid development of new technology, such as AI, combined with a changing threat landscape, puts organizations under pressure to adapt. Simultaneously, the EU has proposed a new directive that forces organizations to adopt stricter cybersecurity measures. This raises the question of how organizations can create sustainable cybersecurity practices that will ensure safety over time despite rapid changes in the environment. This has resulted in the following research question: What are the barriers to establishing sustainable cybersecurity practices? To answer this question, ten semi-structured interviews with experts in the cybersecurity field were conducted. Five barriers were identified: (1) barriers in cybersecurity activities, (2) barriers of existing resources, (3) barriers in the human factor, (4) technical barriers, and (5) external barriers, which contribute to bridging the gap between best practices established in research and issues that practitioners are facing. Further, it contributes to an understanding of the importance of a more holistic approach to cybersecurity measures contributing to previous research within the field of IS.

Keywords: Cybersecurity practices, Awareness, Readiness, Competencies

1. Introduction

Organizations have greatly benefited from using digital technologies, devices, and interconnectivity in various ways (Hasan, Ali, Kurnia & Thurasamy, 2021). With digital technology, organizations can improve their efficiency, communication speed, and system accessibility and reduce operating costs (Hasan et al., 2021). Digital transformation has become more critical for organizations' survival in recent years, forcing organizations to engage with digital transformation (Vial, 2019). According to Jada and Mayayise (2023), organizations must quickly develop and accept new and improved technology due to digital transformation. However, the advancement of digital transformations within companies also includes certain risks, such as cyberattacks (Hasan et al., 2021; Jada & Mayayise, 2023). Further, as technology evolves, organizations see potential in integrating technologies such as Artificial Intelligence (AI) and Machine Learning (ML). However, these adoptions enable consequences that target society, individuals, and organizations with increased cybercrimes, attacks, and vulnerabilities (Jada & Mayayise, 2023).

AI is an intelligent technology that is being used to replace traditional approaches (Berente, Gu, Recker, & Santhanam, 2021; Heyder, Passlack, & Posegga, 2023; Holmström, 2022). With the introduction of AI, technology has been upgraded, but there has also been an increased sophistication of cyber threat actors. This has resulted in the introduction of a new era where AI and ML have made cyberattacks more effective and cyber offenders more powerful than ever before (Gupta, Akiri, Aryal, Parker, & Praharaj, 2023). This has made generative AI an interesting topic for the cybersecurity community concerning cyber defense and offense due to it being beneficial for both parties (Gupta et al., 2023).

Considering the evolving threats and cybercrimes enabled through digitalization and new technology, such as AI, the EU is launching a new/upgraded directive, NIS2 (Network and Information Security Directive). This directive includes more substantial requirements directed to a larger range of sectors than the previous version of NIS (see Appendix 1). The directive is mainly aimed at organizations that fulfill an important role in the upkeep of society and will raise the minimum level of safeguarding (The NIS2 Directive, 2024b). However, research has shown that while standards, such as NIS, can recommend policies and technical solutions, these always need to be implemented to consider the context of an organization's specific cybersecurity risks (Siponen & Willison, 2009). Despite this, the NIS2 Directive will be translated into EU members' national laws in October 2024, requiring swift action from affected organizations to stay compliant (The NIS2 Directive, 2024a).

Consequently, due to constraints regarding resources and time, the needed adaptation for the directive may seem disconnected from the reality for organizations. While there are numerous frameworks that practitioners can consider, organizations face practical challenges such as time constraints, budgetary limitations, and constant pressure, making these frameworks difficult to apply. The difficulty of applying current frameworks combined with an ever-evolving threat landscape and new regulatory requirements to fulfill raises the question of how organizations can create sustainable cybersecurity practices. Sustainable cybersecurity practices can be understood as organizations' ability to adapt to current and future developments, such as an increasing threat level, new technology, or regulatory requirements. The word practice is used since building cybersecurity in an organization involves integrating security behavior into practice.

In this study, we aim to create an understanding of what barriers exist to establishing sustainable cybersecurity practices to better bridge the gap between best practices established in research and issues that practitioners are facing. This has resulted in the following research question: What are the barriers to establishing sustainable cybersecurity practices?

By answering this question, we will contribute by identifying barriers to establishing sustainable cybersecurity practices. In turn, this will give a better understanding of the difficulties of applying best practices established in research and contribute towards understanding a more holistic approach for cybersecurity measures identified by Dhillon, Smith, and Dissanayaka (2021) as lacking in the field of Information Systems.

2. Related Research

In the chapter, research related to our research question, "What are the barriers to establishing sustainable cybersecurity practices?" will be presented. The research that will be presented aims to situate cybersecurity, present trends and regulations, and finally, present cybersecurity practices.

2.1 Situating Cybersecurity

Cybersecurity is a wide concept where multiple researchers have suggested definitions (Craigen, Diakun-Thibault, & Purse, 2014; Scala, Reilly, Goethals, & Cukier, 2019; Shaikh & Siponen, 2023; Szczepaniuk & Szczepaniuk, 2022). Hasan et al. (2021) define cybersecurity as

the process of securing the IT-related assets, such as data, systems, and networks of an organization, from digital attacks that could access, destroy, and/or change information, leading to potential disturbances in business operations. Further, the practice of cybersecurity involves merging people, processes, and technology to safeguard organizations, individuals, or networks from digital attacks (Hasan et al., 2021).

The terms cybersecurity and information security are often used interchangeably; however, they are not synonymous (von Solms & van Niekerk, 2013). Cybersecurity can rather be seen as a subset of information security, where the focus is on upholding integrity, confidentiality, and accessibility of digital assets interlinked via the internet (von Solms & von Solms, 2018). Within the field of Information Systems (IS), both information security and cybersecurity are used, as well as the term Information Systems security (IS security). IS security can be defined as the practice of protecting information handling at a technical, formal, and informal level (Dhillon et al., 2021). Considering the definitions described above, cybersecurity can be seen as a subset of IS security contributing to the field of IS.

Dhillon et al. (2021) have summarized the last three decades of IS security research within the IS field, resulting in a conceptual model consisting of two overarching categories of research streams with two substreams each. The two overarching research streams are studies of the technical system and studies of the social system. The substreams within the technical system are research on (1) *technology,* which focuses on technological applications such as threat detection, and research on (2) *tasks,* which focuses on issues regarding system design, such as access management. Within research on the social system, the substreams include studies of (3) *structures* and (4) *people*. Research regarding structures tends to focus on the impact of laws and regulations, while research regarding people focuses on the impact behaviors of individuals have on security (Dhillon et al., 2021). Table 1 shows an overview of Dhillon et al. (2021) summarization with definitions and examples references of the different research streams.

Overview of Research Streams			
Technical System		Social System	
Technology	Tasks	Structures	People
Research focusing on themes like cybersecurity attacks by exploring technology for detection and avoiding attacks	Research focusing on issues connected to system design and vulnerability management	Research focusing on the impact on cybersecurity caused by laws and regulations such as policies and procedures	Research focusing on the behavior of individuals and the impact on cybersecurity
Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010; Patterson, Hobbs, & Zhu, 2017; Ramesh, Krishnamurthi, & Kumar, 2014	Cheng, 2000; Khan & Madnick, 2019 Steinbart, Keith, & Babb, 2016; Zviran & Haga, 1999	Karjalainen, Sarker, & Siponen, 2019; Moody, Siponen, & Pahnila, 2018; Nazareth, & Choi, 2015; Paananen, Lapke, & Siponen, 2020	Herath & Rao, 2009; Ifinedo, 2014; Li, He, Xu, Ash, Anwar, & Yuan, 2019; Vance, Siponen, & Pahnila, 2012

Table 1. Research streams within IS security (adopted from Dhillon et al. 2021)

In relation to the research streams, we will contribute with a more holistic approach, looking at cybersecurity as a socio-technical system, and viewing barriers that touch on all four streams.

2.2 Trends in Cybersecurity & External Regulations

Today cybersecurity is of great importance for organizations' survival. Warkentin and Willison (2009) express that external factors such as the global market, economic and political stability, as well as technological- and socio-cultural development all impact an organization's environment providing instability. In turn, this makes cybersecurity central for an organization's survival. The introduction of generative AI is an example of technological development that has changed the field of cybersecurity by introducing new and more efficient cyberattacks (Gupta et al., 2023). Gupta et al. (2023) further express that AI can present both opportunities and challenges for organizations, empathizing that it can be used both for defense and attacks. The changing characteristics of the threats are further affecting organizations' ability to protect themselves today. Previously, the actors behind the attacks used to be typical cybercriminals, however, today the actors also include state-affiliated groups and terror organizations (Pawlak & Barmpaliou, 2017).

The NIS Directive was created to respond to the vulnerability resulting from the reliance on information systems and networks in critical infrastructure. Inadequate safety measures threaten not just individual organizations or countries but the whole internal market of the European market since disruption of IT services can cause a ripple effect. Thereby, there was a need to increase the minimum threshold for cybersecurity measures within the EU to raise the common level of security (Markopoulou, Papakonstantinou, & De Hert, 2019). The NIS Directive was incorporated into the legislation of all EU members and improved cybersecurity; however, it is no longer adequate for the increasing threat level resulting in the updated NIS2 directive (Schmitz-Berndt, 2023).

NIS2 has expanded the entities being included in the directive and included state-of-the-art standards and cybersecurity measures that organizations should adhere to (see Appendix 1). Further, the new directive emphasizes management's responsibility and accountability for compliance with cybersecurity requirements and introduces sanctions for not following the requirements, including a maximum fine of 10 million euros or 2% of an organization's annual turnover (Sievers, 2021). The directive also stresses the importance of reporting incidents, requiring organizations to report all incidents that are capable of causing harm. Reporting incidents is important for understanding the threat landscape and heightening the threat intelligence within the different sectors through information sharing (Schmitz-Berndt, 2023).

2.3 Cybersecurity Practices

Sustainable cybersecurity practices are related to both technical and human factors. Therefore, this part of the related research will bring up research related to the human factor of sustainable cybersecurity, concerning *employee awareness* and *security within organizations*.

2.3.1 Employee Awareness

There are both external and internal threats that enable cybersecurity risks within an organization. According to Ifinedo (2014), employees within an organization are the internal threat that can cause disturbance regarding information security. Human error is often defined as the weakest link in an organization's cybersecurity (Pranggono & Arabo, 2021). To improve organizational security, it is important to focus on formal and informal structures, such as policies, procedures, the employees' role in ensuring security, and organizational culture (Herath & Rao, 2009). Organizations find it difficult to maintain security mainly due to employees not understanding the importance of security practices. Therefore, they are unwilling to follow the organization's existing policies to improve safeguarding (Herath & Rao, 2009). Ifinedo (2014) further explains that managers have a responsibility to ensure that the cybersecurity practices are not too burdensome for employees since this can lower employees' willingness to take responsibility for their actions.

The organizational environment can be a sufficient motivating factor for employees to follow directives due to employees being influenced by their colleagues. To clarify, if their colleagues follow the existing policies and regulations, it is more likely that others will follow their behavior and actions (Herath & Rao, 2009; Li, He, Xu, Ash, Anwar & Yuan, 2019). To accomplish awareness within an organization despite existing knowledge gaps, the management must ensure an organizational structure with established and clear authority, providing employee training and efficient communication (Li et al., 2019). Furthermore, with a formal structure, management can develop policies and procedures with established authority and provide employees with workshops, seminars, and training regarding cybersecurity compliance (Li et al., 2019).

Having cybersecurity routines might not guarantee success if the training materials are outdated leading to insufficient interest from the employees. Insufficient interest among the employees can hinder the overall cybersecurity strategy (Yusif & Hafeez-Baig, 2021). To ensure that employees recognize the potential dangers that threats present to the organization the security practices and procedures must be easy to use and understand for the employees (Vance, Siponen & Pahnila, 2012).

2.3.2 Security within Organizations

In recent years, organizations have invested more heavily in their security budgets. However, Li, Leung, and Yue (2023) further explain that research shows that organizations' security budgets are not efficiently spent and that poorly integrated security solutions in organizations can decrease returns on security investments. Furthermore, an issue that may occur when organizations see security and IT investments as independent investments is that the IT investments are not seen as enough to handle the organizations' questions regarding security solutions (Li et al., 2023). To solve these breaches, organizations need to invest in *security awareness*. To ensure security awareness, the senior management must engage in maintaining security, but it also focuses on creating a consistent feeling of awareness regarding security threats and adequate responses (Li et al., 2023). Furthermore, Hasan et al. (2021) argue that it is important that organizations are aware, prepared, and committed to prevent and combat external cyberattacks. However, if the management and employees within an organization

have the belief that their organization is not at risk for cyberattacks, their cybersecurity readiness will be affected by the attitude.

According to Ifinedo (2014) organizations, regardless if they are private or public, are investing a lot in information systems for protection. To achieve perimeter defense, organizations deploy firewalls and monitoring systems such as data leakage prevention and log management. The risks being enabled due to organizations' reliance on information systems provide organizations with major challenges, and sometimes, these risks are only managed by technology-based solutions (Bulgurcu, Cavusoglu & Benbasat, 2010).

By relying on technology-based solutions, organizations can improve their information security to some extent, but the solution itself is not enough to reduce the risks. To reduce security risks successfully, organizations need to invest in technical and socio-organizational measures (Bulgurcu et al., 2010; Ifinedo, 2014). To avoid conflicts between business and security, organizations must enable a wide understanding of countermeasures that help them explore practical solutions (Li et al., 2023). Ensuring the socio-organizational measure indicates that organizations need to enable a cybersecurity culture. A definition of information security culture used by Da Veiga, Astakhova, Botha, and Herselman (2020) is presented below.

> *"Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives." (Da Veiga et al., 2020, p. 19)*

Alshaikh (2020) also uses this definition to describe cybersecurity culture. Further, Alshaikh (2020) explains that enabling a cybersecurity culture is essential to protect the organization from internal incidents caused by employees. With a cybersecurity culture, management can change employees' behavior and make compliance with information security a natural aspect of their daily activities. To achieve this, organizations must go beyond usual computer-based training and adopt a broader approach to develop new skills. The broader approach further enables the possibility of changing attitudes, perceptions, routines, and assumptions in the organization (Alshaikh, 2020). Beyond training, management can also engage in internal meetings with their employees to review the importance of security compliance (Alshaikh, 2020). Johnson and Goetz (2007) also point out the important role managers, at all levels, play in fostering a cybersecurity culture. Like Alshaikh (2020), Johnson and Goetz (2007) also suggest managers engage with employees by asking security questions to keep cybersecurity as a relevant subject.

3. Methodology

3.1 Qualitative Method

This study will follow a qualitative research method. The choice behind this method is based on the social context we want to investigate, which is made possible when following a qualitative research method (Myers, 2013). In this study, we want to create an understanding of what barriers impact the possibility of establishing sustainable cybersecurity practices, in the pressuring context of the new NIS2 directive and technological developments. With a qualitative research method, we can understand the reasoning behind decisions regarding cybersecurity measures by talking to relevant respondents who are working closely with security questions in their organization. A qualitative research method allows us to understand people, motivations, and actions while considering a broader context that might impact (Myers, 2020). If a quantitative research method had been applied in our study, a large sampling would have been required, which might have made results more generalizable; however, the social context would have been lost, leading to a more shallow understanding of the respondents' actions in this particular context, nor would we get access to their insights and thoughts to the same extent (Myers, 2013; Myers, 2020). The method has also been inspired by the Delphi method where the respondents participate by providing expertise on a subject (Brender, Ammenwerth, Nykänen & Talmon, 2006). In this study, the Delphi method has guided the selection of the respondents, where cybersecurity experts have been selected to provide insights regarding barriers to establishing sustainable cybersecurity practices.

3.1.1 Data Collection

Data was gathered through semi-structured interviews with eleven respondents. Our study involved experts from various organizations and various roles in cyber- and information security. This diversity helped us get a better understanding of different challenges that organizations might encounter when trying to establish sustainable cybersecurity practices. There are other ways to gather data besides interviews, such as observation and document analysis. Observations could have been used as a method for the data collection by observing the respondents while they perform their daily tasks to gather insights into how cybersecurity work is performed. This could have garnered insights into potential challenges that the respondents might face. However, this method would have required us to get access to a respondent's workplace and spend a lot of time observing them which Myers (2013) describes as one of the biggest hindrances when doing observation. Further, gathering additional data through documents would have been a possibility to get access to existing cybersecurity policies and strategies within the organizations. However, this would not provide additional data to help us answer the research question: “What are the barriers to establishing sustainable cybersecurity practices?”. Therefore, we found interviews to be the most suitable approach to gather valuable data for our study.

3.1.2 Interviews

Semi-structured interviews were performed since it allowed us to follow an interview guide with prepared questions while also leaving room to improvise and ask follow-up questions, allowing further insight from the respondents (Myers, 2020). The same interview guide was

used for all interviews. The decision was made even though respondents had different roles and worked in different organizations. The reasoning for the decision was due to the respondents all working within the same field and our interest in understanding what barriers existed to building sustainable cybersecurity practices in each organization. We, therefore, deemed that the interview guide would be general enough for all the respondents to answer despite the different contexts they work in. However, given the different roles and focus areas the respondents had, some found certain questions difficult to answer initially. Despite this, given that the interviews were semi-structured this still allowed for space in the conversation where respondents could ask for clarification of the questions.

The interview guide included four main categories; technology, strategy, organization, and environment (see Appendix 2). The first part of the interview guide contained introductory questions regarding the role and experience in cybersecurity. The second part of the interview guide focused on the four categories, technology, strategy, organization, and environment. These categories were inspired by reoccurring themes within previous research. In Related Research, research regarding technology is presented both by Dhillon (2021) and is further described in 2.3.2 *Security within Organizations* where eg. technical tools for security are discussed by Ifinedo (2014). Questions related to the technology theme focused on the technology and technological solutions used within the organization. The strategy theme can mainly be found in *2.3.1 Employee Awareness* where the importance of formal structures such as policies and procedures are presented. In the interview guide, strategy mainly focused on questions regarding existing strategies, resources, and policies, and how these are adopted and continuously being worked on in the organizations. The organization theme is discussed in both *2.3.1 Employees Awareness* and *2.3.2 Security within Organizations* where the role of culture, education, and awareness is presented by researchers. The organization theme in the interview guide therefore contained questions about the overall and day-to-day work with information- and cybersecurity, such as education for employees, and culture concerning cybersecurity. Research regarding the environment theme can be found in *2.2 Trends in Cybersecurity & External Regulations*. The last theme in the interview guide, therefore, focused on external threats, regulations, and laws such as NIS2.

All the interviews were performed on Microsoft Teams to ensure that we gathered the data following the GDPR regulation from Umeå University. The first interview was a pilot interview where we checked how well the interview guide worked and deemed no changes to be required. All interviews were performed in Swedish, due to it being the native language of the respondents. According to Myers (2020), the interviews should be held in the native language of the respondents because it is important to make the respondents comfortable in this situation. Furthermore, in one of the interviews, two respondents participated together which we also accepted due to the statement of Myers (2020) that the participants should feel comfortable.

3.1.3 Sampling Technique

The sampling technique used was purposive sampling, meaning that the participating respondents were chosen because of their experience with the subject of the study (Yin, 2013). All respondents work within the field of cybersecurity and information security which is

relevant for the subject of this study to gather relevant data (Yin, 2013). A critical reflection of our sampling of respondents is that the number of respondents cannot be generalized with the overall organizations within Sweden. As described above in the "Qualitative method" this study has taken inspiration from a Delphi method where one of the focus areas is to gather data from experts within a certain area (Brender et al., 2006). The participants of this study are seen as experts due to their knowledge regarding cyber- and information security and could therefore contribute knowledgeable information to answer the existing research question. A description of the respondents can be seen in Table 2.

Respondents	Role	Work title	Time
Respondent 1	Manager	Chief data officer	35
Respondent 2	Consultant	Junior Cybersecurity Consultant	36
Respondent 3	Consultant	IT - Consultant	59
Respondent 4	Employee	Information security officer	34
Respondent 5	Manager	Security Manager	57
Respondent 6	Manager	Security Manager	48
Respondent 7	Consultant	Cybersecurity Infrastructure Specialist	52
Respondent 8	Employee	Information Security Coordinator	58
Respondent 9	Employee	Cybersecurity Strategist	58
Respondent 10	Consultant Manager	Information Security Consultant	59
Respondent 11	Manager	Chief Information Security Officer	42

Table 2: Description of respondents

3.2 Data Analysis

The thesis followed a thematic analysis by Braun and Clarke (2006) for analyzing the data. Thematic analysis allows for flexibility when analyzing the empirical data but can still provide detail and complexity. Which was ideal when working with rich and detailed data from many different contexts like in this study. Even though thematic analysis provides flexibility, critique has been stated of the risk of possibly losing structure due to the absence of clear guidelines (Bruan & Clarke, 2006). There are six phases in a thematic analysis to consider: (1) *Familiarizing yourself with the data* (2) *Generating initial codes*, (3) *Searching for themes*, (4) *Reviewing themes*, (5) *Defining and naming themes* and (6) *Producing the report* (Braun & Clarke, 2006).

For the first step of getting familiar with our data, the transcription of the interviews was a part of that process. Although Microsoft Team's live transcription tool was used initially to ease the process of transcribing the ten interviews. The transcriptions were all double-checked for mistakes to ensure that the finished transcriptions were accurate. Further, this allowed us to become more familiar with the data. As all interviews were held in Swedish, quotes from the

interviews had to be translated into English. The translations have been done carefully to preserve the context and meaning of the quote to ensure an accurate description of respondents' statements.

Following the first step, we created initial codes (approximately 232 codes) that were close to the text, which later were aggregated into fourteen categories. In turn, these were then combined into five themes that represented barriers that the organization faced when trying to establish sustainable cybersecurity strategies. The final barriers were rewired several times by comparing initial data in its context to the final aggregate form. The final barriers were (1) barriers in cybersecurity activities, (2) barriers of existing resources, (3) barriers in the human factor, (4) technical barriers, and (5) external barriers. An example of how the data was coded can be seen in Figure 1, and the entire coding tree for all the barriers can be found in Appendix 3.

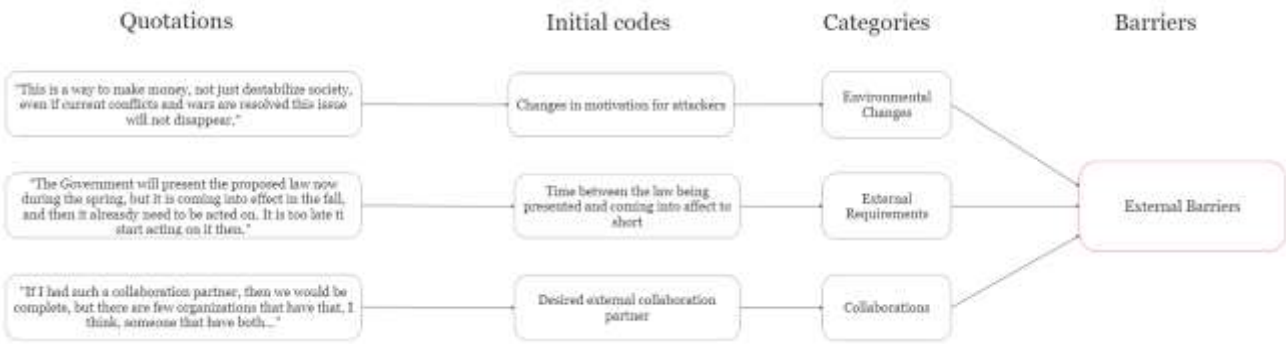

Figure 1: Example of coding, from quote to barrier.

3.3 Ethical Considerations

When conducting research, ethical considerations are an important part that has to be included. Vetenskapsrådet (2002) explains that there are rules that have to be included when performing qualitative research, which implies information and consent. Concerning information requirements, each participant has received information consent including details regarding the subject of the thesis, its purpose, and how the data is being handled. In this consent, the participants have been further informed that their participation is voluntary, which means that they can cancel or withdraw their participation at any time in the process (Vetenskapsrådet, 2002). Furthermore, the consent requirement has been taken into consideration where consent was obtained from each participant when active involvement from the participants was taking place (Vetenskapsrådet, 2002). Lastly, in our research, we have also followed the university's guidelines regarding GDPR, which involves data collection, and storage. In consideration of these guidelines, the gathered data has been collected via and stored in a safe platform provided by the university.

4. Results

In this chapter the result to the question "What are the barriers to establishing sustainable cybersecurity practices?" will be presented in relation to the themes that were created through

the data analysis. The themes are (1) *barriers in cybersecurity activities*, (2) *barriers of existing resources,* (3) *barriers in the human factor*, (4) *technical barriers*, and (5) *external barriers*. The sub-themes presented under the barriers are based on the categories also found in the data analysis.

4.1 Barriers in Cybersecurity Activities

4.1.1 Strategy

All respondents claimed that they have activities for cybersecurity issues, but it requires continuous work and that you can never be 100 percent secure. Many of the respondents explained that they sent out fake phishing emails within the organization to create more awareness, and if the employees fail some respondents explained that they have to participate in further education. However, one respondent explained that it is difficult to reach all employees depending on their role within the organization. "*If you don't work with cybersecurity [...] it's like it ends there. There is no expressed way of working or method or strategy for what to do next, instead, it's like when you have done the education you are seen as done and ready.*" (R3). Further, there is no stated strategy or method of how to work with cybersecurity, they provide one introductive education, but the respondent experienced that it ends there. There is also a desire for resources and time to talk about cybersecurity in meetings.

Due to the increased attacks on companies, one respondent explains that they have a continuous management plan where they inventory their systems. One strategy is also to restrain the rights and accessibility of the systems according to another respondent. A more detailed follow-up is also wanted by one respondent, further, that it is difficult to reach out to everyone in a big organization and a communication plan might not be enough at all times.

Some other respondents also explained that companies possess insufficient preparedness such as backup and exercises for crises. There are many different strategies that the respondents explained such as education, meetings, inventories, sending out fake phishing mail, tests, and internal and external revisions.

4.1.2 Policy and Guidelines

In the interviews, the respondents explained that there are existing policies and guidelines concerning cybersecurity. However, one respondent explained that there is no explicit cybersecurity policy but rather an information security policy that the company has. A few more respondents explained that cybersecurity is not separated from information security in this matter.

> *"[...] but today we have an IT policy, and we have an information security policy, so we'll see what becomes of these in the future. But it is not purely against cybersecurity, but it is probably more information security policy that governs there then." -R6*

Some of the respondents explained that they are certified by ISO and have that as a guideline when working with security. Information regarding guidelines is provided through education and workplace meetings according to one respondent, however, there is still difficulty in

communicating the importance of policies to all employees. Further, another deficiency explained was that new guidelines are not communicated formally within the organization. However, another respondent emphasized the importance of communication when implementing policies "*When it is implemented, it must be communicated, so it is not possible to just write a document and determine and then think that much will happen*" (R9). Many of the respondents agreed that policies and guidelines require systematic and continuous work. The policies and guidelines explained in the interviews often included secure passwords, not clicking on unknown links, encryption of mail, reporting incidents, handling of data, log management/ log checks, and updating programs.

4.1.3 Education

As stated above all respondents said that they provide education for all the employees. The common education formats that some respondents expressed were onboarding education and micro education. Some respondents explained that there is one education occasion each month and security testing. Some respondents explained that they have general education and then more customized education for those who work with these questions. Respondent 6 expressed the importance of educating the employees "*Educate, educate, educate. No, but to raise awareness as much as we can, of course, and it's a constant struggle to find ways to reach out and explain why you shouldn't click on the link.".*

4.2 Barriers of Existing Resources

4.2.1 Resources & Time

Even though some respondents expressed that cyber- and information security has become a higher priority and that resources and time exist, there were still some deficiencies that arose. It was expressed that more resources are required due to the work becoming more time-consuming while the threats are increasing. Some respondents argued that you can never have enough resources for this area, and some respondents explained that security is not the organization's main priority. One respondent explained that they have resource allocation to give employees time to work on security issues, especially cybersecurity. Further, one respondent said that more people are needed to work with security today, rather than just having one responsible for the security questions.

> *"And it is clear that then it was a very big resource to have me working full-time on it. It was a very large resource, but today it is a very small resource to have someone who works both with information security, shell protection, physical security, and so on, all the areas it becomes a bit too much. But it is clear that more resources need to be invested […]"- R6*

One respondent expressed that there will always be vulnerabilities and you will have to prioritize which ones are most important to immediately correct and which ones can wait or be partly fixed. Further, another respondent expressed once again that security work is time-consuming depending on the process. Following this, another respondent explained that big

changes are time-consuming, difficult to find motivation, and resource-demanding for organizations.

4.2.2 Structure

Structure refers to the organizational structure, in other words, how activities are organized within the organization. About structure some of the respondents expressed that the size of the organizations affects the work with cybersecurity, in this case, they emphasized the large size of the organization. One respondent explains that the size makes it difficult to get an overview of readiness and awareness. Furthermore, another respondent claimed that the size affects the need for good communication if a change in security is made and impacts the employees' daily work. Depending on the work area employees are more pushed to work with security questions which was emphasized by another respondent.

Furthermore, the respondent expressed an insufficient structure for continuously developing competencies to work with questions regarding new external requirements. On the other hand, another respondent expressed an existing structure for continuous improvement of cybersecurity work. A challenge that arose from another respondent is to ensure that information about cybersecurity flows between the different departments within the organization. "*We have to tie together the different siloes that separate the departments. We have to drill holes in them and tie them together so that the water can flow between*" (R9). Here the respondent makes a simile between water flowing between departments and spreading a security culture. One common structure that the respondents expressed is the hierarchy they have for decision-making which will be further presented below in *Responsibility*.

4.2.3 Responsibility

Regarding responsibility for cybersecurity questions, the majority of respondents assign the utmost responsibility to top management, which follows the hierarchical order of the organization. Some respondents emphasized that this is where the responsibility should lie since they are the ones with the ability to allocate resources. Although top management has the utmost responsibility for decision-making regarding cybersecurity, the respondents explain that the responsibility for the execution of the decisions often gets delegated.

The respondents' experience with how this responsibility is delegated differs. In some respondents' experiences, it is delegated to a single role, and for some, it is delegated to a separate department. When delegated to a single role this can raise challenges such as described above in *Resources and Time*, where the amount of work becomes overwhelming for one person. If delegated to a single department, the respondents' experience varies. One respondent described how the responsible department worked and communicated their work well towards the rest of the organization. However, another respondent who also had a separate cybersecurity department expressed that while they work with cybersecurity, the questions did not spread outside the department to the rest of the organization. The respondent elaborated and described this as a challenge since it makes it easier for individuals to fall into the mindset of seeing cybersecurity as someone else's responsibility, and rely on their expertise, which can be exploited during attacks.

The respondents further discussed the importance of individual responsibility for every employee. "*The security department cannot go around and do the work for everyone, a lot of that work needs to be done in the day-to-day work*" (R11). According to the respondents, it can become a challenge to motivate and to make employees understand their responsibility, and in turn, this can make the organization more vulnerable since security work needs to be incorporated into everyday routines. Respondent 11 further expressed that they have worked on this in the organization which has resulted in an understanding of individual responsibility: "*There is not a single employee that does not have a responsibility for security issues. You cannot abdicate from that role in the organization, we are very clear with that*".

4.3 Barriers in the Human Factor

4.3.1 Competence

The majority of the respondents expressed the importance of having the right competence within the organization to keep up. One respondent explained that everyone needs to have basic knowledge and that they have a ground structure but that some parts need to change due to updated regulations. However, another respondent expressed an existing lack of competence within the organization, the respondent argued that it has become more difficult to understand and handle warnings. Furthermore, some of the respondents having a consulting role expressed a lack of competence in their clients to safeguard themselves and needing assistance to use functions correctly. Also, respondents described that being a consultant in this area is a motivation to have the right knowledge to provide their customers with the right expertise and knowledge.

Further, a respondent expressed that there is a risk if decision-makers within the organization do not have the competence and are not able to keep up with technical functions.

> *"After all, it takes an enormous amount of knowledge to be able to keep up, and that makes it a risk when decision-makers do not have that competence, but have read in some suitable magazine about how good it is or how bad it is? Do you have a security manager who says that the cloud is bad, but that's not the whole truth either? No, it can go both ways, of course." -R6*

One respondent expressed that there is a variation of competence within the organization in relation to IT and IT security. Further, the respondent explained that there is difficulty in separating IT, cyber, and information security. Some respondents also explained that it is important to have the right competence to reach out to the rest of the organization.

Two other respondents explain that there are rarely deficiencies in the technology but rather the competence to use and handle it.

"The deficiencies lie in the understanding of what strengths and weaknesses the tools have. You cannot trust it on technology 100%. You have to work parallel with several solutions, and how you integrate these solutions is the key to your success, but it is not just a technical question but also a process question of how you consume this type of solutions […]" - R11

4.3.2 Awareness

All respondents expressed that their organizations provide activities to ensure awareness, but a common question that arose was if these activities are enough and how it is received by the end users. One respondent explained that even though some employees do not work specifically with cybersecurity they need to have awareness. However, another respondent expressed that it can be difficult to reach the end-user when the organization is big and there are a lot of users with differing competencies. The respondent further explained that if employees work with information and data, it can make it easier to keep them up-to-date and educated. A barrier that some respondents lifted is the eventual shortcuts that employees take in their daily work due to security measures being troublesome.

"Yes, it is clear that there are many people who take shortcuts. You think it will be too difficult and then it is easy to do something else. Of course, it is, unfortunately. You look at your home computer instead of your work computer, take your mobile phone in the wrong places, email when you shouldn't. So it's clear that there is, we're human, that's how it is. If the road goes around a corner in a park, everyone takes a shortcut, that's how it is." -R6

Further, a respondent talked about the deficiency of talking about awareness and compliance in official channels, and channels that employees use within the organization and that it is more informal talk within specific groups. Insufficient activities to raise awareness are also something that some of the respondents have raised. However, other respondents expressed various activities apart from education, such as meetings, events, and information on their intranet. Many of the respondents expressed that the increased attacks on companies have enabled more awareness and work with security questions in organizations. However, some also explained that there is a general naivety and comfortability that if you have not been exposed it does not imply to you.

4.3.3 Culture

Concerning cybersecurity culture some respondents expressed it as overall good, while some see it as a work in progress. Some of the respondents working as consultants explained that security is a big part of their organization, due to security affecting their work with clients and working with security every day. Furthermore, one respondent explained that the in-house expertise about security is taken for granted, but there is also a calm knowing that this expertise exists. The respondent further expressed a wish that cybersecurity could permeate more throughout the whole organization. Respondent 4 claimed that there is no existing culture for following up policies or guidelines "*No, very bad. Very bad. Not at all or I try, but there is no such culture of following up on policies and guidelines.*" The respondent further

described an existing fear within the organization but a lack of understanding of what to be scared of.

One respondent explained that cybersecurity is about working and providing education, but also a comprehensive action plan of the business' own actions, and rapport of incidence. The respondent also stated that it is important to work to decrease the internal threat image because of the external threat image. Another respondent explains that they need to create a culture that works for everyone. Other respondents expressed that they have a good culture where a lot of focus and time are given high priority. However, one respondent expressed that companies need a structure of what is acceptable and not, so it does not become a threat.

4.4 Technical Barriers

4.4.1 Current Technical Environment

Mutually amongst most respondents, they experience their technical environment as rather secure. All respondents have technical solutions that they use to minimize risks and secure their environment. Some technical solutions that are used by many of the respondents are firewalls, multi-factor authentication, penetration testing tools, backups, segmentation, and scanning digital environments. However, despite feeling relatively secure with the current technical environment many respondents bring up challenges.

Understanding the current technology solution used and the technical environment at large is a challenge mentioned by many respondents. When an organization is large or has a scattered IT environment it can make it harder to secure it since it is more difficult to achieve a comprehensive overview. As a result, important updates, security measures, or known threats can be missed which exposes the organization to unnecessary threats.

> *"From a technical security perspective, it is incredibly important to keep track on your technical environment; what you have, what you have exposed, where this is, and ensure everything is updated. We often see this with our clients, they do not know what things they have, and something gets missed. [...] This can be pretty complicated for a big client where they have an enormous amount of devices." - R10*

A part of this challenge, expressed by some of the respondents, is the insufficient cleaning of access within many organizations "*Many companies are bad at cleaning out system access. An employee could work for 30 years but in different departments and still have all the access. If something happens, that person will infect everyone.*" (R7). Respondents thereby show that insufficient access management is a risk.

A further challenge that some respondents bring up is old technical solutions which are a twofold challenge. First, old technology often limits security as Respondent 1 explains: "*We have old legacy technology, which is extremely limiting when it comes to security.*" Second, over time responsibility for management and upkeep of old systems becomes lacking, as Respondent 5 describes: "*There are old systems that lack support and where no one is responsible for the management anymore. It is unfortunately pretty common, and a risk.*"

Finally, a challenge connected to the challenge of understanding the current technological solutions is the lack of focus on operational technology (OT). Many of the respondents express that OT sometimes is forgotten while the organization wholly focuses on IT security. Resulting in vulnerabilities in the organization's overall technical security, for example, respondent 11 expresses: "*OT systems are something that is often forgotten, which can be used as a way in for threatening actors, especially if you have eg. card readers connected to normal networks.*"

4.4.2 Future Technical Environment

The respondents express that from a technical security perspective, they feel secure today, but that it is not a guarantee for the future. "*The problem is that tomorrow there is a new hole in our security that needs to be addressed. You can never rest on what you have, you always need to keep up the control.*" (R5). Ensuring safety today is not enough according to the respondents. The respondents therefore face the challenge of future-proofing their technical environment.

A part of that challenge is the increasing technical threats that the respondents describe. Most respondents describe the rapid development of new technology such as AI as both an opportunity and a threat. "*AI in its different forms is discussed a lot, the good it can bring but also that it can bring a whole new strength to attacks.*" (R9). The view that new technology such as AI brings new threats is shared by many of the respondents, however, they also express that you need to keep up with the development. "*The more we develop, digitally, the higher the requirements will be on us to also ensure that we develop and can keep safe.*" (R2). Keeping up with this development is described by many of the respondents as difficult: "*It is difficult to keep up, very, very difficult to keep up.*" (R6).

Many of the respondents express that it is important to not become anti-technology despite the new threats that might arise, partially because of the opportunities the new technology could offer but also because that might become a risk in itself.

> *"There are criminals who use AI for the attacks, where we would need AI to also protect ourselves. There's no going back and we can't hide anymore, so we might as well try to take advantage of this technology. We can't build islands where we don't use this technology, because we will still be exposed to attacks that are based on this new technology." - R1*

Finally, an issue that respondents brought up connected to future-proofing the technical environment was the issue of security not being built into the system. "*I wish we had built-in security functions in the system, so that users do it right, instead of having to come up with routines to avoid mistakes, but systems are not built like that.*" (R6). Further, respondent 11 explained: "*It costs $1 in the start, but it costs $600, 600 times more, to put security in as an afterthought [...] We need to think of security from the start, built-in not bolted on*", which elaborates on the issue of security being an afterthought.

4.5 External Barriers

4.5.1 Environmental Changes

The respondents all describe that the threat level has changed, and they can see an increase in attempted attacks on several fronts. This change in the environment requires more continuous work to be put in to ensure safety for organizations. The sentiment of being safe today, but not being guaranteed for tomorrow, as discussed under technical barriers was echoed here as well. Further, respondents raised that it will be challenging to keep up with the quick changes in the environment to decide how to respond and what level is 'good enough'. A part of the challenge of facing more threats in a quickly changing environment is how unprepared many organizations are. Many of the respondents discussed how the view on the importance of security issues in general was dropped. They discuss how security was not seen as an issue since we lived in peace, and as a result, security has not been prioritized and has become lagging. Since it has not been prioritized for a long time, it is now more difficult to catch up. "*It is going to take a long time to get the security culture back, to get the things back in place, and the processes. And the world is now different, we are meeting a fully digital world that needs to be made safe.*" (R9).

Finally, the respondents bring up that it is not just a change in the number of attacks, the motive for cyberattacks has changed, which organizations need to adapt to. Some respondents addressed that thinking you are an insignificant player that no one will care about, does not hold up. For cybercriminals, an attack can be profitable from a monetary standpoint, which many of the respondents view as the motivation. "*This is a way to make money, not just to destabilize society, even if current conflicts and wars are resolved this issue will not disappear.*" (R9). Organizations therefore need to adapt to the changes since the increase in attacks will not go away and no one is insignificant enough to be left alone.

4.5.2 External Requirements

Even though the respondents work in different sectors, all expressed that they are affected by external regulations and requirements that impact how they work with cybersecurity. Some of the respondents expressed how they are often affected by multiple external regulations, meaning they have to ensure they are compliant with all of them. Further, the respondents working as consultants all discussed that their organizations might not directly be impacted by external regulatory requirements like the NIS2 directive or others. However, they still need to have an understanding of them for multiple reasons. First, the respondents expressed that their clients might be affected, meaning they will have to understand how to comply with it. Further, the respondents explained how they are selling their competence in cybersecurity, meaning they have to be updated about regulations that might impact this field since clients will turn to them for advice.

The respondents all agreed that external requirements and regulations such as NIS2 and ISO27000 can be used as guidelines to help arrange cybersecurity work. "*They always work as a reference point of what you do and how you should proceed with your work.*" (R2). Further, many respondents expressed that the external requirements can help motivate their cybersecurity work. One respondent working as a consultant expressed that many clients they work with view the NIS2 directive as something negative that they are affected by. Further,

they view this as something they have to comply with to avoid sanctions, rather than viewing it as important work that can help them stay protected. The respondent further expressed that this makes it more difficult to motivate cybersecurity work since it is viewed as just a cost.

A further challenge with external requirements is that the task of implementing new external regulations takes time. While talking about the new NIS2 directive a respondent discussed the limited time between the proposal of the law being presented and it coming into effect. "*The government will present the proposed law now during the spring, but it is coming into effect in fall, and then it already needs to be acted on. It is too late to start acting on it then.*" (R3). Another respondent elaborated that implementation of new external regulations into an organization's praxis requires them to already have certain functions such as a management system for security work and basic functions.

4.5.3 Collaborations

All respondents discussed collaborations and how they impact work with cybersecurity. Many respondents explained that they partake in external collaborations to help monitor the environment for threats and to facilitate exchanging of experience. The respondents express that this is helpful in their work with cybersecurity. Other respondents discuss the importance of internal collaborations, eg. between different departments for the exchanging of expertise when tackling cybersecurity issues. One respondent explains that they wish for a collaboration partner that would have competence that would complement their own. However, the respondent elaborates that a collaboration partner with that sort of competency would be difficult to find and expensive to hire.

5. Analysis & Discussion

In this chapter, the findings presented in the result will be analyzed and discussed in relation to related research. This chapter will follow the same structure as the result, and this analysis will contribute to answering the presented research question of this thesis "What are the barriers to establishing sustainable cybersecurity practices?".

5.1 Barriers in Cybersecurity Activities

Li et al. (2019; 2023) argue that despite existing knowledge gaps within organizations, management needs to provide its employees with security training, and a consistent feeling of awareness of security threats and adequate response. In the interviews, all respondents explained that one of the strategies is that their organizations provide employees with education to provide awareness. The occasion of education varied, some had education each month, while some also had micro education, and some only had onboarding and introductive education. One barrier found about education was that one of the respondents explained that more education would be necessary. Following this, the respondent expressed an experience that when the introductive education has been completed it ends there, and that there is no stated strategy or method on how to work with cybersecurity.

Furthermore, some of the respondents expressed that they send out fake phishing mail to create an even higher awareness, and one respondent explained that if this test is failed the employees get an education sent to them. According to Herath and Rao (2009), organizations

should focus on both formal and informal structures such as policies, procedures, employees' role in ensuring security, and organizational culture. Concerning policies, the respondents expressed the existence of policies and guidelines. One interesting point that some respondents made was that there is no explicit cybersecurity policy but an information security policy, further that cybersecurity is not separated from information security in this matter. Li et al. (2019) also argue that it is important to have efficient communication about security. In the interviews, one respondent explained that information regarding guidelines is provided through education, meetings, and workplace meetings. Even though some of the respondents expressed activities to provide information about policies and guidelines, one barrier was still the difficulty of communicating the importance of compliance and reaching the end user. Further, another barrier was that new guidelines were not communicated formally within the organization as expressed by one of the respondents, while another also expressed the importance of communication when policies are being implemented in the organization.

5.2 Barriers of Existing Resources

When touching upon resources, some of the respondents expressed that cybersecurity has become a higher priority, but also that the work has become more time-consuming due to the threats. Furthermore, one of the respondents also expressed that it requires more people to work with cybersecurity today. However, some of the respondents expressed that security is not the organization's highest priority and that their main business gets prioritized. Therefore, many respondents experience that they will never have enough resources. This barrier aligns with what Li et al. (2023) express as a conflict between business and security and that organizations need to enable a wide understanding of countermeasures that can help them explore practical solutions.

Some of the respondents discussed how the size of the organization can make it more difficult to get an overview of the awareness and readiness of cybersecurity. Yusif and Hafeez-Baig (2021) expressed the need for both standardized and adaptive education to ensure relevance to end-users. This shows how a lack of overview can become a barrier to sustainable cybersecurity since it makes it difficult to ensure that resources in terms of eg. educational efforts are aimed at the right place.

All respondents appoint utmost responsibility to the top management, which aligns with how Sievers (2021) explains responsibility and accountability in the NIS2 directive. Johnson and Goetz (2007) explain the need for managers at all levels to engage employees by asking relevant security questions to ensure that security becomes a natural part of the day-to-day work. This aligns with how the respondents describe the responsibility is often delegated which, in turn, can be a challenge depending on how it is done. Assigning responsibility to a single role or person can become a barrier as described above since it is simply too much work for one person. The respondents further describe how delegating responsibility to a single department can become a barrier if the department does not continually communicate the issue. In this case, it risks the cybersecurity question not being kept alive in the entire organization. Li et al. (2019) express management's responsibility to ensure a structure and clear authority that can provide employees with training and efficient communication, which strengthens the respondents' explanation of top managerial responsibility. However, the

respondents' experience shows the difficulty in establishing a structure and clear authority for cybersecurity work.

The result also highlights the importance of individual responsibility. The respondents describe that security behavior needs to be present in day-to-day endeavors and routines, and this will not happen if individual responsibility is not taken. A barrier thereby becomes to get individuals to take responsibility, which is connected to how responsibility is formally delegated in the organization. Employees play an important role in the maintenance of cybersecurity according to Herath and Rao (2009) and can further be seen as the weakest link in the organization's defense (Pranggono & Arabo, 2021). If employees do not understand the importance of security practices, they might be unwilling to follow them (Herath & Rao, 2009). Furthermore, the result shows that individual responsibility also plays a role in the organization's protection against threats in their day-to-day actions.

5.3 Barriers in the Human Factor

In this part of the discussion competence, awareness and culture will be discussed. Firstly, most of the respondents said that having the right competence within the organization to keep up is very important. However, there were some barriers seen in relation to competence. One of the respondents expressed an existing insufficiency regarding competence, arguing that it has become more difficult to handle and understand warnings. The respondents having a consultant role explained that organizations do not have the competence to safeguard themselves. Further, a barrier is the risk enabled if management and decision-makers do not have the right competence and are unable to keep up with technical functions.

It was also explained that there is a variation of competence in IT and IT security. This once again, indicates that efficient communication regarding security is important as Li et al. (2019) state, despite the existing knowledge gap management has to ensure organizational structure with established and clear authority and provide training for employees. This can also be compared to the statement of some respondents that having the right competence to reach out to the rest of the organization is important. Deficiencies explained by two respondents rarely relied on the technology itself but rather on the competence to use and handle the technology. Further, one of these respondents explained that the deficiencies lie in the understanding of the strengths and weaknesses that the tools have and that you cannot trust technology 100%. This can be compared to Ifinedo's (2014) argument that employees are an internal threat and can cause disturbance in information security if an understanding is not in place. The competence in handling and use of technology can further be compared to Bulgurcu et al. (2021) and Ifinedo's (2014) statement that organizations need to invest in both technical and socio-organizational measures to reduce the risks. This is due to the technical solutions not providing enough security by themselves, which the respondents also stated.

As presented in *"Barriers in cybersecurity activities"* the respondents explained various existing activities to ensure awareness within the organization. Even though these activities exist some challenges arose amongst the respondents. Two of these challenges concern the difficulty of reaching the end-user when the organization is large with a large mass of users. Secondly, there are the possible shortcuts that users take that might disturb security. The second challenge is usually made when the work is experienced as troublesome by the

employees. This second challenge can be discussed from Ifinedo's (2014) argument that the employees are the biggest internal threat that may cause disturbance in security. Furthermore, Ifinedo (2014) states that managers have to ensure that cybersecurity practices are not burdensome for the employees, which can partially explain why shortcuts are taken as the respondents express. One respondent further expressed that we are only humans and shortcuts will always be taken given the opportunity, thereby emphasizing the need for a culture that pushes everyone to make the right choice.

Insufficient communication regarding awareness and compliance on official channels was expressed by one of the respondents, this once again shows the importance of efficient communication explained by Li et al. (2019) and also Alshaikh's (2020) argument that management should engage and review the importance of compliance in internal meetings with employees. With clear communication, there is a possibility to increase awareness even more within organizations and would eventually permeate cybersecurity more in the organization which is another barrier that the respondent emphasized.

The majority of the respondents claimed that the increased cyberattacks also increase awareness within organizations. However, a lack of exposure to attacks might lead to general naivety and comfortability within an organization when they feel that the threats do not apply to them according to some respondents. This attitude of believing that the organization is not at risk can create a barrier to the organization's cybersecurity readiness according to Hasan et al. (2021). Despite the general awareness of the threats explained by some respondents, the result shows that there is an existing fear but no existing understanding of what to be scared of according to one respondent. This can be aligned with Vance et al. (2012), who emphasize that to ensure employees recognize threats, the security education, and policies provided need to be easy to understand for the employees. Ensuring that the employees are able to understand the development, can create a better understanding of what to be scared of and an understanding of the importance of safeguarding the organization. Furthermore, this will enable a possibility of how the employees can work with the existing policies. This can also be applied to the respondents' further statement, that there is no existing culture to ensure compliance with policies and guidelines.

Alshaikh (2020) states that with a broader approach, organizations can enable the possibility to change attitudes, perceptions, routines, and assumptions. This can be true to a certain extent and accomplished in some organizations, related to the result of this thesis. One barrier that can make it difficult to achieve this entirely is priority. Some of the respondents explained that security is not the highest priority within the organization due to the core business being the main focus point. Furthermore, emphasized that even though there are a lot of activities to ensure awareness the main challenge remains the difficulty of reaching everyone, especially the end user.

5.4 Technical Barriers

From the result, it is clear that the technical environment is mostly perceived as safe. In line with Ifinedo (2014), the respondent described how different technical defenses are used to protect organizations. Similarly, to Ifinedo (2014) firewalls and monitoring systems were

mentioned, beyond this, solutions like MFA, VPN, penetration testing tools, backups, and segmentation were also mentioned.

A barrier towards sustainable cybersecurity presented in the result is to understand the technical environment as a whole. The respondents expressed that when the technical environment was not understood it had consequences such as insufficient access and device management, missing important steps in protecting the OT, and not keeping up with legacy systems, which all posed a threat to the cybersecurity of the organizations. Bulgurcu et al., (2010) and Ifinedo (2014) both express how cybersecurity risks need to be managed by technical and socio-organizational measures since only relying on technical solutions is insufficient, which can partially explain this barrier. The respondents' experiences show that it is not enough to simply have technical solutions, they also need to be understood in the context they are applied to efficiently protect the organization. If the organization is unaware of devices that are used, or if no one is responsible for an old system it is much harder to ensure that they are kept up to date to avoid them becoming a vulnerability that can be exploited as a way in. Thereby, as Bulgurcu et al. (2010) state, relying solely on technology-based solutions is ineffective. Instead, technology needs to be combined with socio-organizational measures (Bulgurcu et al., 2010; Ifinedo, 2014). This connects to another barrier that is brought up, namely how security is often an afterthought when building new systems. Respondents express that security should be built-in not bolted-on, but that that is often not taken into account. Li et al. (2023) express that poorly integrated security solutions decrease the return on organizations' security investments and that IT investments and security investments should not be seen as separate investments. Further, system design is a known issue that has been studied within IS security (Dhillon et al., 2021), however, the results indicate that it is not being applied when building systems.

A further barrier found in connection to technology is the difficulty in future-proofing the technical environment. Respondents expressed feeling safe today, but that it is no guarantee for tomorrow. Rapid technology development is a part of this barrier where respondents express that new technology brings new threats and risks that the organization needs to adapt to. AI is often brought up regarding this barrier, however the respondents view AI both as an opportunity and a threat. This aligns with Gupta et al. (2023) explanation of how AI has introduced a new era of more sophisticated and powerful cyberattacks. Further, Gupta et al. (2023) deem AI to be very important for the cybersecurity community because of the benefit it can provide for cyber defense, while at the same time posing a threat which is reflected by the respondents. However, the respondent further discusses how they experience it to be impossible to opt out of technology development. They express that since the technology is out there, they have nothing to win by opting out since they will be attacked by actors using it regardless.

5.5 External Barriers

In the result, respondents describe how they experience more threats in their environment today, which has resulted in more work for the organizations to ensure safety. The result corresponds with Warkentin and Willison's (2009) observations that external factors can impact an organization's environment to become unstable, making cybersecurity central for

survival. Respondents further expressed that this change is difficult to keep up with, partially because they believe the motivations for attacks have changed. Pawlak and Barmpaliou (2017) express that the type of threats organizations face has changed from typical cybercriminals to also include state-affiliated groups and terrorist organizations. Respondents also believe the motivations for attacks have changed; however, they emphasize that cyberattacks being profitable means that the attacks will not stop, regardless of whether conflicts in the environment are resolved.

Further challenging with the unstable environment is how the respondents expressed that security thinking, in general, dropped for many years, which has made many organizations lag behind on preparations. Schmitz-Berndt (2023) explains that incident reporting is important for understanding the threat landscape and heightening the threat intelligence, which was insufficiently addressed in the first NIS directive. The sentiment of security thinking not being present can partially be understood from the perspective of the importance of reporting incidents to heighten threat intelligence. To elaborate, if incidents are not reported and given attention to it lowers the understanding of external threats. The respondents all clarify that external collaborations have been beneficial when it comes to monitoring the environment which Schmits-Berndt's (2023) statement of information sharing to heighten the threat intelligence supports. The respondents do however also discuss the importance of internal collaboration for an organization's cybersecurity, as well as the difficulty of finding a collaboration partner.

All respondents, regardless of organization, expressed that external requirements are always present, however the attitude towards these requirements can vary. Sievers (2021) explained steps that organizations will have to take to improve their cybersecurity, and that these aim to heighten the minimum standards of organizations' cybersecurity. This aligns with respondents who expressed that external requirements and regulations can be used as guidelines to help arrange cybersecurity work and to motivate it. However, respondents also expressed that there are organizations only motivated to follow external requirements such as NIS2 to avoid sanctions such as fines which Sievers (2021) explains will be included. The respondent discussed how this can make it more difficult to motivate cybersecurity work since it is viewed as just a cost. Further, the respondents expressed that the implementation of external requirements takes time and requires having internal functions in place, which can be difficult if it is viewed as a necessary evil rather than a guideline to increase the safety of the organization.

6. Conclusion

The purpose of this study was to explore what barriers organizations face when trying to establish sustainable cybersecurity practices. The perspective of sustainable cybersecurity was used as a response to the ever-evolving threat landscape and regulatory requirements which pressure organizations' ability to adapt to current and future developments that affect cybersecurity work. With sustainable cybersecurity practices, we refer to the term practice since cybersecurity should be ingrained in the practice of the organization and not just the strategy. The research question we aimed to answer was: What are the barriers to establishing

sustainable cybersecurity practices? To answer this question, ten semi-structured interviews were conducted with experts working with cybersecurity at different organizations. To answer the research question, five barriers were found that make establishing sustainable cybersecurity practices difficult to achieve. These are: (1) *barriers in cybersecurity activities*, (2) *barriers of existing resources,* (3) *barriers in the human factor*, (4) *technical barriers*, and (5) *external barriers*. The identified barriers to cybersecurity activities were insufficient communication and educational efforts. Concerning barriers of existing resources, the identified barriers were prioritization of security, insufficient overview of awareness and readiness due to organizational size, delegation of responsibility, and individual responsibility. The barriers identified concerning barriers of human factors were insufficient competence to keep up with developments, insufficient communication, and naive attitude towards possible threats. The technical barriers identified were the insufficient overview of the technical environment, insufficiency in integrating security in new systems, and difficulties in safeguarding the future. Lastly, identified external barriers were deficient preparation for the increased threats, wrong motivation to comply with external regulations, and the changed motive to perform cyberattacks. The identified barriers contribute to better bridging the gap between best practices established in research and issues that practitioners are facing. Further, by identifying the barriers we contribute towards an understanding of the importance of a more holistic approach for cybersecurity measures contributing to previous research within the field of IS.

6.1 Limitations & Future Research

In our study, we have identified barriers to establishing sustainable cybersecurity practices by interviewing eleven experts in the field of cybersecurity with experience from many different organizations. It should be noted that while interviewing the experts in the different organizations gave us great insight, it is still limited to specific perspectives. Interviewing more respondents might allow for a fuller understanding of the context of the barriers. However, it would not necessarily improve the generalizability of the result. Furthermore, our aim with the study was to contribute by exploring what barriers exist when establishing sustainable cybersecurity practices for the future. Therefore, our study can act as a foundation for future research regarding the subject.

For further research, there is a need to further investigate how these barriers can be solved to ensure sustainable cybersecurity practices. Further research focusing on whether there are differences in barriers depending on the type of organization could be of interest. Public and private organizations have different opportunities to adapt to changes and would therefore be interesting to study further.

6.2 Acknowledgement

Lastly, we want to acknowledge those who have made this process possible. First of all, we want to say thank you to our supervisor Jonny Holmström who has provided great insight and knowledge in guiding us through this process. Last, of all, we want to thank all of the participants who have taken part in our study and brought us great insights by taking the time to participate in our interviews.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory. *MIS Quarterly*, 34(3), pp. 435–461

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, pp. 102003–102010

Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing Artificial Intelligence. *MIS Quarterly*, 45(3), pp. 1433-1450

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp. 77–101

Brender, J., Ammenwerth, E., Nykänen, P., & Talmon, J. (2006). Factors influencing success and failure of Health Informatics systems: A pilot Delphi study. *Methods of Information in Medicine*, 45(1), pp. 125–136

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), pp. 523–548

Cheng, E. C. (2000). An object-oriented organizational model to support dynamic role-based access control in electronic commerce. *Decision Support Systems*, 29(4), pp. 357–369

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), pp. 13–21

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, pp. 101713–101723

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, 30(4), pp. 101693

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access, 11*, pp. 80218–80245

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, pp. 102726

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), pp. 154-165

Heyder, T., Passlack, N., & Posegga, O. (2023). Ethical management of human-AI interaction: Theory development review. *The Journal of Strategic Information Systems*, 32(3), pp. 101772

Holmström, J. (2022). From AI to digital transformation: The AI readiness framework. *Business Horizons*, 65(3), pp. 329–339

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), pp. 69-79

Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, pp. 100063

Johnson, E., & Goetz, E. (2007). Embedding Information Security into the Organization. *IEEE Security & Privacy*, 5(3), pp. 16–24

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*, 30(2), pp. 687–704

Khan, S., & Madnick, S. (2019). Cybersafety: A System-theoretic Approach to Identify Cyber-vulnerabilities & Mitigations in Industrial Control Systems. *SSRN Electronic Journal*.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, pp. 13-24

Li, W. W., Leung, A. C. M., & Yue, W. T. (2023). Where is IT in Information Security? The Interrelationship Among IT Investment, Security Awareness, and Data Breaches. *MIS Quarterly*, 47(1), pp. 317–342

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), pp. 105336

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, 42(1), pp. 285–311

Myers, M. D. (2013). *Qualitative research in business & management* (Second edition). SAGE Publications Ltd.

Myers, M. D. (2020). *Qualitative research in business & management* (Third edition). SAGE Publications Ltd

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, 52(1), pp. 123–134

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88, pp. 101608

Patterson, Hobbs, M., & Zhu, T. (2017). A cyber-threat analytic model for autonomous detection of virtual property theft. *Information and Computer Security*, 25(4), pp. 358– 381

Pawlak, P., & Barmpaliou, P. N. (2017) Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, 2(1), pp. 123-144

Pranggono, & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2), pp. 4-9

Ramesh, G., Krishnamurthi, I., & Kumar, K. S. S. (2014). An efficacious method for detecting phishing webpages through target domain identification. *Decision Support Systems*, 61, pp. 12–22

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis*, 39(10), pp. 2119–2126

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, 9(1)

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, pp. 102974

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), pp. 267–270

Sievers, T. (2021). Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*, 2(2), pp. 223–231

Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication. *Information Systems Research*, 27(2), pp. 219–239

Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, 46(3), pp. 102282

The NIS2 Directive. (2024a). *NIS2 Requirements: Understand and prepare for the upcoming NIS2 requirements*. https://nis2directive.eu/nis2-requirements/ (Accessed 2024.01.29)

The NIS2 Directive. (2024b). *What is NIS2? Confused about NIS2? Here's the basics*. https://nis2directive.eu/what-is-nis2/ (Accessed 2024.01.29)

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

Vetenskapsrådet. (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Elanders Gotab.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), pp. 118–144

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, pp. 97–102

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), pp. 2–9

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

Yin, R. K., & Retzlaff, J. (2013). *Kvalitativ forskning från start till mål* (1. uppl.). Studentlitteratur.

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, 16(4), pp. 490–513

Zviran, M., & Haga, W. J. (1999). Password Security: An Empirical Study. *Journal of Management Information Systems*, 15(4), pp. 161–185

Appendix 1. The NIS2 Directive

With the NIS2 Directive, new organizational requirements and obligations are introduced within four areas: (1) risk management, (2) corporate accountability, (3) reporting obligations, and (4) business continuity. Risk management covers requirements organizations must reach to minimize cyber risks and include measures such as incident management, increased supply chain security, increased network security, increased access control, and utilizing encryption. Corporate accountability is a requirement for management to take responsibility for cybersecurity which includes overseeing, approving, and participating in cybersecurity training. Not complying with these obligations may result in penalties for the management such as liability and a temporary ban from their management role. Reporting obligations require organizations included under the directive to set in place processes to ensure swift security incident reporting. Finally, business continuity requires that organizations have a plan for readiness to maintain critical functions facing cybersecurity incidents. Included in the plan are preparations for (1) system recovery, (2) emergency procedures, and (3) ensuring that a crisis response team exists (The NIS2 Directive, 2024a).

A goal with NIS2 is to establish a minimum baseline security against cyberthreats and thereby, ten minimum measures on top of the four areas described above have been established. The ten minimum measures need to be established and implemented in all essential and important entities and are presented in the table below (The NIS2 Directive, 2024a).

The Ten Minimum Measures	
Establishing risk assessment and security policies for information systems.	Establishing policies and procedures for the evaluation of security measures
Establishing policies and procedures for using cryptography and encryption.	Establishing a strategy for managing security incidents.
Establishing security procedures such as employee data access policies and creating an overview of data assets.	Establishing cybersecurity training to ensure that basic computer hygiene is followed.
Establishing policies for handling and reporting vulnerabilities to ensure security regarding the acquisition of systems as well as the development and operation of them.	Establishing plans and procedures for managing business amid and after a security incident, including up-to-date backups, and access to IT systems and operational functions.
Establishing the use of multi-factor authentication and implementing authentication solutions, voice, video, and text encryption, as well as, encrypted internal communication when needed.	Establishing supply chain security by managing relationships with direct suppliers and tailoring security measures to each supplier's vulnerabilities, as well as evaluating the collective security level across all suppliers

Appendix 2: The Interview Guide

INLEDANDE

1. Är det okej att vi spelar in?

2. Vilken roll har du på företaget?

3. Vilken bakgrund har du? (Utbildning etc)

3a. Hur ser din tidigare erfarenhet med cybersäkerhet/informationssäkerhet ut?

TEKNIK

4.Vilka huvudsakliga tekniker använder ni inom ert arbete ? (gammal eller ny?)

4a. Hur säkerhetsrustad anser du att denna teknik är?

4b.Upplever du att det finns brister med den teknik ni använder utifrån säkerhetsperspektiv

5.Vad använder ni för tekniska lösningar för att skydda er från hot?

5a. Anser du att de är tillräckliga för att skydda organisationen?

5b. Används dessa tekniska lösningar i specifika sammanhang?

STRATEGI

6. Vad har ni för befintliga strategier och resurser för cybersäkerhet?

7. Hur och vem/vilka tar beslut om strategierna?

7a. Är det några fler som är delaktiga i besluten?

8. Vem/vilka ansvarar för säkerhetsfrågor i förhållande till cyber/informationssäkerhet?

8a. Finns det en uttalad roll eller ett delat ansvar?

8b. Läggs ansvaret på en specifik avdelning eller delas det?

9. Har ni policies för cybersäkerhet/informationssäkerhet? Vad innefattar dessa?

9a. Hur säkerställs det att dessa efterlevs?

10. Hur arbetar ni för att kontinuerligt förbättra och säkerställa era cybersäkerhets strategier?

10a. Finns det strukturer som säkerställer detta, ex. planerade revideringar?

11. Vad finns det för andra strategier för att öka medvetenheten för att medarbetare ska förstå vikten av att följa era säkerhetsregler och policies?

ORGANISATION

12. Hur arbetar ni med cybersäkerhet inom organisationen?

13. Hur påverkar cybersäkerhet det vardagliga arbetet?

13a. Upplever du att det ges tillräckligt med resurser/tid för att reflektera kring säkerhetstänk?

13b. Finns det genvägar som kompromissar säkerheten?

14. Hur skulle du beskriva kulturen kring cybersäkerheten/informationssäkerheten inom organisationen?

14a. Hur tror du att detta påverkar arbetet med cybersäkerhet?

15. Har ni några utbildningar för era medarbetare gällande säkerhetsfrågor?

15a. Hur ofta inträffar dessa?

15b. Varför inte?

16. Hur ser du på den rasande utvecklingen inom IT relaterad till cybersäkerhet?

16a. Anser du att varje fördel med utvecklingen även medför sårbarheter/nackdelar? varför/ varför inte?

16b. Anser du att en ökad sårbarhet pga detta är något som bara måste accepteras?

OMVÄRLD

17. Hur anser du att hotbilden har sett ut senaste tiden?

16a. Har det påverkat ert arbete på något sätt? (Strategier osv, eller om de blivit utsatta för hot?)

18. I jämförelse med andra organisationer, hur anser du att er organisation är rustad för dagens hotbild?

19. Hur vana upplever du att din organisation är att arbeta utifrån externa regelverk/krav?

19a. Vilka typer av regelverk/krav arbetar ni utifrån idag?

19b. Påverkar dessa ert arbete med cybersäkerhet? (strategi, practice, osv)

20. Utifrån det nya Nis Direktivet, i vilken utsträckning påverkar det er?

20a. Har ni påbörjat förberedelser för att säkerhetsställa att ni uppfyller kraven för det nya direktivet?

20b. Varför/varför inte?

AVSLUTANDE

21. I en ideal värld, hur skulle arbetet med cybersäkerhet fungera? (strategi, resurser, practices)

22. Något du vill tillägga som vi inte tagit upp men som du anser är viktigt och bör nämnas?

Tack för din medverkan!!

Appendix 3: Coding Tree