UMEÅ UNIVERSITET

MANAGERS' PERCEIVED UNDERSTANDING AND INFLUENCE ON CYBERSECURITY READINESS

Identifying Barriers, Associated Risks, and Strategies

Andrea Egelrud & Jonas Selberg

Department of informatics
Magister thesis, 15hp
Master's program in IT-management
SPM 2023.04

Abstract

Organizations need to protect themselves from cyber threats and a variety of methods exist to mitigate these risks. Factors such as rapid digitalization, expedited by Covid-19, have only made cybersecurity threats a growing concern. Most research within the IS field has focused on technical methods to mitigate risk, leaving non-technical methods less explored. The aim of this study was to develop a deeper understanding of managers', at different levels, perceived understanding, and influence to achieve cybersecurity readiness in order to identify barriers. Further, an objective was to develop possible strategies to mitigate identified risks associated with these barriers. To fulfill this aim, a case study was conducted at a municipality-owned organization who have taken the initiative to raise cybersecurity awareness. Six interviews were conducted with managers from both senior- and middle management, and cybersecurity governance documents were collected. In our findings, we identified three main themes with associated barriers to achieving cybersecurity readiness. These include barriers associated with (1) organizational and managerial factors, (2) pitfalls in communication, and (3) policy and instructions. The study contributes to an understanding of different barriers that managers at different levels might perceive and suggests possible strategies for mitigating the risks associated with said barriers.

Keywords: Cybersecurity readiness, Cybersecurity threats, Cybersecurity governance, Cybersecurity management, Policy and Instructions

1. Introduction

The digitalization of society has changed the conditions for organizations (Agrawal et. al., 2018; Brynjolfsson & McAfee, 2014). Digital technologies have seen rapid development during the last decade with new digital technologies creating opportunities for organizations to enhance their business (Hasan et. al., 2021). To keep up with this changing environment and to take advantage of opportunities organizations engage with digital transformation. Digital transformation is a sociocultural process of adapting an organization to the changing conditions in the digital landscape which requires cultural changes (Saarikko et. al. 2020).

One major implication of digital transformation for organizations is the increasing risks and challenges associated with cybersecurity, especially in the wake of COVID-19 as the use of digital technologies drastically increased (Hasan et. al., 2021; Abukari & Bankas, 2020; Pranggono & Arabo, 2021). The pandemic radically disrupted organizations in their day-to-day operations, and organizations were forced to reactively answer to challenges that were caused by the pandemic (Almeida et. al., 2020). The proactive approach toward digitalization organizations usually could engage in suddenly turned to a more ad-hoc approach, forcing firms to hastily implement new technologies, processes, and structures (Verma & Gustafsson, 2020). Thus, organizations had little time to develop a security infrastructure to decrease cyberattack risks. The challenges with managing cybersecurity during the pandemic are evident from the increase in cyberattacks. The World Economic Forum reported that cyberattacks had increased by 50,1% due to the pandemic (WEF, 2020). With work from home being more normalized during and post-covid the issue of managing cybersecurity is a lasting

challenge that needs attention. Thereby, the changes caused by digital transformation and COVID-19 make cybersecurity a growing concern that needs further attention.

The term “cybersecurity” is becoming more and more prevalent within the field of information system security (ISS). However, the vast and growing terminology in the research field that was historically termed IS security has led to a jungle of different approaches and definitions depending on the research's main objective (Craigen et. al., 2014). These include approaches either being of technical, managerial, behavioral, and or organizational (Crossler et. al., 2012). The many approaches have led to different terms being used in research on ISS such as IS security, information security, computer security, and cybersecurity (Dhillon et. al., 2021). Although IS security still dominates the literature when referring to the issue of keeping organizations protected, cybersecurity is emerging as a common term in the IS security field.

A lot of cybersecurity research has focused on technical issues, and how technology can be used to solve security challenges (Crossler et. al., 2012). However, research has shown the need to focus on socio-organizational factors affecting cybersecurity (Dhillon et. al., 2021). This is much due to the fact that research within the IS security field has identified individuals as the weakest link in organizations' cybersecurity defense (Furnell & Clarke, 2012; Jeong et. al., 2019; Neigel et. al., 2020; Szczepaniuk & Szczepaniuk, 2022; Wiederhold, 2014). As a response, the human factor in cybersecurity research has gained traction. A central theme emerging in the literature is the issue of employees’ compliance with cybersecurity policies and how organizations can enforce compliance (Dhillon et. al., 2021).

Most research on cybersecurity management looks at cybersecurity governance strategies from a boardroom perspective and/or the relations between the top and senior management, and their influence on achieving cybersecurity readiness (Shaikh & Siponen, 2023). When using the term cybersecurity readiness, we refer to it as an extension of cybersecurity awareness and understanding which includes all the organization's non-technical capabilities to detect and respond to security threats.

An important omission in cybersecurity management research is the middle management perspective since leadership at all levels of an organization influences employees' motivation and behavior to reach organizational goals (Al Khajeh, 2018; Johnson & Goetz, 2007). To address this gap, the aim of the study is to develop a deeper understanding of managers’, at different levels, perceived understanding and influence to achieve cybersecurity readiness in order to identify barriers. By including both senior- and middle management, we take a more holistic approach to management and provide a more extensive understanding of managers’ experiences in enforcing cybersecurity policy and instructions. The study further aims to propose strategies that can help organizations manage the risks associated with the identified barriers. This resulted in the following research question.

- What are the barriers to achieving cybersecurity readiness?
    - What strategies can be implemented to mitigate the risks associated with identified barriers?

The study will contribute to a deeper understanding of managers’ perceived understanding and influence to achieve cybersecurity readiness. By identifying barriers related to managers at all levels, we hope to contribute with a deeper understanding of management's role in enforcing cybersecurity governance strategies than the current research provides. To study this a qualitative case study was conducted at a municipality-owned organization.

2. Related Research

In the IS field, cybersecurity has been studied for a long time but with different terms such as IS security, information security, computer security, and cybersecurity (Dhillon et. al., 2021). In this study, we refer to it as cybersecurity. There is no unitary definition for researchers to adopt when investigating the cybersecurity phenomenon since most definitions are context bound to a specific perspective (Craigen et. al., 2014). ITU (2008, p.2) defines cybersecurity as the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets". However, this definition does not clearly distinguish and describe the two main perspectives on cybersecurity: technological and socio-organizational. Therefore, when referring to cybersecurity our understanding of the phenomenon will emanate from ITU's (2008, p.2) definition with a socio-organizational perspective of how different human factors affect how cybersecurity can be managed.

Research streams	Focus	Definition	Example of types of research	Example reference
Social System	Structures	Studies of structures focus on the issue of how laws and regulations e.g., policies and instructions affect cybersecurity. An important substream is research regarding compliance.	Security policy compliance Security risk management Firm security decisions Regulation research	Morris et. al., 2020
	People	Studies of people focus on the issue of individuals' behavior regarding cybersecurity.	Information privacy concerns Trust in security systems Information security behaviors	Herath & Rao, 2009
Technical system	Technology	Studies of technology focus on cybersecurity attacks and also include studies that explore technology that detect and avoid attacks.	Phishing Security threat detection technologies	Jensen et. al., 2017; Patterson et. al., 2017
	Tasks	Studies of tasks focus on research regarding system design issues and vulnerability management.	Privacy-enhancing technologies Data and application security Access management	Paté-Cornell et. al., 2018; Khan & Madnick, 2019

Table 1. Overview of research streams within IS security field

Dhillon et. al (2021) conducted a literature review of the last 30 years of research about IS security within the field resulting in a conceptual model that summarizes the research agenda of the phenomenon. This resulted in four categories that research usually falls within; studies of structures, people, technology, and tasks. Further, these four categories can be divided into two groups that either study the social system (structures, people) or the technical system (Dhillon et. al., 2021). In Table 1 an overview of these different research streams based on Dhillon et. al. (2021) can be seen.

Research on the technical system is mainly focused on either the technology or the design of the systems. Some of the research is closely related to the field of computer science (Dhillon et. al., 2021). Research on the social system tends to fall within policy and compliance management (structures) or cybersecurity behavior and privacy concerns (people). However, there exists an overlap with the research on the social system where the two focuses intertwine (Dhillon et. al., 2021). This study falls within the research stream of social systems with its focus on management's role in enforcing cybersecurity governance strategies.

2.1 Managing Cybersecurity

To control cybersecurity, McLaughlin & Gogan (2018) propose a five-step cycle of interrelated tasks: prepare, prevent, detect, respond, and learn. Within all steps there are challenges. Preparation is about preparing the organization for an incident by identifying risks and creating tools such as priorities, and checklists, assigning responsibility, and making response plans. Challenges within this step are understanding different internal and external threats as well as recognizing cybersecurity as a moving target that changes quickly, response plans, thereby, need to be continuously updated. Another step to take before incidents are prevention. Preventing is about ensuring that vulnerabilities are identified and consists of two approaches, (1) ensuring technological tools are used, and (2) ensuring employees comply with cybersecurity policies. Within this step, identifying rising threats and new technology as well as engaging and changing unsafe behavior amongst employees are prevalent challenges. However, no matter the prevention, incidents are bound to happen, emphasizing the importance of the detection step to quickly detect and trigger a response (McLaughlin & Gogan, 2018).

This step involves involving and encouraging users to report discrepancies in the systems they work in. The challenges within these steps are keeping updated with technology and getting the support of alert users that notices potential issues. This support requires that users both have an easy way to report issues and have alert users that are conscious of the systems. Detection of an incident should trigger a response. The response step includes diagnosing and determining the impact of the incident to ensure the right steps are taken to recover from the incident. Challenges within this step also include finding a balance between following the protocol and giving responders the opportunity to improvise as best seen fit given the circumstances. After an incident, it is important that the organization analyzes the incident and their response to it to ensure that they learn and can improve their preparation. This step should thereby include a debriefing session depending on the impact of the incident, where the response, preparation, and prevention strategies are evaluated and improved before the next incident. This step can easily be forgotten but is important to ensure future readiness. It is also important to make incident reviews a periodic element of the work (McLaughlin & Gogan, 2018).

Whitin all steps McLaughlin & Gogan (2018) describe how challenges and best practices involve taking the human factor into consideration. This is because the human factor is often regarded as the weakest link in an organization's cybersecurity (Furnell & Clarke, 2012; Jeong et. al. 2019; McLaughlin & Gogan, 2018; Neigel et. al. 2020; Szczepaniuk & Szczepaniuk, 2022; Wiederhold, 2014). Recognizing cybersecurity as a sociotechnical problem rather than just a technological problem is of the essence. Simply finding more technical solutions to human-

made errors will not be enough to ensure safety against cyberattacks (Jeong et. al. 2019). Thereby, managing cybersecurity also involves managing the human factor (McLaughlin & Gogan, 2018).

2.1.1 Human-factors

The human factor in cybersecurity refers to situations where incidents are caused by human actions, e.g. lack of attention to detail, inadequate planning, or lack of knowledge, resulting in unintentional threats that might compromise security (Yusif & Hafeez-Baig, 2021). Cybercriminals can exploit such actions and behaviors, leading to successful attacks and breaches in an organization's cyber defense, making it imperative to address human factors in cybersecurity strategies (Yusif & Hafeez-Baig, 2021).

One part that makes humans the weakest link is the inability to comply with cybersecurity policies. One explanation for this is awareness. If the employee is not aware of the potential consequences of their behavior or lacks awareness of the policy at all, this might lead to the employee engaging in unsafe behavior (Li et. al., 2019; McLaughlin & Gogan, 2018). However, awareness cannot explain this behavior fully. Even with awareness, employees sometimes engage in unsafe cybersecurity behavior. This is because employees constantly are faced with the decision of convenience and security, where the unsafe action is more convenient than the safe one (McLaughlin & Gogan, 2018). Non-compliance behavior can also partially be attributed to how serious threats are appraised and the consequences the individual might experience (Li et. al., 2019). However, threats are perceived differently by people in different roles and are thereby contextually bound. Further, norms within the organization also influence cybersecurity awareness, attitude, and behavior of the employee (McLaughlin & Gogan, 2018).

To encourage compliance with policies and instructions there are actions that can be taken. Employee involvement with the development and upholding of cybersecurity improves compliance. Further, if the policies are well-written and clearly anchored to the organization, it is more effective compared to vague policies (McLaughlin & Gogan, 2018).

2.2 Cybersecurity Governance Strategies

Governance refers to the responsibility to lead an organization. In the case of cybersecurity governance, it refers to the responsibility for a strategic plan to address risks associated with cybersecurity. In practice, this is achieved through creating strategic goals to achieve through cybersecurity policies and instructions. The policies and instructions then play an important role in executing the cybersecurity governance strategies. The implication of this is a need for top managers to have a deep understanding of both cybersecurity threats and the different operations within the organizations as well as how these interact (Yusif & Hafeez-Baig, 2021). Also of importance is the support of top managers in the implementation of cybersecurity policy since this signals the importance of compliance to employees (Li et. al., 2019). However, top managers are not the biggest barrier to cybersecurity readiness, rather middle managers can act as a barrier since they are in charge of daily operations (Johnson & Goetz, 2007).

2.2.1 Cybersecurity Policy & Instructions

The development of policies, instructions, and education for cybersecurity is imperative for organizations to raise awareness and readiness for cyber threats. Cybersecurity policy (CSP)

refers to the development of rules, recommendations, and guidelines that seek to ensure the secure usage of systems and the safeguarding of information (Scala et. al., 2019). The instructions are specific instructions that need to be taken in order to follow a policy. The difficulty for organizations is to create awareness and education that enforce adherence to their policy and instructions for cybersecurity (Yusif & Hafeez-Baig, 2021). According to Madnick et. al. (2017), a reason organizations struggle to enforce cybersecurity governance strategies often is derived from the absence of sufficient resources allocated towards education and training in cybersecurity. Further, multiple factors affect organizational compliance and a more holistic approach to management needs to be considered when developing strategies for increasing compliance with CSP.

Internal communication is of great importance for the survival of an organization, however, strategies such as policy are often not perceived to be communicated enough. To ensure satisfactory communication of strategy, factors such as channel and volume are of importance. However, more important is the content and the relevance to the recipients (Ruck & Welch, 2012). Further, engaging employees in cybersecurity is of great importance to ensure secure behavior. To do this, frequent information and reminders that function as cues to actions need to be communicated to employees. This information could include advice, reminders, and so on, and need to be communicated on a regular basis (Li et. al., 2019). McLaughlin & Gogan (2018), also advocate for frequent communication regarding external as well as internal threats since this can improve awareness.

2.2.2 Culture, Training, & Insiders

Organizations have their own culture that encompasses different values, expectations, and norms that apply to all of their members and differentiate them from other organizations. Cybersecurity culture can be defined as a fundamental part of the organizational culture and shapes the policies and instructions to align with core values, expectations, and social principles (Yusif & Hafeez-Baig, 2021). The importance of an integrated cybersecurity culture in the overarching culture that enforces secure and protective behavior is therefore essential for increased awareness and understanding of cybersecurity. Employees in organizations often fall victim to different cyberattack strategies due to a lack of training and education in cybersecurity (Yusif & Hafeez-Baig, 2021). Therefore, fostering a cybersecurity culture where behavior such as risk awareness is of high importance, and cybersecurity training and education are vital for creating a culture where employees adopt secure behavior (Corradini & Nardelli, 2018).

Poor cybersecurity culture and training programs increase the risk of creating so-called “insiders” within the organization; insiders pose a security threat due to their lack of cybersecurity awareness and knowledge, and cybercriminal use their ignorance to exploit systems and retrieve sensitive information (Yusif & Hafeez-Baig, 2021). Thereby, one challenge for organizations is to create incentives and motivate employees to adopt secure behavior (Mclaughlin & Gogan, 2018). If organizations succeed in that regard, a stronger cybersecurity culture will emerge as well as a higher risk awareness. One aspect is developing security awareness programs to motivate employees to participate in the programs (He & Zhang, 2019).

Factors that decrease motivation for employees to undergo training can often be derived from non-updated programs, long and non-interactive programs, or creating generic programs

that do not solve existing non-compliance challenges (Yusif & Hafeez-Baig, 2021). In order to foster good cybersecurity readiness, organizations must have a strategic plan that continuously evaluates and monitor employees' awareness and knowledge of cybersecurity. By adopting such a perspective, organizations can identify specific areas of concern and proactively create tailored programs that seek to solve a particular issue (Yusif & Hafeez-Baig, 2021). Standardizing processes does not automatically mean a cybersecurity culture of repetition will be adopted and realized. A standardized cybersecurity training program might ultimately fail if its components are outdated and unengaging due to a lack of interest or if the training, for example, seems irrelevant among employees (Li et. al., 2017). Therefore, it is imperative for organizations to develop governance strategies that include both standardized and adaptive training programs to keep up with the dynamic landscape and facilitate employee engagement (Yusif & Hafeez-Baig, 2021). it is therefore important to assess security training programs, policies, and instructions to ensure their relevance and user-friendliness (Vance et. al., 2012).

Organizations should integrate cybersecurity risks in their strategic plan and implement structures that increase risk awareness. Organizations could develop occasions within the organization where workshops and/or seminars raise questions about security threats and the potential disruption they might have for operational work (Vance et. al., 2012). Further, to foster a cybersecurity culture, managers at all levels could ask relevant security questions when personnel present progress or propose a new project. By doing so employees will eventually be conditioned to always think about possible threats and risks in their operations (Johnson & Goetz, 2007). To motivate secure employee behavior and enforce security governance strategies, senior management could formally task middle managers to become champions for raising security questions (Ifinedo, 2014).

2.2.3 Cybersecurity Leadership & Motivation

Previous research on cybersecurity leadership mainly takes the perspective of senior- and/or top management, and the relations among them (Hu et. al., 2012; Möller, 2020). Triplett (2022) suggests that cybersecurity leaders, such as the ISO, must be able to motivate employees through their knowledge and passion for cybersecurity and act as role models in cybersecurity issues. However, the influence of lower-level managers' leadership on employees has not received the same attention. Nevertheless, there exists research on leadership and its influence on compliance and motivation, which mainly discuss two forms of leadership, namely; transformational and/or transactional (Zohar & Tenne-Gazit, 2008; Bass & Riggio, 2006; Inness et. al., 2010).

Transformational leadership is proactive and enhances motivation, morale, and performance through four different behaviors (Odumeru & Ifeanyi, 2013; Bass, 1985). (1) idealized influence which refers to leading by example, (2) inspirational motivation which refers to communicating a positive vision, (3) intellectual stimulation which refers to encouraging employee engagement, and (4) individual consideration which means adapting the leadership to employees unique situations (Pilbeam et. al., 2016; Warrilow, 2012). By adhering to these four behaviors, transformational leaders support intrinsic motivation by appealing to individual values to encourage and enforce norms, values, and attitudes that increase compliance (Pilbeam et. al., 2016). Block (2003) concluded that transformational leadership is imperative to affect change in the culture.

Transactional leadership on the other hand is more reactive and promotes compliance through rewards and punishments (Pilbeam et. al., 2016). Transactional leadership involves two types of leadership styles, namely, constructive leadership and corrective leadership (Zohar, 2002). Constructive leadership offers material rewards for performance that satisfy organizational goals. Corrective leadership monitors employee performance, detects errors, and corrects them accordingly (Pilbeam et. al., 2016). By adopting these leadership measures, transactional leaders influence extrinsic motivation in individuals by providing incentives to promote performance that adheres to organizational expectations (Pilbeam et. al., 2016; Block, 2003). According to Block (2003), transactional leaders are less focused on supporting change and innovation, rather avoidance of risks is the primary focus.

With the existing research on management in cybersecurity, there is limited research investigating managers at all levels within an organization. Therefore, this study aims to provide a broader knowledge and understanding of this.

3. Research Methodology

To study how managers at different levels perceive their understanding of cybersecurity governance strategies and their influence on cybersecurity readiness, we conducted a qualitative case study. Qualitative research is interested in creating an understanding of the motivation and context of people and phenomena (Myers, 2013). Given our interest in managers' experience with cybersecurity, a qualitative study was a fitting choice. Further, we have taken an interpretive approach to the study. Walsham (2006) describes that in interpretivism, knowledge of reality is viewed as a social construct that is created with and by human actors. Understanding is thereby created by not separating the data from its context and searching for an objective truth, instead understanding the parts in their context as a subjective truth. This is fitting for our study given the aim to explore managers' experiences and perceptions.

A case study was chosen to be able to study the phenomenon. Myers (2013) defines a case study as the investigation of a phenomenon where the context is not separated but taken into consideration. Further, Yin (2018) explains that a case study should lead to insights regarding the complexity of the internal and external context and add to the understanding of the studied phenomena. With our research questions to identify barriers and strategies to mitigate risk associated with achieving cybersecurity readiness, we aim to contribute to a deeper knowledge of managers', at different levels, perceived experiences of cybersecurity governance strategies and their influence on enforcing strategies. Thereby the phenomenon being studied is cybersecurity governance strategies in the context of managers at different levels. Below is a presentation of the case being studied in this paper.

3.1 Case Description

This case study was carried out at a public organization in the northern part of Sweden, which consists of approximately 170 employees and operates in a specific municipality in the region. On behalf of the municipality, the organization is tasked with contributing to growth and housing provision within the region. The organization is divided into multiple departments

with different operational focuses, implying operational differences in the systems, information, and processes used in their daily operations.

The organization recently allocated more resources towards the operational work with cybersecurity, specifically by hiring an ISO that holds responsibility for developing and implementing strategies in regard to cybersecurity. As municipality-owned, the studied organization has access to more resources and experts on cybersecurity than traditional small organizations. The organization previously had policies and instructions in place for cybersecurity, however, not much was made to ensure compliance with these governing documents. Therefore, the organization is in the initial process of increasing cybersecurity readiness by developing training programs and updating the policy and instructions to increase overall awareness and understanding of cybersecurity. This implies that managers' just recently started undergoing comprehensive training to raise their awareness and understanding of security risks and cybersecurity policy and instructions. This study aims to contribute with comprehensive knowledge of how managers at all levels perceive their understanding of CSP and their influence on organizational cybersecurity readiness to identify barriers. Therefore, given that the organization has recently initiated these changes, and has a variety of departments where work differs greatly, this makes for an interesting case to investigate managers', at different levels, perceptions of understanding and enforcing cybersecurity governance strategies.

3.2 Data Collection

To collect data to be able to fulfill the aim of the study of providing a deeper understanding of managers' perceived understanding and influence on organizational cybersecurity readiness, interviews were conducted. Surveys were deemed to be unfit in this instance for a myriad of reasons. The organization studied is small and was at the time conducting an employee evaluation in the form of surveys leading to a bit of survey fatigue which might have made it difficult to receive an adequate response rate. Further, we wanted to get better access to respondents' experiences and feelings. Myers (2013) explains that interviews give access to rich data from the respondents' perspectives.

In qualitative research, both interviews and observations are common data collection techniques. Observation allows the researcher a new dimension of insight by observing what the participant does and how they interact with the social world (Myers, 2013). Observing managers while working with cybersecurity would also have been insightful data that could further our understanding. However, given the short timeframe of this study, it would have been difficult to gain that kind of access. Myers (2013) emphasizes that building trust with the people you are observing is of great importance to be able to gather rich data, but that this is a process that can take time. Thereby, interviews were chosen as the most fitting data collection technique for gaining insight into managers' perceived understanding and influence on cybersecurity readiness. The following sections describe the sampling criteria for participation and the conduct of interviews and the collection of cybersecurity governing documents.

3.2.1 Sampling & Criteria

The study adopted a purposive sampling strategy for selecting respondents with the highest probability to contribute useful and relevant information for the studied case (Campbell et. al.,

2020). The sampling of respondents was made in consultation with our contact person at the organization. This was done since the contact person had access to and insight into the organization and relevant respondents. This resulted in access to six respondents (see Table 2). Two respondents belonged to senior management, and the rest to middle management. The group of respondents is of heterogeneous composition, with gender differences and an age range between 36 - 64. One criterion was developed to ensure that respondents included in the study had insights that would provide valuable empirical data for the purpose of the study (Denscombe, 2014; Merriam & Tisdell, 2016). The criterion for participation in the study was that respondents had to inhibit a management role with corresponding personnel responsibility. This is with a background in the study's aim to investigate managers' perceived experiences.

Respondent	Length of Employment	Personnel responsibility	Management level	Length of Interview
Respondent 1	6 years	Yes	Senior management	50:08
Respondent 2	13 years	Yes	Middle management	41:47
Respondent 3	1 year	Yes	Middle management	47:48
Respondent 4	12 years	Yes	Senior management	44:22
Respondent 5	6 years	Yes	Middle management	45:08
Respondent 6	8 years	Yes	Middle management	42:03

Table 2: Information about respondents and length of interviews

3.2.2 Execution

Semi-structured interviews were chosen to be able to answer the research question. Semi-structured interviews permit a more free conversation since improvisation and new questions can be explored, but still gives consistency over many interviews (Myers, 2013). Before the creation of the interview guide, informal meetings with our contact person at the organization were held. The purpose of the meetings was to gather a deeper understanding of the organizational structure and their current work with cybersecurity. Further, the meetings in combination with the literature review helped guide us in the creation of the interview guide. The interview guide consisted of six themes (1) understanding of cybersecurity, (2) handling incidents, (3) awareness of threats, (4) continuous improvement, (5) leadership and culture, and (6) external partners (see Appendix 1). Initial questions in the interviews included questions about the respondents' experience at the organization, and their current work and responsibilities. As a concluding question, respondents were asked to reflect and share their thoughts on the biggest challenges for increasing the organization's cybersecurity readiness. During the interview, mirroring was used to ensure a correct understanding of the respondents' answers (Myers, 2013).

The interviews lasted between 40-50 minutes and were conducted in Swedish (see Table 2). We were both present during the interviews but with different roles. One was responsible for asking the questions and keeping the conversation active, while the other had more responsibility to listen and ask follow-up questions actively. The first interview was a pilot

interview which allowed us to test and time the interview guide. After the pilot interview, no considerable changes to the interview guide were made. The insights from the pilot interview were, thereby, deemed to be relevant to the study.

All interviews were conducted via Teams, which was decided given the respondents' familiarity with it and ease with scheduling. However, this choice might have impacted the interviews. Kvale & Brinkmann (2014) describe that an interview is affected by the place and the closeness to the interviewee. Meaning the setting of an interview might have an impact. Therefore, conducting the interviews digitally might have impacted the result, but given the respondents' familiarity with the tool and ability to choose where to be interviewed, a relaxed setting for the conversation was reached. Further, the interviews were recorded which might also have impacted the outcome of the interviews. Myers (2013) explains that recording interviews comes with benefits such as being able to relisten to exactly what a respondent answered. However, a potential pitfall with recording interviews according to Myers (2013) is that it changes the setting of the interview and might impact how freely a respondent answers questions. During the interviews, this was not an issue as respondents answered questions freely.

3.2.3 Other Data Sources

Besides the interviews, the organization's governing documents were also collected. This included four different documents that constituted the organization's cybersecurity policy and instructions. The documents that were included were the organization's policy and goals regarding information security, instructions for employees and instructions for management, and finally instructions for incident reporting. These documents were used in three ways. First, to create an understanding of the organization's work with cybersecurity and the goals that have been agreed upon. Second, the documents were also used when formulating the interview guide. Third, the documents were used to triangulate the data from the respondents by comparing respondents' answers to instructions and the policy to gather a fuller understanding. This type of triangulation, where data is collected via different sources, is referred to as data source triangulation and is used to establish a more extensive comprehension of a phenomenon (Carter et. al., 2014).

3.3 Data Analysis

During the interviews, Teams' automatic transcription tool was used to start transcribing the interviews to ease this process. The transcriptions were then double-checked to fix errors and to get more familiar with the material. To further familiarize ourselves with the data each interview was read through multiple times. This first step is consistent with Braun & Clarke's (2006) initial phase in the thematic analysis. Thematic analysis is a good fit for a bottom-up inductive approach. This means that identified themes are driven by the collected data, and not fitted to an existing framework (Braun & Clarke, 2006). Since no theoretical framework was used, the inductive bottom-up approach was decided as most fitting. Given the flexibility of thematic coding to be able to find and develop themes, this was chosen as the data analysis method. Further, Braun & Clarke's (2006) descriptions of the process of thematic analysis guided our data analysis. They explain the process as consisting of six phases, starting with familiarizing with data, followed by generating codes. After this, three phases followed

including searching for, reviewing, and naming the themes, and the final step is producing the report.

After familiarizing ourselves with the data, initial codes were generated by highlighting sentences that were summarized to create our open codes. This was done separately to avoid getting influenced by each other, and to ensure that more possible codes were found. This step resulted in about 170 initial codes each that were compared and sorted through. Codes that were connected were combined into categories, and in total 13 categories were created. To ensure that these categories were true to the data collected, a description of all categories was created and checked against the code extracts. This was an iterative process. In the next step, categories were combined and sub-themes were developed. This resulted in five sub-themes, where considerable overlap and similarities still existed which led to these being combined into three overarching themes. The overarching themes were reviewed in comparison to the collected data to ensure no discrepancy existed. For examples of data analysis see Appendix 2.

3.4 Ethical Considerations

When conducting research there are ethical principles to take into consideration. Shamoo & Resnik (2009) describe honesty, objectivity, and confidentiality as some of these principles that need to be followed. Honesty has to do with being true to collected data and not misrepresenting. Objectivity has to do with avoiding biases influencing the study, and confidentiality has to do with handling the data and information in a secure way. These principles were taken into account during the study.

Another ethical consideration has been complying with Umeå University's rules regarding the handling of sensitive data. GDPR has resulted in new guidelines for how data generated during studies should be handled. We have complied with this in regard to recording, storing, and deleting data. When recording we did not use phones since the storage of data on such devices is not secure for personal or sensitive data. Further, the data was stored on secure platforms approved by the University. Participants were informed of this as well as when the data would be deleted.

Myers (2013) describes informed consent as an important principle to follow when people are being studied. Informed consent means that participants are given the opportunity to make an informed decision if they would like to participate or not (Myers, 2013). Myers (2013) also stresses that participants should be informed that their involvement is voluntary and can without question be ended at any time. To adhere to this principle a consent form was delivered to respondents and signed before the interviews. These include information about participation and handling of data.

4. Results

In this section, the gathered empirical data in the form of internal documents, and quotes from interviews with the respondents are presented. All quotes have been translated from Swedish into English to ensure comprehension of the result for more readers. Minor rephrasing has been made in the translations of quotes to clarify what the respondents are expressing, and irrelevant digressions and repetitions are indicated as [...]. When context is deemed necessary

parentheses are used to indicate this and are not part of respondents' actual response. The respondents are referred to as (R1-R6).

Through the thematic coding of the interviews, three themes emerge that all relate to challenges that made cybersecurity readiness more difficult. These three themes are (1) Cybersecurity Readiness - Barriers with Organizational & Managerial Factors, (2) Communicating Cybersecurity - Barriers to Information Sharing and Responsibility, and (3) Policy boring? - Barriers to Keeping Policy & Instructions Alive. The structure of the result will follow these themes.

4.1 Cybersecurity Readiness - Barriers with Organizational & Managerial Factors

4.1.1 Formal Education & Managers' Perceived Experiences

In order to enhance the overall awareness and understanding of cybersecurity within the organization, more resources have recently been allocated to handle the organization's work with cybersecurity. As part of this initiative, an Information Security Officer (ISO) was hired last year to support the IT manager in overseeing cybersecurity operations. The ISO has the responsibility to create comprehensive training programs and educational initiatives, as well as auditing policies and instructions. The ISO reports to the CIO as well as presents cases for top management. This initiative seems to have had a considerable impact on managers' perceived awareness and understanding of security risks and threats. The ISO has implemented standardized formal digital training programs as well as in-person training opportunities. The formal digital training programs provide cybersecurity training through a digital platform and offer managers and employees the flexibility to undergo training when convenient. The in-person training opportunities are either provided in the form of workshops or seminars. During the interviews, some respondents expressed that they do not get any specific training in cybersecurity, instead everyone in the organization undergoes the same training.

All respondents expressed a positive attitude towards the training initiatives taken during the last year, and have experienced a considerable change in the focus on cybersecurity within the organization.

> *We receive security training via email every now and then. I think it's great. An email arrives with a course that might take 3 to 6 minutes, explaining topics such as how a website is structured and what risks are associated with it. The next email could be about phishing or something else [...] And it was less I can say at least now it's more frequent and more structured, a lot more structured. - R5*

Another respondent elaborates on the importance of combining both digital- and physical training opportunities. "*We had a physical training session about information security [...] And it was more in a group setting which led to more discussion [...] That's a disadvantage with web-based (education) [...] there is most often no discussion afterward [...].*" -R2

During the interviews, it became evident that the general awareness and understanding of potential cybersecurity threats have increased because of more frequent training programs. However, some respondents point out that while the awareness has increased, it does not constitute organizational readiness. R3 describes their experience: *"I would say that with that*

(readiness), we have some work to do […] If I say like this, for this year, it's more about […] awareness". Another respondent from senior management describes what level of cybersecurity readiness the organization currently inhibits: *"I would say average […] The knowledge that day-to-day operations might completely stop, to think like that I don't believe […] all functions have done that in the (company)." - R1*.

When asked to reflect on the educational efforts taken recently, all middle management respondents expressed a similar response, that it's sufficient enough as of now and simply wish for recurrent training to keep their awareness on high alert. R3 expressed a need for this: *"[…] even if I would work here until I'm 100 years old I believe a top-up dose is necessary"*. This result could partly be interpreted and understood from the fact that this is the first time they receive extensive training on cybersecurity. When senior management was met with the same question, more elaborated responses were provided. One respondent from the senior management expressed a desire of having a higher degree of overall IT competency in the organization since it would increase threat awareness and identification of security risks. The respondent further expressed difficulty knowing what educational level is sufficient and how you actually validate that the organization reaches that level. To summarize, the main challenge of educational efforts and managers' experience of such efforts seems to be correlated to the fact that cybersecurity recently became a main priority as every respondent indicated in their interviews.

4.1.2 Operational Differences and Leadership

A couple of respondents described how departments within the organization have different prerequisites since the organization is involved in multiple operations, and the type of information that is handled differs between departments. For example, R6 describes: *"We have the luxury […] of not getting a lot of external emails, we mostly use internal emails amongst each other." R6*. This stands in contrast with other respondents' descriptions of the information they handle. They involve external partners on a more frequent basis, requiring a responsibility to inform and educate them about the organization's rules and guidelines of cybersecurity. R6 was also the only respondent expressing that employees seem to procrastinate and postpone undergoing cybersecurity training: *"I know they postpone it, it is like that you know […]." - R6*. This indicates a difference in the engagement and interest between different departments regarding cybersecurity depending on what kind of operations they are involved in daily.

During the interviews it became clear there are differences in the way managers exert leadership and their methods of keeping cybersecurity on the map and as a recurring theme in their daily operations. This emerged when R3 and R2 described their own perceived responsibility and influence on keeping the question alive.

> *It is indeed true that as a manager, one influences more than one might think or desire. If I show no interest or talk about it as a necessary evil [...], it certainly has an impact. So even if there are things that sometimes I find challenging or demanding, I tend to choose to be [...] extra positive and talk about it a bit more to spread the message [...] I might even highlight it if someone comes up with an idea or has a question related to this topic [...] Because I believe it's the only chance we have to invest time and effort into it. If I'm more interested [...] in something else it will have an effect. -R3*

R2 on the other hand, seems to not emphasize the impact one's own influence has on enforcing guidelines and rules to the same degree as R3. Instead, R2 seems to rely much on the information shared by senior management and focuses on disseminating that information. However, R2 does mention that after undergoing training they sometimes talk about it in more informal settings and encourage such behavior:

> *Now we have hired an expert in this field who helps us other managers stay updated and disseminate information [...]. It's usually during lunchtime that we talk [...] and bring up questions 'Has anyone gone through this, and how did you experience it? - R2*

An important difference to clarify is that R3 has had previous roles with responsibility over cybersecurity while R2 has not had a role encompassing such responsibility previously.

4.1.3 Organizational Culture

The culture experienced by the respondent seems consistent throughout the interviews. All respondents express an open climate where questions are encouraged and not disregarded, independent of where in the organization a question might arise. R6 describes their experience with the culture that permeates the organization: *"The culture is open, honest, and supportive, and we assist one another. It's fundamental to our operations that we ask questions." - R6.*

The experienced culture correlates to when respondents describe and express gratitude towards the support available to them if uncertainty in cybersecurity questions arises. It's evident that the new ISO provides a great sense of support for the respondents. However, one respondent mentions that it might take extra time to double-check if something is correct, but that it's worth it: *"I rely on (name) 99 percent of the time to ensure accuracy and to be certain [...] I prefer to be correct, even if it means waiting an additional hour for a response [...]." - R5*

A majority of the respondents explain that the organization is currently in its learning phase regarding cybersecurity. Therefore questions are encouraged and welcomed, and formal sanctions are not used to promote conformity to policy and instructions, but it can be a challenge to enforce such behavior.

> *Encourage everyone to speak up when they notice a flaw or when they make a mistake and thank them for acknowledging their error. We must avoid fostering a culture of silence where people are afraid to speak up, and how do you achieve that? I don't know, but engage in open communication, ask questions, and listen actively. And remember, never get angry at someone who reveals that they have done something foolish. On the contrary, they should be praised. It's the only way we can learn. There will always be individuals who find it difficult to admit that 'I clicked on that PostNord link despite all the warnings and prior information not to do so.' It happens every time. - R1*

R3 also acknowledges the importance of encouraging employees to come forward and describes a real example of a security incident where the culture played an imperative role.

> *It became very evident that we have a culture where it's not about someone making a mistake or being at fault. Instead, it's more about curiosity and learning together. It's like, 'Okay, what can we learn from this?' [...] Instead of pointing fingers or looking for a scapegoat, we found it interesting and started exploring how we can improve. - R3*

4.2 Communicating Cybersecurity - Barriers to Information Sharing and Responsibility

4.2.1 Information Sharing & Gathering

The managers express some similarities in how and what kind of information is shared regarding cybersecurity initiatives. All respondents describe how updated information regarding policy or instructions is communicated to them at managerial meetings, which they later inform their personnel about during workplace meetings. Some respondents also mention that information brought up at such meetings is published on the organization's intranet, but various degrees of certainty can be found in their answers.

> *It usually starts with the management team first, and then it cascades down to all employees during the workplace meetings. Afterward, there will be a brief announcement on the intranet with a link to where it can be found. - R5*

Another respondent describes the same process but is not as certain the information is published on the intranet. *"Sometimes I believe it's also published on the intranet, but we always go through it at workplace meetings" - R2*. Multiple respondents described that updated information on policy and instructions is published on the intranet, but when asked specific questions about policy and instructions some respondents tried finding it on the intranet. However, this proved to be time-consuming, and one respondent only found the information at the end of the interview.

The respondents also express differences in how they are kept updated on the topic of cybersecurity with information from the IT department. R2 means that the new ISO provides relevant information: *"Now we've hired an expert on the area which helps us managers to keep ourselves updated and also send out information that should be disseminated." - R2*. R6 however expresses a contrasting experience regarding how, and what information is shared about the current state of cybersecurity within the organization. "*It would be beneficial to receive more frequent updates from our IT department regarding ongoing developments and*

events, or at least keep us managers informed on what is going on and what we should think about.". Although multiple respondents explain how information is published on the intranet and brought up during managerial meetings, R6 describes a situation that arose when the first link with digital cybersecurity training was distributed throughout the organization: *"The first time I got it (the training link), I thought it was like a virus or something, and I just said no, I'm not going to do this, so I just threw it away." - R6*

4.2.3 Responsibility & Ownership

The question of ownership and responsibility are connected and differ in perception among the respondents. The respondents' perception of responsibility also differs from the description in the policy and instructions. The policy stated that every employee has a responsibility to follow the policy and instructions as well as report potential incidents. Further, the policy divides responsibility into the following: (1) The CEO is responsible for ensuring sufficient resources for the security work as well as revising the policy. (2) The IT manager is responsible for operational coordination cybersecurity, as well as, reporting results of the work. (3) Owners of the company's information assets are responsible for ensuring availability, accuracy, and confidentiality. Further, specific instructions for managers as well as employees also exist to clarify processes and responsibilities. Managers' information security responsibility cannot be delegated and includes being an incident recipient, as well as a responsibility to enforce that all employees and consultants within their department follow the policy and instructions. However, the policy for employees also makes it clear that all employees are responsible for ensuring that their behavior aligns with the instructions and fulfills a security behavior.

This is not how every respondent perceives their responsibility or where the responsibility of cybersecurity lies. Consistent with the policy, the responsibility is discussed at different levels such as senior management, middle managers, and individual level as well as IT's responsibility. Differing from the policy is the extent of the responsibility for these levels. R2 discusses their responsibility to ensure that employees within their department take part in the education, and perceive this to be at the senior management level rather than at a middle manager level. "*It is not a course I would say you have to do to work for me, that would be on a senior management level [...] to ensure that it is sent out and that everyone is booked to attend*." - R2. R5 on the other hand describes ensuring that employees in their department take part in education as their responsibility. "My role in this is to ensure that employees take part in internal education, and are updated on the policy through our workplace meetings and so on." Further R5 also clarifies the individual responsibility that everyone has for cybersecurity. "*You should of course always have it in the back of your mind, IT security and what you are doing. It is a big responsibility that is put on the employee."*

Many of the respondents show great trust in and feel supported by the IT department and the ISO for dealing with cybersecurity threats. Thereby, many respondents also see the IT department as more responsible in these questions. For example, R4 discusses the IT department's responsibility as the expert: "*I am not an expert on cybersecurity, right? But we have people in the IT department that should know that*."

The IT department is seen as the expert thereby leading to them being seen as having the utmost responsibility and ownership over these questions. A potential problem that arises from

this is how it might affect others' awareness and managers' sense of responsibility. A respondent from the IT department explains that they rarely get any sort of feedback on cybersecurity work. The respondent believes this has to do with others' lack of engagement and technical knowledge about the subject which makes them less aware of risks. However, they wish that this was not the case and that there was more engagement from others in the organization. The trust that the IT department will deal with any potential risks and threats, might impede on other managers' perceived responsibility to actively look for threats since they feel secure that the IT department will catch such problems before them. For example, R2 describes how cyber threats within their department would be discovered:

> *I am pretty sure that a program at IT would give an alarm if you accidentally clicked on something or there was an intrusion. I don't think employees or my group would know. [...] The IT staff is at another department, and I think they would notice it before us. - R2*

Thereby the trust in the IT department might lead to the manager not actively trying to look for cybersecurity issues within their department as the cybersecurity policy states that managers should.

From the IT department, this is seen as an issue that needs balancing. The respondent describes how they have to ensure that they do not take over the responsibility from the end-users of systems since they are not the ones that use the systems. They also lack full insight into how end-users interact with the systems. Thereby, they see a need to engage and ensure that users are the ones that start thinking of these questions since they work with the systems daily. The respondents see their role in identifying threats as somewhat limited. Although they can enforce safe behavior by informing employees on what not to do, the end-users who use a specific system daily need to be alert to notice and flag potential issues. To conclude the understanding of responsibility in cybersecurity questions are not clear. Many of the respondents put the ownership of cybersecurity work within the IT department, which also shifts the responsibility to that department.

4.3 Policy boring? - Barriers to Keeping Policy & Instructions Alive

4.3.1 Policy and Instructions

The respondents agree that the cybersecurity policy is essential. They motivate that the policy provides documentation of a shared vision with agreed-upon goals within the organization. The policy also signals the support of top management and the prioritization of cybersecurity.

> *I would say that it's vital because you can't as a [...] manager be responsible for security if the goal is not defined. And the owner, senior management, and board needs to stand behind this, because otherwise you will never get money and resources for the work and it will always be possible to question why you should follow it. When [...] it's documented and said this is how we do this, that's when the rest of work starts, which is hard enough as is. But without a policy, you're left in the dark, you need to agree in the organization of what you want to achieve. - R1*

However, whether or not the existing cybersecurity policy and instructions are enough is not agreed upon. The organization has developed governing documents for cybersecurity, including a policy and instructions designed to assist employees at all levels, both managers and non-managerial staff. The governing documents include a policy with overarching guidelines and security goals the organization strives to achieve. Many of the respondents perceived that they have good knowledge of it. However, when asked specific questions about the policy and instructions the respondents are unsure of the content. For example, a majority of the respondents were unable to recall any of the five goals stated in the policy when asked if there are any security goals. "*I don't think so. [...] It is not something I can remember seeing*." - R2.

Another example of respondents not being familiar with the policy is when R3 described having to handle an incident. The organization has instructions for how to handle incidents within the policy, but the respondent describes that when the incident happened the department was not familiar enough with the instructions. Despite not being fully informed about the instructions, the incident was mostly resolved in accordance with the instructions. However, the respondent emphasizes that at the time this was mostly from luck rather than familiarity with policy and instructions.

> *What happened in practice, that was really what we wanted to happen. That is, no one had to work with this alone, and instead got a hold of the manager and you just have to know these things. But this time it was more luck than anything. - R3*

In other words, the respondent's department managed to resolve the incident mostly in accordance with the instructions, but with a better knowledge of the incident instructions this could perhaps have been solved more efficiently.

Being updated on the cybersecurity policy might not just be a cybersecurity issue, instead keeping policies alive is an overarching issue.

> *You would think that a subject such as the working environment, which also has policies and instructions, and often is a question of great importance [...] but if I ask my coworkers how many actually have read the working environment policy? It is not that many, and even fewer have read this (the cybersecurity policy). - R3*

R3 thereby describes how difficult it is to motivate personnel to use and reflect on policies in general since it is seen more as a necessary evil that is a bit boring. "*It's (new policies) maybe not any kind of bestseller that everyone thinks 'yippie, better check this out'*." - R3

Further, many of the respondents do not feel involved or like they have any influence on the policy. This does however differ for the respondents who are part of senior management, who very strongly feel involved with the policy.

4.3.2 Adaptation of Cybersecurity Strategies

All respondents bring up that changes in the environment have impacted their awareness and readiness.

> *If you look at the media, especially now with Russia and all that, there is a lot more being written about it (cyber threats), which means that you talk about it a lot more. And there is maybe an underlying worry that something could happen - R2.*

They perceive the threat of cyberattacks as rapidly changing and evolving. At the same time, digitalization and hybrid work are also present and making these threats a continuously growing issue. "*We have put a big empathizes and resources on this, and we obviously hope that that is enough, but I think the risks are increasing (with cyber threats)"* - R4

As a response to this, the respondents describe that the need for cybersecurity awareness and readiness within the organization has increased. The respondents partly see this need as met through the education described earlier. However, one issue identified and highly ranked by all of the respondents was how to keep the question alive.

> *A challenge is understanding that we need to continue to spend time and energy on this question to make sure that it is more than something that is interesting for only a short time. We might be alert and on our toes right now, but if all meetings in the future continue to be filled up with something else? - R3.*

The issue is in other words to make cybersecurity a part of everyday work. To not just make it a question that is topical during education or after an incident, but an ingrained part of the culture.

One part of the issue is integrating and adapting the current cybersecurity strategy in the form of the cybersecurity policy and instructions. Many of the respondents describe the issue that the policy and instructions are written at a very generic level, meaning they might perceive it to be insufficient in certain scenarios that are within the limits of a specific department. "*It (the policy and instructions) could be clarified and be made more tailored to be relevant to different work groups.*" - R6. The genericness of the policy also contributes to the issue of keeping the policy alive since the formulation makes it less exciting.

> *The challenge is that this is a policy document that needs to include and be applicable to all different parts of the organization. […] The issue is making it go from being a benchwarmer to something that someone actually reads and uses. - R3*

However, the genericness of the policy is also indicative of a different issue. Because the policy needs to be all-encompassing for the whole organization, this creates an inertia in changing it.

> *It is rarely possible for a policy or a governing document to be comprehensive of a whole topic. Ongoing information and education about what is happening is essential. With policy documents, we talk about them being kept alive and responsive, but there is always an inertia where a week later they are out of data in some way. Even when you continually look them over and update them, the changes outside are faster. - R5*

In conclusion, this creates a challenge given the dynamic threat scenario identified in combination with a policy that is not as dynamic.

5. Discussion

In this segment the objective of the study, to identify barriers and potential improvements related to managers' perceived experiences of cybersecurity initiatives is presented. The results are discussed in connection with the existing literature on cybersecurity management and provide knowledge on the importance of managers at all levels for enforcing cybersecurity governance strategies. The aim of the discussion is to interpret the results and highlight barriers in order to explore the implications of managers' experiences in relation to cybersecurity endeavors. The discussion is structured as follows: Each heading corresponds to the results headings to facilitate a clear transition from the findings to our interpretation and analysis. Further, a summary of the discussions identified barriers and solutions is presented as a figure. Lastly, a section dedicated to the limitations of the study is presented.

5.1 Organizational & Managerial Factors - Standardized Training, Role of Middle-Managers, & Leadership

The formal training programs, both digital and in-person, are generally described as positive by the respondents. With a background in the development of digital technologies, and with the increased use of digital technologies as a result of the pandemic, cybersecurity has recently become a core question for many organizations (Hasan et. al., 2021; Abukari & Bankas, 2020; Pranggono & Arabo, 2021). This was the case for the studied organization, and cybersecurity training programs were just recently implemented. This could explain respondents' positive attitude towards the cybersecurity training programs because they lack a frame of reference regarding expectations or needs they might have in cybersecurity training. The result shows that currently the training programs implemented are standardized over the entire organization, which could have negative implications in the future. Standardized training programs carry the risk of becoming too generic and outdated, leading to lower engagement from all levels of employees (Yusif & Hafeez-Baig, 2021; Li et. al., 2017). The organization, therefore, has to tackle this barrier by continuously evaluating and monitoring employees' awareness and understanding of cybersecurity, for them to proactively be able to develop more tailored training programs adhering to different departments' needs (Yusif & Hafeez-Baig, 2021). However, the results show that the respondents desire a continuous top-up dose to keep their awareness as high as possible. For such cases, a standardized training program might be the best choice but should be combined with more adaptive training programs to keep up with the dynamic landscape of cyber threats (Yusif & Hafeez-Baig, 2021).

The results show that combining both digital and in-person training opportunities is perceived by middle managers as important since the digital training programs don't induce informal discussion to the same extent as in-person training. However, this does not seem to be sufficient enough to create a cybersecurity culture, where latent awareness of threats and risks that permeates the organization. The results indicate that some middle managers perceive cybersecurity readiness to be relatively low. Senior management has to implement structures and strategies to ensure latent risk awareness becomes part of each employee's daily work. This stands in line with Vance et. al. (2012) perception that organizations have to incorporate security risks and the potential disruption they might have for daily operations in workshops and/or seminars. Furthermore, middle managers could formally be tasked with becoming champions for raising security questions (Ifinedo, 2014). This can be done by frequently asking about security issues when employees present progress or propose new projects (Johnson & Goetz, 2017). The issue of standardized training is, thereby, a recurring issue. To become champions of cybersecurity, middle managers need more training to become more risk aware. This aligns with previous research on the importance of continuously assessing training programs to ensure their relevance (Vance et. al., 2012). By doing so, the organization can proactively identify areas of concern that will facilitate the development of tailored training programs, policies, and instructions (Yusif & Hafeez-Baig, 2021). Thereby, senior management not understanding the imperative role middle managers play in enforcing CSP and secure behavior (Johnson & Goetz, 2007) could become a barrier to increasing organizational cybersecurity readiness.

The middle managers' perception of their influence on employees conflicts with each other. Some respondents are more aware of their influence than others and take a more active part in keeping the question of cybersecurity alive in day-to-day operations. These respondents exhibit a more proactive approach by, on their own accord, acting as role models, expressing a positive attitude towards training programs, and involving employees in discussions about cybersecurity questions. The results show that respondents expressing proactivity in cybersecurity questions have prior experience with cybersecurity responsibility. Since middle managers play an imperative role in fostering secure behavior (Johnson & Goetz 2007) they have to take on the role of a cybersecurity leader. According to Triplett (2022), cybersecurity leaders have to act as role models and involve employees in discussions on cybersecurity to motivate employees. He and Zhang (2019) point out that motivating employees will result in fostering a cybersecurity culture where safe behavior is extended throughout the organization.

Previous research on leadership and compliance (Zohar & Tenne-Gazit, 2008; Bass & Riggio, 2006; Inness et. al., 2010), shows that leaders with a proactive approach inhibit transformational leadership, and enhance intrinsic motivation through similar behavior as mentioned above (Bass, 1985; Odumeru & Ifeanyi, 2013; Pilbeam et. al., 2016). Transformational leadership is effective in fostering and changing culture by motivating employees to feel responsible and involved (Block, 2003). Therefore, senior management should encourage transformational leadership, and exert tendencies related to this leadership style. Other respondents do not exhibit this proactive approach, but rather a more reactive one. With the reactive approach, the managers take a less active role in cybersecurity and mostly disseminate passed-down information. The reactive approach is more in line with what previous research calls transactional leadership (Zohar, 2022). An important part of this type

of leadership is extrinsic motivation which the leader creates through rewards and punishments (Pilbeam et. al., 2016). In this case, the managers lack the needed structures for creating this motivation. Since the organization is still in a learning phase, no rewards for following policy or punishment for breaking it have been enacted. This means that leaders who take a more reactive approach with the transactional leadership in this question struggle to motivate employees to follow instructions. McLaughlin & Gogan (2018) advise creating incentives that motivate employees to adopt secure behavior, but this can be a challenge. Thereby, lacking incentive structure can act as a barrier to transactional leadership.

However, transactional leadership could have negative consequences in the short term given the organization's current work and goals with cybersecurity of raising the overall awareness and creating a cybersecurity culture. The respondents perceive the current culture to be open and supportive where it is okay to make mistakes. Introducing incentive systems for rewards and punishments could have a negative impact on the current open culture. The potential negative consequences of transactional leadership also stem from it being focused on risk avoidance and efficiency that do not motivate changes in the culture (Block, 2003). Using transactional leadership through incentives could result in fostering a culture of silence where the risk of unintentionally creating "insiders" increases (Yusuf & Hafeez-Baig, 2021). Therefore, this could act as a barrier to achieving the organization's objective to foster a cybersecurity culture with high-security awareness.

5.2 Pitfalls in Communication - Relevance, Responsibility, & Ownership

The respondents' perceptions regarding how information is shared differ to some extent regarding what channels are used and if enough information is shared. One respondent expressed a desire to receive more frequent updates on cybersecurity initiatives. Previous research shows the importance of frequent information sharing to ensure that employees engage in secure behavior (Li et. al., 2019; McLaughlin & Gogan, 2018). Further, strategies in the form of policy are often not perceived to be well communicated (Ruck & Welch, 2012). One explanation for why some respondents experience that not enough information is shared might have more to do with the relevance and content of information rather than the volume of shared information. Ruck and Welch (2012), explain that factors like channel and volume are less important compared to content and relevance for satisfactory communication. How relevant managers perceive the information to be for their work could impact their opinion of how well policy is communicated. A barrier to cybersecurity awareness and readiness is thereby, how relevant the information is perceived by the managers.

The result shows that there is uncertainty regarding the responsibility of enforcing cybersecurity policy and instructions in the organization. The organization's policy shows that it is a shared responsibility, where middle managers have a responsibility to ensure that the policy is followed by employees in their departments. However, not all respondents perceive this as their responsibility. Previous research shows that middle managers can become a barrier to cybersecurity readiness since they control the daily work and decide what their employees focus on (Johnson & Goetz, 2007). The respondents are managers that are thereby responsible for enforcing the policy. However, if this responsibility is not communicated clearly, it could become a barrier since the managers see this as someone else's responsibility.

Thereby, they might not focus on it, leading it to unintentionally act as a barrier to cybersecurity awareness.

The middle managers all express that they feel supported and that the IT department and the ISO is a great resource that they can rely on. However, this can also turn into a challenge which was identified in the result. The responsibility and ownership for cybersecurity are passed to the IT department and the ISO since some of the middle managers rely too much on them as a resource and experts. This turns into an issue since too much trust is put in the systems at the IT department for the detection of threats. Which in turn, could lead to end-users relying on someone else to detect threats and thereby lower their own awareness. One respondent saw a need for more involved users who take responsibility and actively notice potential issues. This aligns with recommendations from previous research that advocate for the use of technology in combination with alert system users that notice and report discrepancies (McLaughlin & Gogan, 2018). Thereby, this manager's experience aligns with previous research. However, this was not an understanding shared amongst all respondents. Communicating the shared responsibility is of utmost importance since this can ensure that all employees take ownership of the question. This in turn can then lead to improved cybersecurity awareness and readiness.

5.3 Policy & Instructions - Importance, Adaption, Inclusion, & Alignment

From the result it is clear, having a cybersecurity policy is essential. The respondents identified that this created a shared vision and signaled support as well as prioritization of cybersecurity from top management. This corresponds with previous research that stresses the importance of top management support for employee compliance (Li et. al. 2019). However, our result also shows that few of the respondents knew what was included in the policy. Previous research on policy compliance has identified that an employee's understanding and awareness of a company's cybersecurity policy increase CSP compliance (Li et. al., 2019; McLaughlin & Gogan, 2018). Thereby, managers not knowing the policy could become a barrier to compliance since they are unaware of what to enforce. This further emphasizes the importance of formally tasking middle managers to become champions for cybersecurity questions (Ifinedo, 2014). However, to foster a cybersecurity culture through champions, top- and senior management have to, in addition to increasing risk awareness (Corradini & Nardelli, 2018), also increase middle managers' awareness and understanding of policy and instructions. Threats are contextually bound and might thereby be perceived differently depending on the role (McLaughlin & Gogan, 2018), making it even more important to increase middle managers' awareness and understanding of CSP.

The respondents clarify that policy being perceived as boring is not unique to just the cybersecurity policy. Respondents express that policy and instructions are written at a generic level, which is necessary to encompass the entire organization. This results in the policy and instructions being perceived as less relevant and not as dynamic. Previously research shows that well-written cybersecurity policies clearly anchored in the recipient's work are more effective compared to policies that are vague (McLaughlin & Gogan, 2018). Thereby, a barrier, in this case, is the perceived genericness of both policy and instructions. The respondents see a need for both a shared vision for the organization that signals top- and senior management

support and more relevant information that is applicable to their work. Thereby, a recommendation could be to adapt the instructions to further apply them to respondents' work while the policy is kept at a more all-encompassing level to ensure the shared vision.

Further, research shows that employee involvement in the development and upholding of the policies encourages compliance with policies (McLaughlin & Gogan, 2018). From the respondents, it became clear that most middle managers did not feel involved in the development of the cybersecurity policy, while senior managers that are a part of top management are more involved. Policies and instructions are an important part of executing cybersecurity governance strategies which require top managers to have deep insights into both the operative work within the organization and emerging cybersecurity threats (Yusif & Hafeez-Baig, 2021). Middle managers hold a lot of insights into the daily operative work of their department and could, therefore, contribute to the development of policy and instructions. This would be beneficial twofold since involvement in the development of policy and instructions encourages compliance, and middle managers could contribute with deeper insights into the operative works (McLaughlin & Gogan, 2018; Yusif & Hafeez-Baig, 2021).

The respondent identifies that an issue stemming from the policy being generic is the issue of keeping them alive and present in everyday work. They also identify that with cybersecurity this is even more important since cyber threat is a dynamic threat that quickly changes. This issue is consistent with previous research where cybersecurity has been identified as a moving target that requires the organization's response plan to be continuously updated (McLaughlin & Gogan, 2018). An organization's work with cybersecurity is a continuous cycle of trying to prepare, prevent, detect, respond, and learn which needs to be present in the daily work (McLaughlin & Gogan, 2018). Therefore, a barrier to cybersecurity is ensuring that policy and instructions are responsive to a dynamic threat and that the work with cybersecurity remains active. Support from top management is essential for ensuring resources for cybersecurity work (Madnick et. al., 2017). However, middle managers can become barriers since they are in charge of daily operations (Johnson & Goetz, 2007). Consequently, if middle managers do not prioritize and call attention to the cybersecurity policy, efforts in updating policy and instructions might be wasted. Thereby, an alignment between top-, senior- and middle management is needed where efforts are consistent at all levels by involvement and engagement.

5.4 Identified Barriers, Associated Risks & Solutions

In Table 3, barriers, associated risks, and strategies identified in each segment of the discussion are summarized and presented.

	Identified Barriers	Associated Risks	Strategies
Organizational & Managerial Factors	Standardized training	Generic and outdated training leads to lower engagement, motivation, and risk awareness.	Continuous evaluation of employee cybersecurity awareness. Developing tailored training programs adhering to departments' needs
	Senior management foreseeing the role of middle managers	Impeding the development of a CS culture	Continuously assessing training programs to proactively identify specific areas of concern. Implementing security risks and potential disruption in training programs. Formally appoint CS champions.
	Using transactional leadership methods for fostering a cybersecurity culture	Fostering a culture of silence - insiders	Senior management promoting transformational leadership methods
	Lack of structures for transactional leadership, and extrinsic motivation	Difficulty motivating employees to adopt secure behavior	Creating incentive structures
Pitfalls in Communication	Relevance of information	Managers might perceive generic information as irrelevant to their work	Evaluating department needs to ensure information relevance
	Responsibility not clearly communicated	Managers do not engage or prioritize CS questions	Communicate managers responsibility of CS in the role description
	Too much trust to IT & ISO	Impeding proactive threat awareness among middle managers	Clearly communicating shared responsibility to ensure alert managers - send out policy reminders
Policy & Instructions	Generic policy & instructions	Difficulty enforcing CSP in daily operations	Cybersecurity instructions should be closely anchored in department's daily operations
	Top- and senior management not involving middle management	Generic policy & instructions, resulting in lower engagement and motivation for compliance	Involve middle managers to a larger extent in updates to policy & instructions
	Keeping policy alive and adaptive with dynamic threats	Outdated policy and instructions: Difficulty using policy & instructions as support in daily operations	By involving and engaging all levels of management, align efforts to ensure that CS is seen as a dynamic issue that need continues work

Table 3: Barriers, associated risks, and solutions for achieving increased CS readiness

5.5 Limitations of the Study

The case study was conducted on a single organization; however, we believe it would be beneficial and interesting to conduct a study on multiple municipality-owned or private organizations in the future. This would provide deeper insights into differences and similarities

in managers' perceived experiences with management questions in relation to cybersecurity. This could result in drawing more precise conclusions regarding the influence and best practices of management at all levels within organizations and identify additional barriers to achieving cybersecurity readiness. Further, it would have been interesting to compare the studied organization with other organizations that have worked with cybersecurity for a longer period. This could provide a higher quality of empirical data since managers would have had more time to reflect on cybersecurity initiatives and their own influence. With the time limitations of the study and limitation of the number of respondents, we also believe it would be interesting to include more respondents with different individual properties. This could provide a deeper understanding of how age, gender, experiences, and personality affect managing cybersecurity endeavors.

6. Conclusions

The aim of the study was to provide a deeper understanding of how management at all levels understands and influences organizations' initiatives to achieve cybersecurity readiness to identify barriers. This was explored through a case study where six managers were interviewed about their perceptions. The result and discussion showcase multiple barriers related to managers' perceived understanding and influence on enforcing compliance with cybersecurity policy and instructions (see Table 3). Standardized training, foreseeing the role of middle management, generic policy and instructions, and relevance of information are some examples of barriers that might appear in organizations during cybersecurity initiatives. Thereby, the research question of: "What are the barriers to achieving cybersecurity readiness?" has been answered. The second research question "What strategies can be implemented to mitigate the risks associated with identified barriers?" has been answered by analyzing the result with previous research. These are presented as possible strategies in Table 3. Continuous evaluation of employees' cybersecurity awareness, developing tailored training programs adhering to departments' needs, communicating managers' responsibility of CS in the role description, and involving middle managers to a larger extent in updates to policy and instructions are some solutions that could mitigate the risks of specific barriers.

The study's findings provide additional knowledge on the impact management play in achieving cybersecurity readiness. Specifically, our findings significantly highlight the important role middle management plays in enforcing cybersecurity policy and instructions and enhancing cybersecurity readiness. The study is conducted within the context of a municipality-owned organization in the initial phase of their work with cybersecurity and might thereby not be generalizable to all contexts. However, the study is exploratory and can act as a foundation for future research to further investigate identified barriers to present best practices that are applicable to a wider array of organizations. Further, it would be interesting for future research to conduct a comparative case study between multiple organizations, highlighting similarities and differences between middle managers' perceived experiences of enforcing cybersecurity governance strategies. The dynamic landscape of cybersecurity threats constitutes the need for future research that can identify updated practices and strategies for organizations to consider.

References

Abukari, A., & Bankas, E. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *International Journal of Scientific and Engineering Research* 11(4):1401-1407

Agrawal, A., Gans, J., & Goldfarb, A. (2018). *Prediction machines: the simple economics of artificial intelligence*. Harvard Business Press.

Al Khajeh. (2018). Impact of Leadership Styles on Organizational Performance. *Journal of Human Resources Management Research*, 1–10. https://doi.org/10.5171/2018.687849

Almeida, F., Duarte Santos, J., & Augusto Monteiro, J. (2020). The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World. *IEEE Engineering Management Review*, 48(3), 97–103. https://doi.org/10.1109/EMR.2020.3013206

Bass, B. M. (1985). *Leadership and performance beyond expectations*. New York: Free Press.

Bass, & Riggio, R. E. (2006). *Transformational leadership* (2. ed.). L. Erlbaum Associates.

Braun, & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age : work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.

Campbell, Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, 25(8), 652–661. https://doi.org/10.1177/1744987120927206

Carter, N., Bryant-Lukosius, D., Dicenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5), 545–547. https://doi.org/10.1188/14.ONF.545-547

Corradini, & Nardelli, E. (2019). Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. In *ADVANCES IN HUMAN FACTORS IN CYBERSECURITY, AHFE 2018* (Vol. 782, pp. 193–202). Springer Nature. https://doi.org/10.1007/978-3-319-94782-2_19

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. https://doi.org/10.22215/timreview835

Crossler, Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

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), 101693. https://doi.org/10.1016/j.jsis.2021.101693

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988. https://doi.org/10.1016/j.cose.2012.08.004

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, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 29(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528

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

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

Inness, Turner, N., Barling, J., & Stride, C. B. (2010). Transformational Leadership and Employee Safety Performance: A Within-Person, Between-Jobs Design. *Journal of Occupational Health Psychology*, 15(3), 279–290. https://doi.org/10.1037/a0019380

ITU, 2008. Overview of cybersecurity, ITU-T X.1205. [online] Available at: https://www.itu.int/rec/T-REC-X. 1205-200804-I/en [Accessed 14 Apr. 2023].

Jensen, M,. Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems*, 34(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019*, 338–345. https://doi.org/10.1109/CIC48465.2019.00047

Johnson, E., & Goetz, E. (2007). Embedding Information Security into the Organization. *IEEE Security & Privacy*, 5(3), 16–24. https://doi.org/10.1109/MSP.2007.59

Khan, S., & Madnick, S. (2019). Cybersafety: A System-theoretic Approach to Identify Cyber-vulnerabilities & Mitigations in Industrial Control Systems. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3542551

Kvale, S., & Brinkmann, S. (2014). *Den kvalitativa forskningsintervjun*. (Tredje [reviderade] upplagan). Studentlitteratur.

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, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Madnick, S., Jalali, M. S., Siegel, M., Lee, Y., Strong, D., & Wang, R. (2017). *Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems* (pp. 113–127). Mit Press.

McLaughlin, M. & Gogan, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, 17(3), 237–262.

Merriam, S.B., & Tisdell, E.J. (2016). Qualitative research: *a guide to design and implementation Fourth edition*. San Francisco, CA: Jossey-Bass, a Wiley Brand.

Morris, D., Madzudzo, G., & Garcia-Perez, A. (2020). Cybersecurity threats in the auto industry: Tensions in the knowledge environment. *Technological Forecasting and Social Change*, 157, 120102.

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

Möller, D.P.F. (2020). Cybersecurity Leadership. In: *Cybersecurity in Digital Transformation*. SpringerBriefs on Cyber Security Systems and Networks. Springer, Cham. https://doi.org/10.1007/978-3-030-60570-4_8

Neigel A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92, 101731–101736. https://doi.org/10.1016/j.cose.2020.101731

Odumeru, J.A. & Ifeanyi, G.O. (2013). Transformational vs. transactional leadership theories: Evidence in literature. *International Review of Management and Business Research*. 2(2). 355-361.

Paté-Cornell, E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis*, 38(2), 226-241. https://doi.org/10.1111/risa.12844

Patterson, Hobbs, M., & Zhu, T. (2017). A cyber-threat analytic model for autonomous detection of virtual property theft. *Information and Computer Security*, 25(4), 358–381. https://doi.org/10.1108/ICS-11-2016-0087

Pilbeam, Doherty, N., Davidson, R., & Denyer, D. (2016). Safety leadership practices for organizational safety compliance: Developing a research agenda from a review of the literature. *Safety Science*, 86, 110–121. https://doi.org/10.1016/j.ssci.2016.02.015

Pranggono, & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, 4(2). https://doi.org/10.1002/itl2.247

Ruck, K. & Welch, M. (2012). Valuing internal communication; management and employee perspectives. *Public Relations Review*, 38(2), 294–302. https://doi.org/10.1016/j.pubrev.2011.12.016

Saarikko, T., Westergren, U. H., & Blomquist, T. (2020). Digital transformation: Five recommendations for the digitally conscious firm. *Business Horizons*, 63(6), 825-839.

Scala, N., Reilly, A., Goethals, P., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, 39(10), 2119–2126. https://doi.org/10.1111/risa.13309

Shamoo, A.E. and Resnik, D.B. (2009). *Responsible conduct of research*. 2nd edition. Oxford: Oxford University Press.

Shaikh, & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974–. https://doi.org/10.1016/j.cose.2022.102974

Szczepaniuk, E. & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, 46(3), 102282–. https://doi.org/10.1016/j.telpol.2021.102282

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Verma, S., & Gustafsson, A. (2020). Investigating the emerging COVID-19 research trends in the field of business and management: A bibliometric analysis approach. *Journal of Business Research*, 118, 253-261. https://doi.org/10.1016/j.jbusres.2020.06.057

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*. 15(3), pp.320–330.

Warrilow, S., (2012). Transformational leadership theory-The 4 key components in leading change & managing change. *Harvard Business Review*., 2(3).

World Economic Forum, 2020, *COVID-19 risks outlook: A preliminary mapping and its implications*, viewed 04.12.2023, from https://www.weforum.org/global-risks/reports.

Wiederhold, BK. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior and Social Networking*., 17(3). https://doi.org/10.1089/cyber.2014.1502

Yin, R.K. (2018). *Case study research and applications: design and methods*. 6th edition. Thousand Oaks, California: SAGE

Yusif, S. & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, 16(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995

Zohar. (2002). The effects of leadership dimensions, safety climate, and assigned priorities on minor injuries in work groups. *Journal of Organizational Behavior*, *23*(1), 75–92. https://doi.org/10.1002/job.130

Zohar, D., & Tenne-Gazit, O. (2008). Transformational leadership and group interaction as climate antecedents: A social network analysis. *Journal of Applied Psychology*, 93(4), 744–757. https://doi.org/10.1037/0021-9010.93.4.744

Appendix 1. Interview Guide

Du intervjuas idag då du är anställd av och jobbar för [företaget] och innefattar en roll som har ett personalansvar, stämmer det?

Har du några funderingar eller frågor innan vi kör igång?

Bakgrund

- Hur gammal är du och när började du jobba hos [företaget]?
  - Vilken verksamhet har du ansvar för och vad arbetar ni med?
  - Kan du berätta lite om din arbetsroll och hur en arbetsdag ser ut idag?
  - Vilken roll spelar du för att upprätthålla organisationens informationssäkerhets policys och instruktioner?
- Vad gjorde du innan du började jobba hos [företaget]
  - Har du någon tidigare erfarenhet av att ha ansvar för informationssäkerhet?
  - Hur har det påverkat ditt nuvarande arbete med informationssäkerhet?
    - Vilka lärdomar har du tagit med dig från tidigare anställningar?

Då rör vi oss vidare till det första segmentet som behandlar dina upplevelser kring förståelse och kunskap kring informationssäkerhets policys och instruktioner:

***Förståelse* för informationssäkerhetspolicy**

- Kan du beskriva informationssäkerhet som du själv vill definiera det?
- Hur bekant är du med organisationens informationssäkerhet policys och instruktioner?
  - Vart hittar du dessa policys och procedurer?
    - (På ett intranät? Privat lagringsyta? Analogt?)
  - Ser du det som viktigt att en verksamhet har en policy och instruktioner för informationssäkerhet?
    - Varför?
- Vilka steg har du tagit för att försäkra dig att du har en grundlig förståelse av dem?
  - Kommuniceras vikten av ditt ansvar att upprätthålla regler och rutiner?
    - Hur kommuniceras den?
  - Ställs det några krav på dig att kontinuerligt uppdatera din förståelse och medvetenhet om organisationens policy och instruktioner?
  - Upplever du att styrdokumenten som finns är tillräckliga för att få en bra förståelse för ditt ansvar kring informationssäkerhet?
- Har du någonsin upplevt svårigheter med att följa eller förstå organisationens policy och instruktioner?
  - Om ja: Hur, beskriv?
  - Om nej: Vad är anledningen bakom det?
- Har du fått någon utbildning i informationssäkerhet?
  - Kan du beskriva hur sådan utbildning sett ut?
  - Hur upplevde du processen? (Hur har det hjälpt dig i din nuvarande roll?)
  - Fanns det något som du upplevde saknades med utbildningen, i så fall vad?

Nu tänkte vi gå vidare och prata lite om dina upplevelser kring incidenthantering och medvetenhet om hotbilder och hur du säkerhetsställer att du själv men även dina medarbetare har förståelse för hur incidenter ska hanteras och kontinuerligt är medvetna om potentiella hot.

Incidenthantering

- Kan du beskriva hur processen ser ut vid en säkerhetsincident?
    - Är det en skillnad på hur incidenter hanteras beroende på allvaret av incidenten?
        - På vilket sätt?
    - Hur säkerhetsställer du och ni som organisation att liknande incidenter inte upprepas i framtiden?
- Kan du ge ett exempel på när du varit tvungen att använda organisationens informationssäkerhet policys och instruktioner?
    - Hur visste du vilken strategi eller rutin att vända dig mot? (svårigheter/enkelhet)
    - Kan du beskriva resultatet av denna incidenthantering?
- Vilka steg har organisationen tagit för att försäkra att organisationen är redo för att hantera incidenter i framtiden?
    - Har du personligen gjort något för att försäkra att oraganisationen är mer redo för potentiella incidenter i framtiden?
- Kan du beskriva konsekvenserna av att inte följa organisationens informationssäkerhet policys och instruktioner?
    - Anser du att de instruktioner och utbildningar organisationen förser anställda med är tillräckliga för att hantera olika incidenter som kan uppstå?
        - Om ja: Varför?
        - Om nej: Vad anser du saknas?
- Vad tror du är den största risken för att information hanteras fel?
    - Varför? Vad gör du för att minimera den risken?

Medvetenhet om hotbild

- Hur upplever du att din medvetenhet kring cyberhot är?
    - Upplever du att du har en god förståelse kring vilka hot som finns mot organisationen?
    - Upplever du att du har färdigheter att hantera denna hotbild?
- Hur håller du dig uppdaterad och medveten om potentiella hot mot verksamheten du arbetar inom?
    - Vilka metoder använder du dig av för att samla information om informationssäkerhet hot?
    - Hur beslutar du vilka hot som är mest relevanta att motarbeta?
- Hur bekant är du med olika former av cyberattacker, såsom phising (nätfiske), malware (skadlig programvara), och ransomware (utpressningsprogram)?
    - Kan du beskriva hur sådana attacker kan se ut, och vilka potentiella risker de har för din verksamhet?
    - Har du någonsin upplevt någon av dessa attacker personligen?
        - Hur gick du tillväga för att upptäcka och hantera attacken? (hjälpte policys och instruktioner eller utbildning dig i en sådan situation?)
- Hur upplever du att beredskapen och medvetenheten för cyberattacker är på organisationen?
    - Hög/låg? (på vilket sätt, varför?)

Som du säkert är medveten om lever vi i en tid där mycket förändring sker inom alla områden i samhället, så för att gå vidare tänkte vi prata lite om hur du personligen samt ni som organisation säkerhetsställer att arbetet med att utveckla och förbättra informationssäkerhet är något som sker parallellt med vardagligt arbete?

Kontinuerlig förbättring

- Hur ser du och organisationen till att medvetenhet och kunskap om informationssäkerhet förbättras bland alla medarbetare?
    - Brukar ni ha kontinuerliga möten där informationssäkerhet diskuteras?
    - Vad brukar ungefär tas upp under sådana möten?
        - Känner du att du har möjlighet att lyfta frågor kring informationssäkerheten ifall du har funderingar eller känner dig orolig kring informationssäkerheten?
            - Har du någonsin varit involverad i att implementera eller uppdatera informationssäkerhetspolicys och instruktioner?
            - Kan du beskriva hur den processen såg ut?

Det nästa segment vi tänkte prata om är ledarskap och kultur, då man som ledare har ett ansvar att säkerhetsställa att riktlinjer följs och respekteras inom organisationen, men även frågor kring hur ni som organisation och verksamhet fungerar.

Ledarskap och kultur

- Hur väl tror du medarbetare förstår och är medvetna om organisationens policys och instruktioner?
    - Hur upplever du din förmåga att få personal att följa policys and instruktioner?
        - Hur upplever du din förmåga att få personal att genomföra utbildningar?
        - Hur upplever du att det är att försöka motivera personalen att genomföra träning/följa policys och instruktioner?
        - Gör du något för att se till att medarbetare inom din verksamhet faktiskt genomför utbildningar och följer policys?

- Upplever du att du har tillräckliga resurser för att ansvara över informationssäkerhet inom din verksamhet?
    - Om ja: Kan du ge ett exempel på något som hjälpt dig i ditt arbete?
    - Om nja/nej: Vad upplever du saknas?
- Har du någonsin upplevt motstånd från medarbetarna att följa rutiner och strategier för informationssäkerhet?
        - Om ja: Beskriv hur du gick tillväga för att lösa problemet?
        - Om nej: Hur skulle du lösa ett sådant problem?
- Har ni några informationsäkerhetsmål ni arbetar efter och strävar efter att uppnå?
    - Vad är det för mål?
    - Hur arbetar du för att se till att samtliga inom din verksamhet gemensamt arbetar mot att uppnå dessa mål?

- Hur skulle du beskriva kulturen hos er organisation, och hur tror du den påverkar ert arbete med informationssäkerhet?
    - Vad anser du viktiga värderingar, normer och attityder som kan bidra till en stark informationssäkerhetskultur?
    - Har du upplevt förändringar i organisationskulturen under de senaste åren, i så fall, vilka faktorer tror du påverkat dessa förändringar?
- Involverar du medarbetare inom din verksamhet för att utveckla och förbättra arbetet med informationssäkerhet?

Det sista segment vi tänkte prata lite om är hur du och din verksamhet arbetar med externa parter när det kommer till informationssäkerhet, och din upplevda förmåga att sköta sådana processer.

Externa parter

- Finns det andra typer av informationssäkerhetsfrågor eller andra typer av risker som dyker upp i ert arbete med externa partners?
- Hur säkerhetsställer du att externa parter som behandlar eller har insyn i Bostaden informationstillgångar är medvetna om hur information ska skyddas?
    - När externa parter ska involveras i Bostadens operativa arbete, finns det viktiga riktlinjer som måste följas då?
        - Vilka är dessa riktlinjer?
        - Hur säkerhetsställer ni som verksamhet eller organisation att information som behandlas av externa parter förblir skyddat?

Då har vi gått igenom alla segment och tänkte avsluta med att fråga lite kring dina tankar om utmaningar och områden du anser kan utvecklas.

Utveckling

- Vad ser du som den största utmaningen med att upprätthålla din egen och medarbetarnas medvetenhet och förståelse för informationssäkerhet?
    - Vad, om något, anser du att du kan göra annorlunda för att upprätthålla att policy och instruktioner följs?
    - Finns det något du önskar som skulle få dig att känna dig mer kompetent inom informationssäkerhet?
- Hur ser du på den ideala situationen för er när det handlar om informationssäkerhet?
    - Hur fungerar informationssäkerhet när det fungerar som bäst?
- Är det något du känner att du vill lyfta eller något annat du vill tillägga?

Appendix 2 Examples of Data Analysis

Example respondent statement	Summary of statement	Open codes
Can you, in your words, describe the importance of having CS policy and instructions? I would say that it's vital because you can't as a manager, or whatever role you have be responsible for security if the goal is not defined. And the owner, senior management, and board needs to stand behind this, because otherwise you will never get money and resources for the work and it will always be possible to question why you should follow it. When you put the foot down and it's documented and said this is how we do this, that's when the rest of work starts, which is hard enough as is. But without a policy, you're left in the dark, you need to agree in the organization of what you want to achieve.	Policy is essential Importance of communication Shared visions between management levels in order for resources to be allocated towards CS Security goals need to be clearly defined and communicated	Importance of policy Shared visions Management support Security goals Clear communication Agreement - management

Figure 1: Example of coding

Categories with related codes	Sub-theme with related codes	Overarching theme
Collaboration and information Information sharing Information gathering Clear communication Relevant information APT (workplace meetings) Contact chain Lack of communication Incorporate policy Reminders Reflection Availability Updates External parties **Role Clarity** Personal responsibility Role responsibility Ambiguity of responsibility Taking responsibility Work role Managerial responsibility Managerial role Own responsibility Functional responsibility Shared responsibility Management responsibility System owner involvement Business responsibility Uncommitted Nonchalance	**Communication, Information & Responsibility** Information sharing Information gathering Clear communication Relevant information APT (workplace meetings) Contact chain Lack of communication Incorporate policy Reminders Reflection Availability Updates External parties Personal responsibility Role responsibility Ambiguity of responsibility Taking responsibility Work role Managerial responsibility Managerial role Own responsibility Functional responsibility Shared responsibility Management responsibility Business responsibility Uncommitted System owner involvement Nonchalance	**Communicating Cybersecurity - Barriers to Information Sharing and Responsibility**

Figure 2: Example of combined categories and sub-theme with related codes, and overarching theme

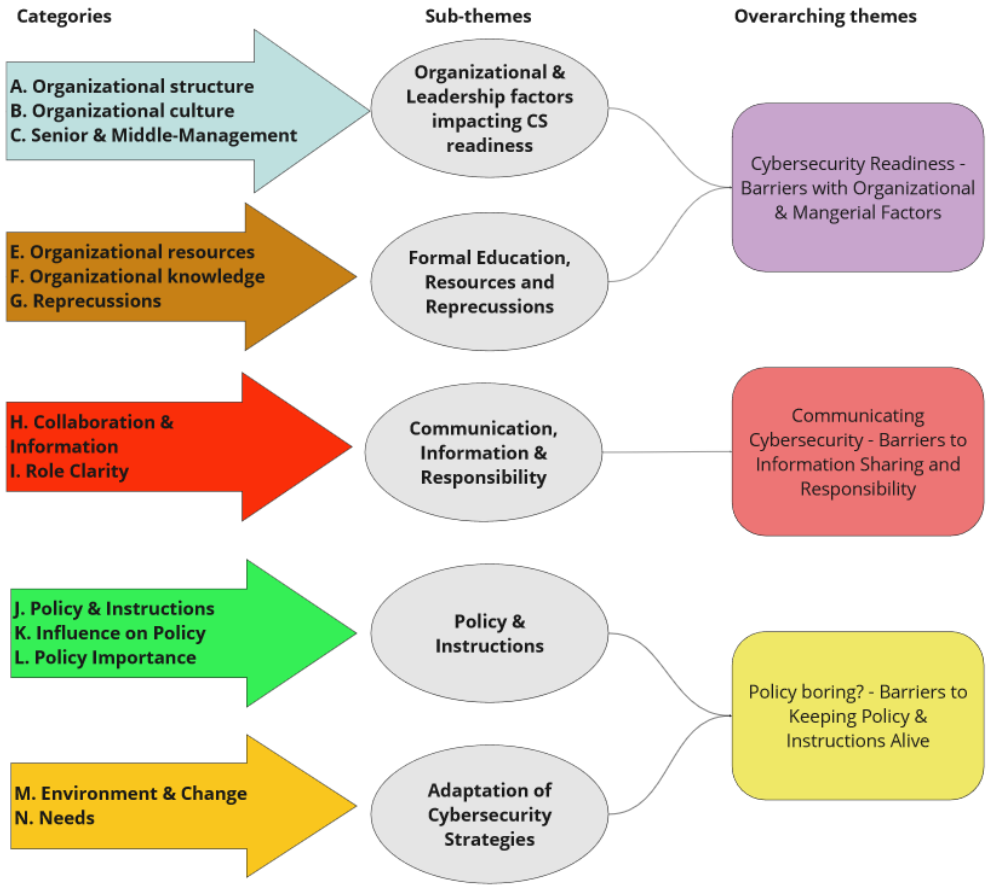

Figure 3: Overview of combined categories, sub-themes, and overarching themes