LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Fighting AI with AI

Decision Influencers' Considerations Regarding the Implementation of AI-driven Cybersecurity in Large Swedish Companies

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Tim Brinkhagen
Hendrik von Krusenstierna

Handledare: Nicklas Holmberg & Markus Lahtinen

Rättande lärare: Blerim Emruli & Umberto Fiaccadori

Fighting AI with AI: Decision Influencers' Considerations Regarding the Implementation of AI-driven Cybersecurity in Large Swedish Companies

SVENSK TITEL: Beslutspåverkares överväganden gällande implementering av AI-driven cybersäkerhet i stora svenska företag

FÖRFATTARE: Hendrik von Krusenstierna, Tim Brinkhagen

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: maj, 2024

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 69

NYCKELORD: AI-driven cybersecurity, Decision influencers, Considerations, TOE framework, Large Swedish companies

SAMMANFATTNING (MAX. 200 ORD):

This thesis examines the considerations of decision influencers in large Swedish companies concerning the implementation of AI-driven cybersecurity solutions. Through a qualitative analysis involving semi-structured interviews, this study explores the interplay of technological, organizational, and environmental factors influencing these decisions. Our findings reveal that while AI is perceived as a potential complement to cybersecurity systems, its implementation is fraught with challenges. Technological considerations include the integration complexity with existing systems and the need for infrastructural readiness. Organizationally, the adoption is influenced by the perceived benefits, organizational structure, and the commitment of top management. Environmentally, regulatory compliance and competitive pressures play significant roles. Overall, large Swedish companies seem to have a low adoption rate regarding AI-driven cybersecurity and generally, they are cautious of AI by itself.

Table of Contents

Figures

Tables

1 Introduction

1.1 Background

The digital ecosystem is increasing in size while the frequency and sophistication of cyber-attacks have gone up, creating difficult challenges in cybersecurity. A recent example is the ransomware attack, where malicious software encrypts a victim's data, making it inaccessible until the ransom is paid to the attacker (IBM, 2024), on the large IT-provider Tietoevry which, among other things, affected the payroll system for over 100 government agencies in Sweden (SVT, 2024). According to Microsoft (2023), organizations faced an increased rate of ransomware attacks compared to the previous year, with the number of human-operated ransomware attacks up more than 200% since September 2022. Furthermore, a recent report by Microsoft (2024), in collaboration with OpenAI, reveals the emergence of AI-assisted cyber-attacks. They have identified several state sponsored hacker groups using Large Language Models (LLM) to find vulnerabilities in systems. Besides the frequency and sophistication, the economic losses caused by cyber-attacks is also on the rise. According to IBM Security (2023), the economic losses caused by data breaches are at an all-time high. They report that, in 2023, the average cost for a company suffering from a data breach has reached USD 4.45 million, which is an increase of 2.3% from the previous year and a substantial increase of 15.3% compared to 2020.

Artificial Intelligence (AI), as detailed by Russel & Norvig (2016), is, among other things, the study and design of intelligent "agents", where an intelligent agent is a system that perceives its environment and takes actions that maximize its chances of success. They explain that AI involves the development of algorithms and models that enable machines to perform tasks that require human-like intelligence. These tasks include understanding natural language, recognizing patterns and images, making decisions based on incomplete or complex information, and learning from experience. Craigen et al. (2014) has described cybersecurity by coming up with an all-inclusive and coherent definition. In their definition, cybersecurity is "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al. 2014, p.1). AI-driven cybersecurity, as described by Sarker et al. (2021), is the utilization of AI technologies in cybersecurity defense mechanisms to increase the security of the digital assets and networks.

As a result of the evolving threats, traditional methods in cybersecurity have become heavily strained by the increased severity and complexity of these attacks (Varma et al. 2023), calling for businesses to adapt, or face the growing cost of data breaches and reputational damage. Consequently, the development and implementation of cybersecurity measures to detect and mitigate such threats have become increasingly critical. Technologically, AI and machine learning have played a critical role in developing predictive models that can identify and neutralize threats before they occur (Apruzzese et al. 2018) and according to Gerlach et al. (2022), the market for AI-driven cybersecurity solutions is on the rise.

The role of AI in cybersecurity seems to be an important factor as IBM Security (2023) has found that implementations of AI in cybersecurity strategies has been able to mitigate breach costs and shorten the time from breach to containment. They state that the average breach cost for organizations with an extensive use of AI in their cybersecurity processes is USD 3.6 million compared to organizations with no use, suffering an average of USD 5.36 million per breach. The time to identify and contain a breach was 214 days for extensive users and 322 for no use. This clearly highlights the benefits for organizations of implementing AI-driven cybersecurity processes but as IBM Security (2023) show, only 28% of organization fall into the category of extensive use while 39% have not adopted it at all. Although the benefits of AI-driven cybersecurity are evident, what are the considerations for companies regarding the implementation?

1.2 Problem Statement

The evolving cyber threat landscape calls for evolving cyber defences. As IBM Security (2023) has shown, there are several advantages of implementing AI-driven cybersecurity and considering Microsoft's (2024) findings on the increasing use of AI in cyber-attacks, this advantage can be expected to be even more valuable as time goes on. Lourens et al. (2022) Varma et al. (2023) argue that traditional security measures are insufficient in today's threat landscape while shedding light on the possibilities of AI technologies in preventing breaches.

However, as IBM Security (2023) have concluded, far from every organization have implemented extensive AI-driven cybersecurity measures. Broadening the perspective beyond just AI, it appears that the adoption of cybersecurity measures presents challenges for companies. Wallace et al. (2020) have interviewed IT-leaders at large companies in different sectors in the U.S. Midwest and have found several factors affecting cybersecurity adoption. They saw that IT-leaders had a fear of the unknown and user vulnerabilities as well as a perception that their firm wasn't mature enough. Switching focus to the adoption of AI itself, Merhi (2023) have concluded there are several factors hindering organizations' ability to implement. By interviewing ten AI-experts from various sectors, he could deduce that both ethics and IT infrastructure problems were major concerns. When it comes to implementation of AI-driven cybersecurity, AL-Dosari et al. (2024) have researched factors affecting Qatari banks. They have found challenges like a lack of employees with the appropriate skillset, compatibility with existing systems and regulatory compliance issues. According to Jackson (2020), regulations like GDPR could impact the development and use of autonomous AI-driven cybersecurity solutions as their decision-making capabilities could conflict with GDPR's requirements for human intervention and explainability in decisions affecting individuals.

The research we have found regarding AI and cybersecurity has often been with a focus on challenges and limitations of the actual technological solutions themselves, for example Zhang et al. (2022) & Lourens et al. (2022), researching challenges and solutions for AI techniques in cybersecurity. Furthermore, the reports like the one from IBM Security (2023) showing statistics on the advantages, does not delve into why organizations have not adopted AI in their cybersecurity strategies. The findings from Wallace et al. (2020) and Merhi (2023) provides a good starting point, but they are not specifically researching both AI and cybersecurity. Research by AL-Dosari et al. (2024) on Qatari banks delves into factors affecting implementation of AI-driven cybersecurity, however, their finding does not necessarily apply in other countries. Factors like regulations (Jackson, 2020), could be different in Europe. As for

Sweden, we have not been able to find any similar research, therefore we believe there is a research gap to be filled.

1.3 Research Question

With the above mentioned in mind, our research question is as follows:

- How are decision influencers in large Swedish companies considering the implementation of AI-driven cybersecurity?

1.4 Purpose

The primary purpose of this study is to explore the decision-making process of large Swedish companies regarding the implementation of AI-driven cybersecurity. The findings are expected to offer valuable recommendations for companies considering AI-driven solutions and contribute to a broader understanding of perceptions regarding AI in cybersecurity.

1.5 Delimitations

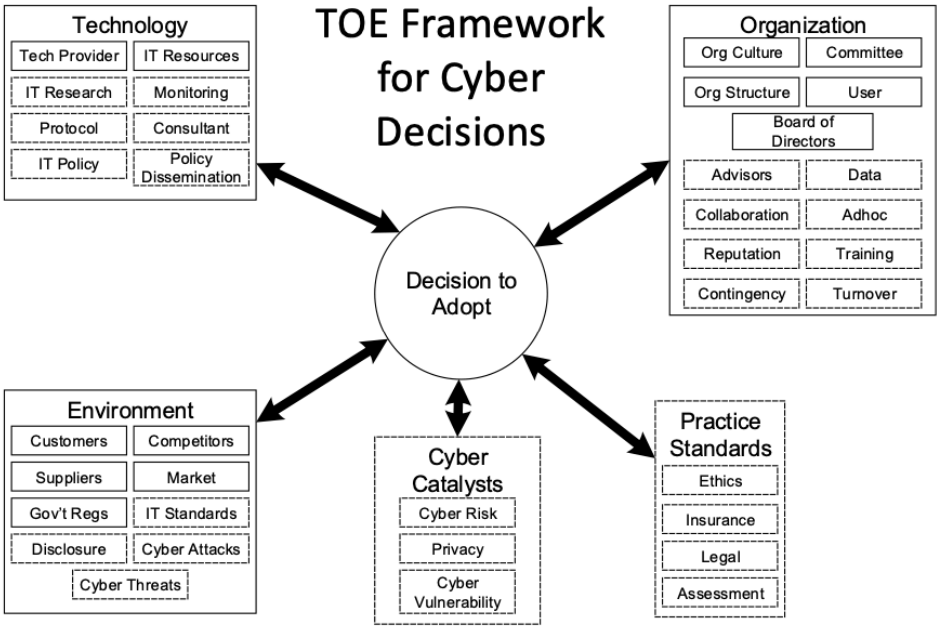
This thesis focuses specifically on the decision-making processes related to the implementation of AI-driven cybersecurity in large Swedish companies. The perspectives explored are primarily those of decision influencers at a strategic or management level.

2 A Framework for Cyber Decisions

2.1 Extended TOE Framework

Wallace et al. (2020) has in their research, based on the original Technology, Environment, Organization (TOE) framework (Depietro et al. 1990), proposed a new and extended framework for cybersecurity adoption. They argue that the traditional TOE framework uses dimensions that are better suited for more generic technology adoption. Because of this, they have added two new dimensions, *Cyber Catalysts* and *Practice Standards*, that are specific for cybersecurity adoption decisions. Furthermore, they have included additional factors in the original dimensions to encompass a more tailored view. In the traditional TOE framework, factors and dimensions can affect each other, for example, organization affecting the environment by virtue of personnel (organization) interacting with customers (environment). Similarly, for this extended framework, the new dimensions can affect other parts of the framework.

Wallace et al. (2020) highlights that further research is required to validate the new extended framework. They suggest others to validate the framework by for example, researching the magnitude of the new dimensions in adoption decisions and the impact of GDPR. The framework is appropriate for our study as it offers a tailored, comprehensive, and dynamic model for understanding cybersecurity adoption. Its specificity to cybersecurity, combined with the inclusion of new dimensions that capture the unique aspects of cybersecurity adoption, provides a solid foundation for analysing and deriving insights into the factors influencing the implementation of cybersecurity technologies and practices. We believe their framework proves suitable for the purpose our study and therefore, we will use this as basis for our theoretical framework.



Note: All dimensions affect each other. Boxes with dotted borders are new dimensions/factors not found in traditional TOE Framework

Figure 2.1: The Extended TOE Framework (Wallace et al. 2020)

2.2 Technology

In the original TOE-framework, *Technology* includes the current technological solutions available in the market that an organization can choose to implement (Depietro et al. 1990). The decision to adopt a particular technology is influenced by the available options to the organization or company. Wallace et al. (2020) describes the technological dimension as including for example, IT infrastructure and IT personnel that affect the decision to adopt. This represents the organization's technological readiness.

The technological dimension includes not only the hardware and software infrastructure but also the strategic implementation of emergent technologies like artificial intelligence, particularly in sensitive sectors, where cybersecurity is of high importance (AL-Dosari et al., 2024). These technologies can offer significant advantages in detecting and countering cyber threats but also introduce new challenges related to their integration, management, and regulation.

Merhi (2023) have identified a lack of adequate IT infrastructure as a factor in AI-implementation. He argues that this is a prerequisite for successfully implementing and adopting AI-systems. Wallace et al. (2020) has similarly to Merhi (2023), seen IT-infrastructure as a factor. Furthermore, Merhi (2023) saw that integration complexity plays a significant role, meaning, the ability to integrate AI systems with current infrastructure such as existing systems and databases. This can be compared with Hasani et al. (2023) findings on IT modularity in cybersecurity adoption. Integration complexity is something AL-Dosari et al. (2024) also have identified as factor. They found that legacy systems can hinder the integration of AI technology and that it's difficult to convert all these systems at once. Additionally, their respondents suggested that in-house development of AI-driven cybersecurity was not feasible and therefore, they were heavily dependent on third party tech providers. The tech provider factor can also be seen by Wallace et al. (2020) for cybersecurity adoption. Furthermore, one of their respondents, a CISO at a large manufacturing company, said that his employer didn't have a dedicated cybersecurity department.

2.3 Organization

In the original TOE framework, the dimension *Organization* covers the characteristics of the firm that affect adoption decisions (Depietro et al. 1990). This includes for example, organizational structure, personnel, culture and size.

AL-Dosari et al. (2024) have identified several organizational factors affecting the implementation of AI-driven cybersecurity. They have seen obstacles like the need to train employees and a lack of workers with the appropriate skillset. This is also seen by Wallace et al. (2020) for cyber adoption. Furthermore, they have observed that a common occurrence is that a well-defined plan for AI implementation does not exist, a factor which Merhi (2023) also has pointed out in his research about factors impacting AI implementation.

Merhi (2023) has also identified that the top management's commitment to implementation is a crucial factor, which AL-Dosari et al. (2024) also has pointed out. Additionally, he saw that the lack of visibility on benefits was the second most important factor in the organizational context. Furthermore, he argues that organizations consider how the implementation could impact and change the organization's structure and also that the organizational culture is an important factor in successful integrations of AI. This aligns well with Hasani et al. (2023) and their investigation of cybersecurity adoption using the TOE framework.

2.4 Environment

In the original TOE framework, the dimension *Environment* covers the external forces that may affect implementation (Depietro et al. 1990). This includes for example, suppliers, competitors, government regulations and industry.

Merhi (2023) have identified several environmental factors in implementation of AI. They include high cost of AI and selection of suppliers. As for high cost of AI, they argue there's a financial obstacle for implementing AI-systems. This is because it's associated with not only the initial cost but also ongoing expenses for maintenance and training. They argue that this is a critical factor for the decision-making process. When it comes to selection of suppliers, they argue that this can influence the success of AI implementation, however, they noted that this factor had the lowest weight in their study. For cybersecurity adoption, Hasani et al. (2023) found supplier support a significant factor. Wallace et al. (2020) also found suppliers as a factor but for their respondents, the perceived importance varied heavily. Furthermore, they could see that the two original factors of the TOE framework, competitors and market, had little to no relevance in cybersecurity adoption decisions. On the contrary, Hasani et al. (2023) observed competition to be a notable factor.

As for IT-standards, Wallace et al. (2020) saw that most respondents perceived this as factor in their cybersecurity decisions. The majority of respondents said that their cybersecurity decisions were influenced, at least in part, by IT standards or best practices, such as the standard framework ISO 27002. When it comes to regulations, AL-Dosari et al. (2024) have identified a concern for regulations conflicting with AI-based technologies. They saw that several experts were worried about regulations like GDPR and CCPA hindering some of the AI implementation. Wallace et al. (2020) has also expressed GDPR as an issue for cyber adoption. This is also supported by Jackson (2020) who argue that the continuous development of AI-based cybersecurity systems will lead to systems with more autonomy that could potentially struggle with GDPR compliance.

2.5 Cyber Catalysts

In the extended TOE-framework, the dimension of *Cyber Catalysts* is one of the proposed extended dimensions. The *Cyber Catalyst* dimension identifies factors that incite the adoption of cybersecurity measures beyond the traditional technological, organizational, and environmental aspects (Wallace et al. 2020). This includes cyber vulnerability, privacy, and cyber risk (Wallace et al. 2020). These catalysts capture the complexity and unpredictable nature of cyber threats. This also includes an organization's exposure to cyber vulnerabilities, privacy considerations critical to stakeholder trust, and the assessment and management of cyber risk.

Cyber vulnerabilities refer to the weaknesses or flaws in a computer or system, that if exploited can result in unauthorized access or attacks. Unlike traditional information security, which focuses primarily on protecting information assets, cybersecurity extends to protecting not only information and technology, but also the users and their personal data. This also includes tangible and intangible interests that are vulnerable to cyber threats (von Solms & van Niekerk, 2013). Cyber vulnerabilities also influence decisions regarding cybersecurity adoption as they signify weaknesses that decision makers must recognize to ensure the safety of their organization (Wallace et al. 2020).

Privacy relates to safeguarding personal information from unauthorized access, misuse, or exposure, ensuring that individuals data is protected and only accessed by authorized parties (Herrmann & Pridöhl, 2020). Nowadays, with the privacy landscape constantly shifting, decision makers in companies and organizations must also think about privacy issues like GDPR when they make decisions, while still having to make sure they protect the personal information and data of their employees and stakeholders (Wallace et al. 2020).

Cyber risk includes the uncertainty and potential negative and damaging outcomes associated with securing system and data against cyber threats. Wallace et al. (2020) highlights the need for organizations to adopt a comprehensive and forward-thinking approach to cybersecurity, acknowledging the important role of cyber catalysts in influencing cybersecurity adoption decisions. This perspective from Wallace et al. (2020) emphasizes the growing and evolving challenges organizations and companies may face in securing their digital landscapes and the importance of integrating these catalysts into strategic planning and decision-making processes, to efficiently mitigate cyber risks and vulnerabilities.

2.6 Practice Standards

In the extended TOE-framework, Wallace et al. (2020) proposes the dimension of *Practice Standards*. The *Practice Standards* dimension covers the general best practices influencing cybersecurity decisions. More specifically, the consideration of ethical, legal and cybersecurity assessment factors in the decisions of cybersecurity adoptions.

Wallace et al. (2020) highlights the legal factor as a critical factor in cybersecurity adoption. They point out the importance of compliance with laws and regulations as a driving force behind adoption decisions. Legal considerations extend beyond mere compliance, they involve proactive engagement with legal frameworks to minimize cybersecurity breach costs and mitigate the consequences of breaches. They bring up the Equifax incident (U.S. House of Representatives Committee on Oversight and Government Reform, 2018) to illustrate the severe repercussions of failing to adhere to legal and ethical standards.

The ethical factor is another aspect of cybersecurity adoption explored by Wallace et al. (2020). Ethical considerations are integral to the decision-making process, as they reflect a firm's commitment to conducting its operations responsibly. They underscore that adherence to ethical standards is not only about making sound decisions but also about executing processes that safeguard the firm's reputation and the trust of its stakeholders. This can be seen for AI adoption as well through Merhi (2023) who found ethics to be the number one factor.

Furthermore, Wallace et al. (2020) explores risk assessments. They identified the significance of conducting thorough risk assessments to identify potential threats and vulnerabilities for organizations to address and mitigate cybersecurity risks.

2.7 Literature Summary

In the following table (Table 2.1), the factors affecting the implementation of AI, cybersecurity, and AI-driven cybersecurity according to previous research are presented. The table structure is based on the dimensions from the Extended TOE Framework.

Table 2.1: Literature Overview

	AL-Dosari et al. (2024)	Hasani et al. (2023)	Jackson (2020)	Merhi (2023)	Wallace et al. (2020)
Technology					
IT-infrastructure				x	x
Integration complexity	x	x		x	
In-house development	x				
Tech provider	x				
Organization					
Employee training	x				x
Implementation plan	x			x	
Lack of skilled employees	x				x
Lack of visibility on benefits				x	
Organizational structure		x		x	
Organizational culture		x		x	
Top management commitment	x			x	
Environment					
Cost of implementation				x	x
Supplier support				x	x
IT-standards					x
Competition		x			
Regulations	x		x		x
Cyber Catalysts					
Cyber risk	x	x			x
Practice Standards					
Legal					x
Ethics				x	x

3 Methodology

In this chapter, we describe our research approach and the method used to gather data. We also cover the process of analysing the collected data and how we selected interview participants. Furthermore, we explain the quality and reliability of the data and ethical considerations.

3.1 Research Approach

We employed a qualitative approach in our study and collected data through semi-structured interviews. Oates (2006) argues that the responder is more receptive to new information when using a qualitative technique. Furthermore, the qualitative method is also suitable for investigating theories in order to learn more about a present issue. Although we had predetermined the interview questions, the semi-structured style allowed us to modify or add to them as necessary to further the discussion depending on the respondents' responses.

3.2 Collection of Literature

The purpose of the literary collection was to provide a thorough and comprehensive review of works that illustrate various aspects of the research subject. We used search engines like Google Scholar and LubSearch to locate papers. When looking for literature, the terms listed below were used:

- AI adoption
- Cybersecurity adoption
- AI and cybersecurity
- Challenges with AI in cybersecurity
- Factors affecting implementation of AI
- Factors affecting implementation of cybersecurity
- Factors affecting implementation of AI-driven cybersecurity

As there were not many papers focusing on explicitly factors affecting implementation of AI-driven cybersecurity, we mainly used papers researching either AI implementation or cybersecurity implementations. This approach allowed us to triangulate insights from both fields, building a nuanced understanding of the unique challenges and factors at play when implementing AI-driven cybersecurity. Through this method, we aimed to identify common themes, barriers, and facilitators.

Additionally, we made an effort to limit the sources we used to those that had been published within the last five years in order to be sure we were depending on the most recent research. It is noteworthy that while we have predominantly depended on information released in the past five years, there might have been certain cases in which we used older sources. This is because older sources still offer insightful and relevant information in cases when there hasn't been any recent research or advancement in a particular area of study. Furthermore, we read the abstracts and conclusions of the papers that we deemed relevant before analysing the entire paper.

3.3 Data Collection

3.3.1 Interview Format

Since interviews are a primary means of data collecting in qualitative research, we made the decision to use them to gather empirical data for our thesis research. We decided that semi-structured interviews were the most appropriate interview format for our research scenario. According to Bryman (2016), a semi-structured interview is a technique that mixes structured and open-ended questions to let the interviewer and respondent have a conversation. The semi-structured interview proved to be an appropriate approach.

Bryman (2016) claims that semi-structured interviews offer flexibility. We were able to follow up on intriguing and surprising comments from the respondents because of the approach's flexibility. Using both closed-ended and open-ended questions, we were able to go into a variety of subjects.

Another benefit with semi-structured approach was that the respondents were able to convey their ideas and opinions in their own terms throughout the interviews. As a result, the semi-structured interviews gave us a thorough understanding while also allowing us to record the respondents' responses without imposing our own prejudices or expectations.

Additionally, Bryman (2016) contends that although semi-structured interviews are open-ended, they do introduce some level of standardization. Standardization across the interviews was made easier by the use of organized topics that were outlined in the interview guide (see Appendix B). Even though the respondents may have had varying backgrounds, levels of expertise, and perspectives on the many topics, this standardization guaranteed that they all addressed the same subjects and questions. As a result, it was easier for us to compare and evaluate the interview data, finding themes and patterns in each respondent's response.

3.3.2 Selection of Respondents

In order to ensure that there was a wide representation of experiences and roles related to cybersecurity across sectors, participants were selected purposefully. This selection tried to balance through depth of insight and breadth of experience guaranteeing saturation but without detracting from the focus of this study. The intention was to capture a diverse array of perspectives on AI-driven cybersecurity implementation factors. We sought out individuals holding key positions in cybersecurity, specifically, people that had a direct or indirect influence on decisions in cyber security.

We decided to only research large companies because we believed that they were more likely to be further in thinking process regarding AI in cybersecurity. Furthermore, we only studied Swedish companies because it was the only market available within our reach and scope.

As our study was aimed at large companies, we selected respondents from companies that fulfilled the criteria of being a large company. For the criteria, we adhered to the definition from Bolagsverket (2019) which is as follows:

Larger companies are companies that meet two or all three of the following criteria during the last two fiscal years:

- more than 50 employees on average during the fiscal year
- more than SEK 40 million in balance sheet total
- more than SEK 80 million in net sales.

Table 3.1: Respondents Overview

Respondent	Sector	Role	Time and Date	Interview Length	Appendix
1	Telecom	CISO	14:00-14:30 12th April 2024	20 min	C
2	Tech	Senior Systems Developer	14:00-14:30 15th April 2024	22 min	D
3	Construction	Practice Lead – EA & IT Strategy	15:00-15:30 15th April 2024	25 min	E
4	Tech	Security Officer	09:00-09:30 30th April 2024	23 min	F

3.4 Data Processing and Analysis

This paper used thematic analysis to analyse the data we received from our semi-structured interviews, adhering to the framework specified by Braun and Clarke (2006). This qualitative method was specifically chosen for its strength and versatility in exploring complex topics.

3.4.1 Data Familiarization

Our process began with verbatim transcription of interviews, a critical step in preserving the authenticity and nuances of the participants insights (Braun & Clarke, 2006). Rigorous engagement with the transcripts through repeated readings enabled a profound immersion in the data. This initial phase was instrumental in highlighting emergent ideas and conceptual underpinnings, setting the groundwork for a data-driven analysis.

3.4.2 Generating Initial Codes

In order to keep the structure from the theoretical background, we decided to use the dimensions from the Extended TOE Framework as our themes. The themes were assigned a code letter representing the dimension. We also decided to add a theme for eventual additional findings beyond the framework. With this theme coding in place, we could simply match statements from the transcripts with the respective code corresponding to the theme being discussed. This made it easier and more structured for comparing our results and discussion with the theoretical background.

Table 3.2: Themes with Codes

Theme	Code
Technology	T
Organization	O
Environment	E
Cyber Catalysts	C
Practice Standards	P
Additional Findings	A

3.5 Use of AI

3.5.1 Transcription

The transcription of the interviews was done with the assist of AI. We used a local instance of Whisper where we could get the sound files transcribed automatically. Whisper offers compliance with the ethical conduct of Lund university. We considered this tool adequate for our integrity and confidentiality purposes. The transcripts made in Whisper, were afterwards manually gone through to correct mistakes and censor certain parts to keep anonymity.

3.5.2 Analysis of Literature

When analysing the literature, we made use of ChatGPT. Papers we deemed relevant based on abstracts and conclusions, were downloaded in PDF format and uploaded to ChatGPT. We made prompts to the chatbot that gave us information about the paper. This made it less time consuming to analyse the authors' methodologies, results and discussions.

3.6 Reliability and Validity

Oates (2006) points out that reliability and validity of empirical research are of crucial significance. Reliability is the ability of research findings to be repeated and verified. In essence, it is about the reproducibility of the results of a study if the experiment is repeated under the same conditions. For the sake of data reliability, we used the same data collecting methods for all the participants, minimized any possible errors and carried out the interviews in a uniform manner. In addition, we have focused on the sources that were either peer-reviewed or published, to ensure that the information we used as a base for our study is reliable.

Validity refers to the accuracy and relevance of the study's findings in terms of the research question (Oates, 2006). It checks whether the results are indeed true reflections of the phenomena under examination. In order to build the credibility of our research we did multiple interviews, applied proven research methods, and made sure that the information gathered was directly related to our research question. The selection process for interview participants was carried out using the criteria that had been set to identify individuals whose contributions would be most beneficial to our study aims and questions.

The role of semi-structured interviews was to enable an in-depth analysis of the key issues, making it possible to ask additional questions that contributed to the understanding of the issues. This is the same as what Oates (2006) says, that the study can be made more applicable and accurate if personal insights are added to it. Moreover, with the consent of recording and transcribing the interviews, we were able to precisely capture and reflect upon the participants' replies, that helped us to enhance the reliability of our research.

3.7 Ethical Considerations

In line with the ethical considerations outlined by Oates (2006), this study ensured that all participants were fully informed about the purpose of the research, the use of collected data, and their rights to confidentiality and withdrawal at any point. Informed consent was obtained from all participants prior to the interviews (see Appendix A). Measures were taken to anonymize data and protect participant privacy.

4 Results

In this chapter, we present our findings from each interview respondent according to the identified dimensions from chapter 2.

4.1 Technology

R1 notes that their company does not utilize pure AI solutions for their cybersecurity strategy, however, R1 mentions that they employ anti-malware software that autonomously shuts down sessions based on identified anomalies. This is not a pure AI implementation but R1 suggests it involves some form of automated learning and logic.

> *R1, "[...] we don't use a pure AI solution, however, we do use things like anti-malware software and so on which in its own way can shut down sessions on servers and workstations based on identifying abnormal processes and so forth on the devices [...] it's not pure AI, but it is still a form of learning and, what should I say? Logic and some form of knowledge in these services. So, that is probably what I would say we use today that is most connected to an AI concept." (Appendix C, #10)*

R1 describes an interest in exploring AI for monitoring systems like SOC (Security Operations Center), to simulate attack scenarios.

> *R1, "So it might also be an opportunity for AI going forward that as a company you can have an AI that constantly simulates various types of attacks on your environment and then you can gradually close the vulnerabilities that you have." (Appendix C, #14)*

R1 underscores the complexity of data models as a challenge in implementing AI, that the data model and system architecture need support for an AI implementation. R1 argues that the AI performance could be dependent on the structure for how data is organized and risk sorted.

> *R1, "I'm thinking mainly of the data model then, in many companies it can be very scattered, so to speak. There can be many systems, the architecture around the systems and how the entire infrastructure is built. [...] the data model can indeed be a challenge to really find a good basic structure for how data is organized and risk-classified so that AI can work efficiently and based on risk [...]" (Appendix C, #17)*

R2 says that they don't have their own AI-driven cybersecurity, however, R2 notes that their third-party provider AWS may use AI for different services, for example, their global anti-DDoS.

> *R2, "I guess that AWS, Amazon's cloud service [...] perhaps their global anti-DDoS mechanisms and such, should be using anomaly detection in some way. [...] But we don't have anything that we ourselves have actively activated." (Appendix D, #12)*

R2 mentions that they have mostly modernized their IT-infrastructure. R2 argues that their IT-infrastructure would not be an obstacle for further AI implementation. If AWS releases a new service, they can simply activate it.

> *R2, "Now we are beginning to establish a more modern foundation in our systems. We also have some legacy parts that we are phasing out. But it is still the case that we don't have any physical servers of our own. If AWS now can offer a service that we feel is cost-effective and adds something, then we could probably activate it. I don't think we have a barrier in that sense." (Appendix D, #19)*

R3 have an extensive use of AI in their cybersecurity systems. R3 explains that AI is used for their EDR (Endpoint Detection and Response) system.

> *R3, "I would say that to a very large extent it is used in what we call the EDR (Endpoint Detection and Response) platform that we have. So a lot of different types of telemetry end up in this security platform, which then contains the types of mechanisms you referred to." (Appendix E, #10)*

R3 explains that there can be issues with compatibility between systems from different IT providers.

> *R3, "Sometimes it can happen that we wanted to standardize on a certain set of tools, and then it partially conflicted with what one of our subcontractors had already decided to have in their platform." (Appendix E, #14)*

R4 mentions that their company does not currently use AI within their cybersecurity but that they see potential for it when it comes to analysing logs from their upcoming SIEM.

> *R4, "[...] we are in the process of implementing something called SIEM, where we can set up certain rules. We log a lot of information, and we don't have a team actively digging into these logs. But if you set up rules in a SIEM system, you can find out when you should start looking at the logs. And artificial intelligence could definitely play a part in it by learning what is normal and what is abnormal, both from our logs and from the central system." (Appendix F, #9)*

R4 argues that their company is well-prepared in terms of IT infrastructure, utilizing centralized systems through Azure and not maintaining any physical data centers, which positions them well for integrating AI in the future.

> *R4, "We have a very well-organized IT department [...] everything is centralized through Azure and we don't have our own data center, everything is in the cloud. So, we have a very good infrastructure to build upon." (Appendix F, #13)*

4.1.1 Preliminary Analysis

R1:

- Uses anti-malware software with autonomous features to shut down sessions based on anomalies; not pure AI but incorporates some automated logic.
- Expresses interest in exploring AI to enhance monitoring systems like SOC for simulating attack scenarios.
- Points out the complexity of data models and the necessity for a structured system architecture to effectively implement AI, emphasizing the dependence of AI performance on proper data organization and risk classification.

R2:

- Does not have in-house AI-driven cybersecurity but utilizes AI services from AWS, such as global anti-DDoS.
- Notes that their modernized IT infrastructure would support further AI integration, and that they could activate new AI services as they become available from AWS.

R3:

- Extensively uses AI in their EDR system, indicating a significant integration of AI in their current cybersecurity operations.
- Discusses potential compatibility issues with systems from different IT providers, which could hinder seamless integration of standardized tools.

R4:

- Currently does not use AI within their cybersecurity but is considering its potential, especially for analyzing logs in their upcoming SIEM system.
- Highlights that their well-organized IT infrastructure, centralized through Azure and cloud-based, is well-prepared for future AI integration.

4.2 Organization

R1 explains a lack of visibility on the benefits of AI. However, R1 acknowledges that the benefits will likely become more apparent as AI is identified and utilized across various operations and companies.

> *R1, "[...] the concept is a bit difficult and vague to grasp. I have a little challenge in seeing what the actual benefit of this technology will be moving forward. But of course, it will probably be identified in various types of operations and companies [...]" (Appendix C, #4)*

R1 states the importance of having a strong foundational understanding and implementation of basic information security measures before integrating AI into cybersecurity efforts.

> *R1, "You still have to start with these basic information security building blocks and create your foundation for future AI so that you focus on the right risks and threats with the software you are going to implement." (Appendix C, #12)*

R1 continues with emphasising the importance of having a solid foundation and solid basic security culture before even starting to implement AI. R1 also underscores that importance of knowledge throughout the company.

> *R1, "Once again, I believe it's more about establishing this basic security culture and then subsequently starting to look at, like, technical solutions that can further strengthen the culture. [...] I think that training would be needed at all levels in the company, both our company and all other companies as well. We work with awareness when it comes to security [...]" (Appendix C, #23)*

R1 continues with arguing that risk analysis, incorporated into the IT strategy, is vital.

> *R1, "[...] Then you need to find a strategy for AI to navigate through, I think. But above all, it's about risk analysis and continuously working with the risks [...]" (Appendix C, #17)*

Additionally, R1 highlights the problems that come with changes in the organization.

> *R1, "Then the challenge for the operation becomes, well, how are we going to handle it when there is a change? How are we going to manage it in our daily processes and so forth?" (Appendix C, #27)*

R1 discusses the balance between the benefits and challenges of AI and digitalization in businesses. They acknowledge the potential threat to certain jobs and services but emphasize the importance of developing a strategy to effectively implement these technologies while maximizing benefits and minimizing negative impacts.

> *R1, "[...] there's a balance in that somewhere, you know. When talking about AI and digitalization, it can be perceived as a threat in many businesses, because it can mean that certain roles disappear and so on. So, it's important to find a strategy for how to package and sell that within an organization." (Appendix C, #21)*

R1 continues with emphasizing balance in managing business interests alongside digitalization efforts. R1 stress the importance of evolving business models with new digital offerings while also considering security measures. R1 believes finding the right balance between investing in security and fostering business growth is crucial, but challenging.

> *R1, "[...] there's always a balance in that, you know, somewhere there's also a business aspect in companies. You need to develop your business model with new services, new digital products, and so on. So, security needs to be somewhere there too, it shouldn't hinder the business but there's a balance in that, like where you invest and how you focus your resources, so it's also a difficult balance in some cases." (Appendix C, #31)*

R2 explains that they don't have a role responsible for security in the company. R2 also argues that it's more financially feasible to hire a person who thinks user interface design is more interesting as opposed to security. R2 suggests that they would probably be further in the cybersecurity process if they had security responsible.

> *R2, "We don't have a specific role for a security officer here, but it's something that we somehow share according to the level of interest." (Appendix D, #3)*

> *R2, "It's easy to choose someone who might not find security the most exciting, and instead pick someone who enjoys working with, for example, user interfaces. That gives us more bang for our buck. If we had someone who was very interested in security, we would probably be further along in these thoughts and in the process." (Appendix D, #20)*

R2 highlights that within their organization, there's a general lack of familiarity with AI in cybersecurity. Furthermore, there's currently minimal interest from management in integrating AI into their cybersecurity strategy.

> *R2, "We don't have a great handle on these things, or perhaps, especially, there isn't much interest in driving it forward. There isn't a specific interest from the management to pull those strings yet, it should be noted. But as I said, maybe it will become hotter." (Appendix D, #24)*

R3 highlights the limitations of relying solely on technology for security. R3 emphasize that while purchasing security services provides a basic level of protection, it's essential for organizations to have the capability to act upon security threats. This involves not only implementing security measures but also monitoring and responding to potential threats effectively.

> *R3, "[…] just because you have technologies in place, and this is in the form of us buying these services from service providers, it only provides a basic level of protection. Sure, you get out-of-the-box protection, and these will always stop some things. The next step one must take from an organizational perspective is to have the ability to act on this as well. So there are always two sides to this. One is being able to measure sensible things and ensure that these types of agents and others are installed in the right places. Then this must be monitored, and there must be people in place to act on it." (Appendix E, #14)*

R3 points out that being part of a large organization has its advantages and disadvantages. While they have the financial resources to implement projects, they also face challenges due to bureaucratic processes, which often slow down decision-making and implementation timelines.

> *R3, "Company X is quite a large company. We have leverage in being large. Perhaps we have budgetary space to make these types of investments. Protecting our information, our IP, our customers' information. In that sense, it's an advantage to be large. One disadvantage might be that decision-making processes are a bit more difficult, budgeting and all that also take longer in a larger company." (Appendix E, #16)*

R3 further mentions that while the management generally views AI in a positive light, R3 doesn't believe that cybersecurity is specifically on their radar when discussing AI; rather, the management focus on AI as a broader technology.

> *R3, "I think our leadership, X, who is the CEO, has talked about how he views AI and the opportunities it presents for a knowledge company like Company X, to benefit from it in various ways. However, I don't believe X is really considering how we can leverage AI within the cybersecurity domain." (Appendix E, #18)*

R4 highlights that their company's most valuable asset, besides their employees, is customer data. They maintain a cautious stance towards the use of artificial intelligence, particularly in the areas of information security and IT.

> *R4, "[...] our greatest asset, aside from our employees, is data, specifically customer data, which we are of course responsible for securing. [...] we have a very cautious approach to artificial intelligence, at least on the information security and IT sides. We have product managers who are eager to move forward very quickly." (Appendix F, #11)*

R4 states that the interest in integrating AI within their company primarily comes from the product managers.

> *R4, "Yes, it is primarily the product managers who are interested in integration. We have one of our products in the portfolio that uses AI today. It is our chatbot." (Appendix F, #15)*

4.2.1 Preliminary Analysis

R1:

- Acknowledges limited visibility on the benefits of AI but expects these to become more apparent as AI is utilized more broadly.
- Emphasizes the importance of a strong foundational understanding of basic information security before integrating AI into cybersecurity.
- Highlights the necessity of a solid security culture and thorough risk analysis as precursors to AI implementation.
- Discusses the balance required in implementing AI, noting both the potential to displace certain jobs and the need to align AI with business strategies.

R2:

- Lacks a designated security officer; cybersecurity responsibility is shared based on interest.
- Points out a general lack of familiarity and minimal management interest in integrating AI into cybersecurity, which could change as AI becomes a hotter topic.

R3:

- Notes the limitations of relying solely on purchased security services and stresses the need for organizational capability to act on security threats.
- Mentions advantages and disadvantages of being a large organization, such as financial resources for investment versus slow bureaucratic processes.

- Suggests that while management views AI positively, it is not specifically focused on cybersecurity applications.

R4:

- Identifies customer data as the company's most valuable asset and maintains a cautious approach towards using AI in information security.
- Indicates that interest in AI integration primarily comes from product managers, particularly visible in applications like their AI-powered chatbot.

4.3 Environment

R1 explains a concern regarding the use of AI by the attacking side. R1 suggests the increased use of AI will escalate the cyber warfare from both the attacking side and the defending side.

> *R1, "They will also be able to benefit from this technology moving forward, so it will essentially build an escalation on both the defensive side and the attacking side of the cyber threat." (Appendix C, #12)*

R1 argues that the telecom sector is heavily regulated which affects their services. R1 explains that they today must manually analyse the laws for the different markets that they operate in. R1 also highlights that the law landscape is rapidly changing.

> *R1, "I am currently in the telecommunications industry, and there are many different legal provisions and so on that affect our services. [...] There is a manual job that we do today, scanning the markets where we are active for these legal provisions, and then there are always new laws coming into effect. [...] Laws change and so on [...]" (Appendix C, # 27)*

R2 believes that attackers will leverage AI for their cyber operations, leading to a conflict between offensive and defensive forces. However, R2 maintains that AI alone won't resolve every issue, though it will play a supportive role in this struggle. R2 anticipates a competition to see who can most effectively utilize these technologies.

> *R2, "I think that the attack mechanisms will become more sophisticated with the help of AI. There will probably be a little battle between them. I don't believe AI in itself solves the fundamental protections. It can probably help, but I think the hackers will come, it will be a battle over who is the smartest in some way. How to best utilize these mechanisms." (Appendix D, #16)*

R2 argues that competition from other companies does not affect their decision to implement AI-driven cybersecurity (Appendix D, #28). R2 does argue that regulations could affect their decisions if they are put under pressure (Appendix D, #30).

R3 explains that they are aware of the threats that could potentially harm them and that they therefore acknowledge the need for security measures.

> *R3, "We understand that there are different types of threat actors who want to affect us in some way [...] We must have protective mechanisms, and that's where cybersecurity measures of various kinds come into play." (Appendix E, #6)*

R3 also describe that they benchmark themselves in comparison to other companies of similar size in different sectors. Furthermore, R3 brings up a desire for the company to be perceived as just as good or better in this area.

> *R3, "[…] we must also be able to benchmark ourselves in this area and say that we are just as good or better than our competitors […] that we are perceived a proactive partner in relation to our customers […] it also means that we must be able to, so to speak, stand up for having a good cybersecurity posture too. […] even if it might not be something that is highlighted in customer meetings, these kinds of questions about how we handle the cybersecurity area and information security are there, so to speak, you always come to that point in a dialogue with a customer today" (Appendix E, #20)*

R3 argues that there is currently nothing regulatory preventing them from using AI-driven cybersecurity. R3 explains that this is something they have addressed in their process.

> *R3, "Well, we do get into GDPR and so forth, of course, in this context. I have looked at how we express our privacy notice and some other aspects, and yes, in itself, I don't see that we have any, there is nothing that prevents us from using these types of cybersecurity tools and similar given the rules and requirements in this way. We have covered it, I think, in how we communicate, how we use information, metadata, and so forth." (Appendix E, #22)*

> *R3, "And there we could just confirm that we had already prepared everything correctly, so we could just check it off and see that there were no obstacles to proceeding with this implementation." (Appendix E, #26)*

R3 explains that they used to have a product that they were not very satisfied with due to several issues. It had many technical lifecycle-oriented problems and significant maintenance issues. It was more of a traditional antivirus solution with limited capabilities which did not meet their current needs.

> *R3, "We had a product before that we were not very pleased with. It had a lot of technical lifecycle-oriented problems. There were many maintenance issues with it, and it was not modern; it was not part of an EDR concept, it was more of a traditional antivirus solution with some capabilities to run SIEM and similar things, but it was nowhere near what we decided to purchase" (Appendix E, #24)*

R3 suggests that the societal development in this area is putting more pressure on the organizations to mature regarding cybersecurity.

> *R3, "[…] it is becoming clearer who the threat actors and others are, which really puts more pressure on everyone to move and become more and more mature in this area. What we see today is just the beginning." (Appendix E, #30)*

Furthermore, R3 emphasizes the importance of having the right supplier. R3 suggests that it is necessary to have suppliers that can deliver in this area.

> *R3, "I believe that it's important for companies in general to choose the right partners in this area. So that they choose partners who have both visions and the ability to deliver on those visions." (Appendix E, #30)*

R4 acknowledges the constant threat of cyberattacks, stating that it's not a question of if, but when an attack will occur. They highlight that customers who maintain on-premise servers are more vulnerable. R4 argues that the goal is to minimize the risk for customers, attributing any potential issues to their own system upkeep rather than shortcomings on their end.

> *R4, "No, not really. I mean, we're constantly exposed to attacks like any other company. [...] It's always a matter of time, not a matter of if but a matter of when something happens [...] What we see above all is that our customers who don't migrate to the cloud but choose to run their own servers on-premise are the ones mainly affected by attacks. What we can do, of course, is make sure that we spend a lot of time ensuring that, both in the development of our product so it doesn't fall behind and become the cause, but also that we have secure configurations when setting up integrations with other systems so that, knock on wood, if or when a customer faces something, it's because either they haven't updated their systems and it's not because of us." (Appendix F, #21)*

R4 reflects on the dual nature of AI in cybersecurity. R4 highlight the ethical and unethical applications of AI, emphasizing its potential to strengthen organizational security or be exploited by malicious actors.

> *R4, "As I mentioned before, it's a double-edged sword [...] Let's take an example. We currently undergo penetration tests on our products. Such a penetration test can provide a very good picture of where the product stands or where the organization stands. But it also assumes that the pentesters are at least as skilled as the attackers. If you have a junior pentester, you can get a lot of value from a junior pentester. But it will never perform better than a senior attacker. Similarly, I mean that AI can be used both ethically and unethically. You can use AI to strengthen your position and protect the organization and its data. But in the same way, attackers can exploit it." (Appendix F, #29)*

R4 acknowledges the presence of strong competitors and the risk of falling behind if not quick to adopt new technologies like AI. However, R4 also emphasizes that their decision to integrate AI is not merely influenced by competition but is primarily driven by customer needs.

> *R4, "[...] we have very sharp competitors [...] The risk is that if we are not quick on the uptake, we may fall behind the competition." (Appendix F, #15)*

> *R4, "One could say both yes and no. Absolutely, we look at what, for example, X or X does. But ultimately, it is primarily the customer perspective that guides us. Just throwing in AI for the sake of it is something we would not do. [...] So, if we see that AI can satisfy or meet a need that our customers have, then we are more inclined to do it [...]" (Appendix F, #17)*

R4 emphasizes the importance of adhering to legal requirements in their AI implementation strategy. They highlight the need for caution to ensure compliance with GDPR and the AI regulation and to avoid adopting technologies prematurely.

> *R4, "But it is also a balancing act to meet legal requirements set by the AI regulation, ensuring that we do not adopt anything for which we are not 100% ready." (Appendix F, #15)*

> *R4, "GDPR is still very much a part of our daily operations and is of utmost importance to comply with, ensuring that no risks are taken in this area. It will be a part of any strategic decision about implementing AI, and must be considered. Also, the AI Act regulation by the EU needs to be taken into account. I must say that I am not personally handling this, it is our legal counsel who is delving into it." (Appendix F, #19)*

4.3.1 Preliminary Analysis

R1:

- Expresses concern about AI being used by attackers, predicting an escalation in cyber warfare on both offensive and defensive fronts.
- Highlights the heavy regulation in the telecommunications sector, which affects their services and necessitates ongoing legal compliance efforts.

R2:

- Believes attackers will leverage AI to sophisticate their operations, creating a battle of technological prowess between attackers and defenders.
- Views AI as supportive in cybersecurity but not a complete solution, emphasizing the need for strategic utilization.
- States that competition does not influence their AI adoption, but regulatory pressures might.

R3:

- Acknowledges the constant threat from various types of attackers and stresses the need for effective cybersecurity measures.
- Discusses the advantages of benchmarking against other companies to ensure they are perceived as proactive and secure by customers.
- Suggests that current regulations do not prevent the use of AI-driven tools in their operations.
- Emphasizes choosing the right suppliers to meet cybersecurity needs and expectations.

R4:

- Notes the inevitability of cyberattacks and the increased risk for customers with on-premise servers.
- Reflects on the dual nature of AI in cybersecurity, pointing out its potential to both enhance security and be exploited by attackers.

- Asserts that their AI adoption decisions are driven by customer needs rather than just competitive pressure.
- Stresses the importance of adhering to legal standards, including GDPR and upcoming AI regulations, to ensure responsible AI implementation.

4.4 Cyber Catalysts

R1 highlights that the focus of their work revolves around managing risks, with a structured approach based on different scenarios and focus areas at a higher level. Their risk-based strategy primarily addresses the major contemporary threats, notably ransomware, which is one of their key areas of concern.

> *R1, "[…] we are constantly working with risk, […] where we have various scenarios and focus areas that we work on at a higher level. […] ransomware especially, which is one of our focus areas. Then it also involves other types of what should I say, risk related to data leakage and so […] the big thing is usually finding strategies to handle a ransomware threat, which can particularly impact the availability of services, but also data leakage. So, we do this through our risk management work." (Appendix C, #29)*

R1 suggests that external events, such as attacks on companies in other or similar industries, drives further investment in new technology.

> *R1, " […] there are external events that we see in our environment, like similar attacks on major IT providers or companies in other or similar industries, and so on. This also drives a focus on further investing in new technology and new threat management." (Appendix C, #31)*

R2 says they did experience a significant exploit a few years ago, which heightened their awareness and focus on security. This incident led to the implementation of new routines for better integration of security measures. R2 acknowledges the potential benefits of an AI-based service, which could enhance their ability to detect attacks more quickly.

> *R2, " […] we were affected by an exploit a couple of years ago, which definitely made us pay more attention to security. But it has rather involved implementing different types of routines […] However, it is quite possible that an AI-based service could help us detect an attack faster as well. " (Appendix D, # 32)*

R3 notes that artificial intelligence has recently become a hot topic, especially with the surge in generative AI and developments like ChatGPT over the last few years. R3 mention that machine learning and related technologies have been around for many years, often operating behind the scenes. R3 argues this has contributed to the hype around AI, which is increasingly becoming a common component in virtually all IT-related environments.

> *R3, "[…] the whole story with generative AI and so on with ChatGPT and that type of packaging or development that has occurred in the last few years here has just been an explosion. Then there is the fact that machine learning and these kinds of phenomena that are found everywhere have been around for many years*

> *behind the scenes, so it is a hype and then it is something that becomes more and more prevalent in essentially everything that we do, everywhere where there is IT there is some type of such component in the background [...]" (Appendix E, #4)*

R3 explains that the decision-making process about investing more in cybersecurity likely coincided with or occurred shortly before the onset of the COVID-19 pandemic. The pandemic served as a catalyst, prompting further investment.

> *R3, "[...] we made these decisions, which must have been around the time or just before the COVID-19 pandemic started. COVID-19 perhaps became a trigger for us to actually invest more in this area. Everyone at the company went home and started working remotely, and because of this, we had less visibility into what was happening with all our endpoints. At the same time, there was a concern that threat actors and others would increase their activity because of this." (Appendix E, #14)*

> *R3, "I mentioned a catalyst that faced us with a choice: whether to step in and buy a product suite or not. Then COVID came along and we decided to purchase this EDR product, covering all our endpoints [...] So, I would say that COVID was perhaps a catalyst, maybe that was a good word, that really made us, well, press the order button here." (Appendix E, #24)*

R4 argues that specific cyber-attacks on other companies is not something that drives development in their cybersecurity strategy. R4 explains that it's a part of their day-to-day.

> *R4, "No, not really. Being ISO-certified or having an ISMS involves continuous improvement, something we live every day, it's a living part. It's not like we see something happening and then we have to wake up, it's something we do all the time. [...] If you're ISO-certified, you already have certain things in place, such as a disaster recovery plan, a continuity plan in case things go wrong. The key question there is to revise it to ensure it's still up-to-date in its current form." (Appendix F, #23)*

4.4.1 Preliminary Analysis

R1:

- Emphasizes a structured, risk-based strategy primarily focused on addressing major threats like ransomware and data leakage.
- Suggests that external events such as attacks on similar industries drive the adoption of new technologies and enhance threat management strategies.

R2:

- Experienced a significant security exploit that heightened their focus on security and led to the implementation of new security routines.
- Recognizes the potential benefits of AI-based services in detecting attacks more swiftly, indicating a shift towards more proactive measures.

R3:

- Notes the rise in popularity and integration of generative AI, like ChatGPT, and machine learning in IT, attributing some of the hype to their long-standing presence behind the scenes.
- Describes how the COVID-19 pandemic acted as a catalyst for significant investment in cybersecurity, particularly in enhancing remote work security through products like EDR.

R4:

- Argues that specific attacks on other companies do not drive their cybersecurity strategy; rather, being ISO-certified involves ongoing improvements and preparedness.
- Maintains a consistent approach to cybersecurity, emphasizing the importance of regular updates to disaster recovery and continuity plans to remain resilient against threats.

4.5 Practice Standards

R1 explains that they have not looked into standards regarding AI as they are not at that stage yet. However, R1 brings light to considerations for ethical rules and strategic rules for an eventual implementation in the future.

> *R1, "We are not yet at the point where we consider it an option in our daily operations. But when it comes to that question in the future, one will need to look at managing your AI solution so that you don't rely on it too much. It is, after all, a matter where you need to ensure that your AI solution not only follows the ethical rules of society but also our specific strategic rules [...]" (Appendix C, #33)*

As for ethical considerations, R3 says that this was not a primary focus. R4 explains that it is not something he is responsible for, however, R4 argues that it is part of their code of conduct.

> *R3, "We didn't really have many ethical discussions in that way; instead, we focused on GDPR aspects." (Appendix C, #26)*

> *R4, "Not really what I deal with, to be honest. Ethics is a big part of our corporate culture [...]" (Appendix F, #25)*

> *R4, "It's not part of a risk analysis, but it's sort of our code of conduct. We have policies that regulate it." (Appendix F, #27)*

R3 anticipates potential impacts from future regulatory changes like the frameworks NIS2 and DORA, which might indirectly affect their company even if they are not the primary target of the legislation.

> *R3, "[...] we might be affected in the long run by regulatory changes that come in, for example, NIS2 and DORA and similar frameworks, even though we may not be the primary targets [...]" (Appendix E, #22)*

4.5.1 Preliminary Analysis

R1:

- Has not yet explored standards related to AI as it is not currently a part of their operations.
- Highlights the future need to integrate ethical and strategic rules into their AI solutions, emphasizing the importance of not overly relying on AI and ensuring compliance with both societal ethical norms and specific strategic objectives.

R3:

- Indicates that ethical considerations were not a primary focus, with more attention given to GDPR compliance.
- Expresses awareness of potential future impacts from regulatory changes like NIS2 and DORA, suggesting a need to stay prepared for how these frameworks could affect their operations indirectly.

R4:

- Mentions that ethical considerations are not a direct responsibility but are embedded in the company's code of conduct.
- Describes ethics as an integral part of corporate culture, regulated through existing policies rather than specific risk analysis procedures.

4.6 Additional Findings

Furthermore, R1 underscores that the AI will become a valuable asset prone to cyber-attacks which could be troublesome if it gets hacked. R3 and R4 also suggests AI as a security risk.

> *R1, "But it can also pose threats because, you see, AI will also become a very valuable asset that you must protect. If it gets hacked, for example, it could cause a lot of trouble in an operation." (Appendix C, #21)*

> *R3, "Then the question is how much autonomy you want to give this type of solution. It might eventually decide something and shut everything down for us. We don't want that to happen either. That it becomes a security threat in the end." (Appendix E, #28)*

> *R4, "Most recently, when we conducted management reviews, we discussed and reviewed internal and external risks, and we see AI as an internal risk for the organization [...]" (Appendix F, #15)*

R2 argues that there's a low interest in cybersecurity and that they therefore don't have the knowledge about what tools are available.

> *R2, "But no one really finds the stuff super exciting. So, it also means that we don't have a great understanding of what tools are available. [...] More options are starting to emerge that we can look into." (Appendix D, #20)*

4.6.1 Preliminary Analysis

R1:

- Points out that AI, while a valuable asset, could pose significant risks if compromised, emphasizing the potential for serious operational disruptions if AI systems are hacked.

R2:

- Notes a general lack of enthusiasm and understanding within their organization regarding AI in cybersecurity, suggesting a gap in knowledge about available AI tools and emerging options.

R3:

- Raises concerns about the level of autonomy granted to AI systems, cautioning against allowing AI to make autonomous decisions that could inadvertently shut down operations or become a security liability.

R4:

- Acknowledges AI as an internal risk during management reviews, indicating a proactive approach to identifying and mitigating the risks associated with AI within the organization.

5 Discussion

In this chapter, we discuss the findings from the previous chapter and draw comparisons to the theoretical background from chapter 2.

5.1 Technology

In the Extended TOE framework, technology is a crucial factor that includes the current technological solutions available, IT infrastructure, and IT personnel affecting the adoption decision (Wallace et al. 2020). Wallace et al. (2020), AL-Dosari et al. (2024), and Merhi (2023) can all see that the technological readiness which includes hardware infrastructure, software infrastructure and integration complexity, as important in the decision to implement. They all emphasize the need for a robust IT infrastructure and they highlight the complexities involved in integrating new technologies within existing systems.

R2 and R4 argue that their IT infrastructure does not pose a significant barrier to AI implementation (Appendix D, #19; Appendix F, #13). R2 discusses their modern IT infrastructure that can integrate new services provided by AWS which suggests a technological readiness to implement AI-driven solutions as they become available. Similarly, R4 mentions that their centralized systems through Azure offers a solid base for future AI integration which also underscores the readiness and strategic positioning for adopting new technologies. These findings align with Merhi (2023) and Wallace et al. (2020) who argue that adequate IT infrastructure is a prerequisite for a successful implementation. The readiness described by R2 and R4 supports the claim that infrastructure readiness influences implementation decisions.

As mentioned by R1, the complexity of data models and system architectures presents a significant challenge (Appendix C, #17). R1 highlights the scattered nature of data and the need for a structure to efficiently implement AI. This issue aligns with the concerns raised by AL-Dosari et al. (2024) about the difficulty in converting legacy systems and the integration complexity of AI technologies.

Moreover, R3 notes compatibility issues with systems from different IT providers which complicates the standardized application of tools across platforms (Appendix E, #14). This shows a practical example of the integration complexity which Merhi (2023) has brought up and it supports the theory that the technological dimension involves not only the availability of AI-driven solutions but also the capability to integrate these solutions into existing infrastructure.

Companies with ready and modern IT infrastructures appear well-positioned to integrate AI-driven cybersecurity solutions. However, challenges related to integration complexities and legacy system conversions are real obstacles that companies must navigate which validates concerns noted by AL-Dosari et al. (2024) and Merhi (2023).

5.2 Organization

The Extended TOE framework identifies organizational factors like organizational structure, personnel, culture and size in the adoption of cybersecurity (Wallace et al. 2020). AL-Dosari et al. (2024) and Wallace et al. (2020) have seen organizational challenges like skilled personnel, implementation plan as well as the top management's commitment. Furthermore, Merhi (2023) have seen the lack of visibility on benefits and the impact of organizational changes.

R1 discusses the challenge in seeing the benefits of AI (Appendix C, #4). This aligns with the observation by Merhi (2023) about the lack of visibility on benefits and its impact on AI adoption. Furthermore, R1 highlights a concern over change in the organization regarding how they will manage the new technology in their daily processes. This aligns with the findings from Merhi (2023) on the impact of organizational changes.

R1 highlights the fact that first of all the organization must lay down a foundation of basic security culture and knowledge before integrating AI into the cybersecurity systems (Appendix C, #23). R4 convey a reserved and pragmatic attitude towards AI which is an organizational strategy that focuses on managing risks before embracing aggressive technology adoption. Thus, it is in line with the assertion of Merhi (2023) and Hasani et al. (2023), who both argue that a company's culture is critical in the decision making process. Among other things, R1 also highlights the necessity of risk analysis and alertness to security risks. This emphasizes the fact that the level of organizational preparedness in terms of understanding and managing the risks is the key to the successful AI implementation.

R2 says that they don't have any particular role as security in their company and they fill positions based on other interests. This is an issue that is related to the organizational structure and a lack of skilled employees. Additionally, R2 indicates that there is a weak push from management in terms of cybersecurity investments. R3 notes that while management side is positive about AI it is not evident that there is a specific attention towards utilizing AI in cybersecurity. This supports Merhi (2023) who states that the management's commitment is one of the vital factors in adoption.

R3 discusses the advantages and disadvantages of being a large organization, noting that while financial resources are available, bureaucratic processes can slow down decision-making and implementation (Appendix E, #16). This shows that organizational size influences adoption with larger organizations possibly facing more complex internal processes that could delay or complicate technology integration.

5.3 Environment

The Extended TOE framework shows that external environmental forces like suppliers, competitors and government regulations significantly influence cyber adoption decisions (Wallace et al. 2020).

With regards to R1 and R4, it is clear that government regulations play a critical role in the decision-making process of AI adoption for cyber security. R1 showed the weight of the compliance procedures in the telecommunications sector, indicating the time-consuming process of going through the complicated legal system which is very frequently changing. This is similar to the difficulties of regulations like GDPR and CCPA which may restrict the implementation of AI as was observed by AL-Dosari et al. (2024). The fear of regulations is also mentioned by Wallace et al. (2020) who believe that GDPR is an additional factor that makes cybersecurity adoption difficult. This reinforces the notion that although regulations are intended to guarantee data protection and privacy, they may also hinder the quick adoption of AI technologies.

In terms of market competition, the findings illustrate a rather complex picture. R2 argues that competition from other companies does not play a role in their decision to implement AI in cybersecurity (Appendix D, #28), while R3 states that they set the standards for themselves in relation to the competitors (Appendix E, #20). Moreover, R4 is ambivalent, that is, they claim there is a risk of losing the ground while at the same time it is a matter of their particular needs (Appendix F, #15; Appendix F, #17). This diverse attitude about competition's effect demonstrates a difference from the findings reported by Hasani et al. (2023) where competition was a significant factor. It aligns well with the findings from Wallace et al. (2020) who suggests that it varies heavily. This implies, therefore, that the impact of competition might not be uniform among different sectors and individual organizational strategies.

Regarding the matter of supplier support, R3 highlights the necessity of choosing reliable partners who are competent to provide the required cybersecurity services. This goes along with the findings of Merhi (2023) and Wallace et al. (2020) who, in turn, both found supplier support as a significant but variably perceived factor. The importance of supplier selection and support is demonstrated by the fact that the implementation of AI-driven cybersecurity systems is highly dependent on the reliable and technologically advanced suppliers.

A common aspect discussed by the respondents was that they think AI in cybersecurity could be a double-edged sword. The insights from respondents such as R4 and R1 emphasize the dual nature of AI in cybersecurity, illustrating how it can be used both to enhance security and to facilitate attacks (Appendix C, #12; Appendix F, #29). R2 points to an emerging arms race in cyber security, where both attackers and defenders compete to leverage AI most effectively (Appendix D, #16), highlighting AI's role not just as a tool but as a potential battleground. The concern is that while AI can automate and improve defense mechanisms, it also elevates the risks and sophistication of attacks, possibly leading to an escalation in cyber conflicts.

5.4 Cyber Catalysts

The empirical findings correspond well with the extension of Cyber Catalysts as proposed by Wallace et al. (2020), in the Extended TOE framework, which shows factors beyond the traditional aspects that affect cybersecurity adoption. This dimension captures the complicated nature of cyber threats that involve cyber vulnerability, privacy issues, and cyber risk management. These catalysts do not only affect the organizational security policies but also they influence the strategic decisions in adopting and investing in cybersecurity tools.

R1 and R2 give concrete illustrations of the ways in which cyber vulnerabilities affect the strategies of the companies. R1 applies a risk-based approach that is organized around the most prevalent risks in the area such as ransomware, which includes scenario planning and specialized focus areas. This approach clearly demonstrates the importance of the recognition and management of vulnerabilities which is one of the key issues as explained by Wallace et al. (2020). Likewise, R2's story of an exploit demonstrates the organization's heightened awareness and following security routines adjustments, which is a practical example of cybersecurity precautionary measures taken in response to vulnerabilities.

External events in particular can be a major factor in the adoption of cybersecurity measures, as explained by R1 and R3. R1 stated that the attacks on other organizations encourage for more investments in technology and threat management (Appendix C, #31), which is in line with Wallace et al. (2020) opinion that the external cyber threats can stimulate proactive organizational responses. R3's narrative continues this conversation, declaring how the COVID-19 pandemic was a trigger for cybersecurity investment that increased because of the new vulnerabilities that arose from remote work and the heightened cyber activities during the pandemic (Appendix E, #14).

R4's perspective stresses that upkeep and standard compliance are key elements of cybersecurity. This respondent gives an example that for some companies, cybersecurity is not just a response to a particular event but it is an ongoing process and a part of the operational day-to-day. This route also aligns with the viewpoint of Wallace et al. (2020) that managing cyber risk is a critical part of strategic planning, which requires regular updates and revisions to be relevant and effective.

5.5 Practice Standards

In the Extended TOE framework, Wallace et al. (2020) proposed the dimension of Practice Standards and they especially emphasized the legal and ethical factors as the central themes within this dimension. Taken together, these factors contribute to the way organizations approach the adoption of new technologies in general and cybersecurity strategies in particular.

Our respondents manifests a mixed approach to legal factors. Wallace et al. (2020) suggests that compliance with the law is not just the act of adhering to laws but studying how the legal frameworks can be applied to minimize the impacts of cybersecurity breach. However, the respondents themselves do not specifically discuss their existing legal frameworks dealing with AI. Nevertheless, anticipation by R3 of the emergence of such future regulations like NIS2 and DORA (Appendix E, #22) is an indication of their awareness and of a forward-looking approach that is in line with the emphasis that Wallace et al. (2020) places on legal readiness as a major factor in cybersecurity adoption.

As for the ethical considerations, Wallace et al. (2020) stress that following the ethical principles is not only vital for the sound decision-making process but also for the reputation of the company and the trust of the stakeholders. Our results, however, show a variety of views on ethics. R1 points out that ethical and strategic rules can be incorporated into AI solutions in the future (Appendix C, #33), demonstrating an understanding that ethical issues should be taken into account in strategic planning. R4, although not directly responsible for ethical supervision, still points out that ethics is deeply rooted in the corporate culture and code of conduct (Appendix F, #25; Appendix F, #27). This gap in the direct involvement with ethical issues indicates that although ethical issues are recognized, they may not be the first in line of operational decisions but are incorporated into the overall corporate practices.

Overall it can be seen that the respondents believe in the importance of the practice standards in theory but the practical application and focus on these standards differ among them. Companies can be seen to be in different phases of focus and preparedness regarding legal and ethical issues.

5.6 Additional Findings

Our findings emphasize that the perceived risks of AI technologies being considered as both valuable but also at risk of being exploited within organizations is important. These concerns are highlighted by respondents R1, R3, and R4 who, collectively, point out that although AI brings undeniable benefits, also it has a potential to introduce serious security risks.

R1 effectively emphasizes the two-sidedness of AI as an asset and threat, underlining how drastic the operational disruptions could be in case of a system breach (Appendix C, #21). This is the idea of R3 who is worried about the extent to which AI systems can be autonomous and he thinks that the AI systems can make decisions that are independent and not necessary for the safety of the organization or can become a threat (Appendix E, #28). R4 also stresses AI as an internal risk to be reviewed during management reviews, highlighting the possible negative impact of the AI on the organization (Appendix F, #15).

5.7 The Extended TOE Framework

Although the Extended TOE Framework by Wallace et al. (2020) is very comprehensive and covers different aspects of cyber security adoption, we think that it has some difficulties due to overlapping dimensions. These overlapping characteristics muddled the categorization of data and made it difficult to separate specific factors for one category without acknowledging their role in another. This matter not only adds complication to the analytical process but also raises a doubt about the framework's clarity and practical application.

For instance, the overlap between Legal in Practice Standards and Government Regulations in Environment means that data related to legal compliance could ambiguously fit into either category. This made it challenging to distinctly analyze how internal compliance efforts are influenced by external legal pressures or vice versa. Similarly, distinguishing between Tech Provider in Technology and Suppliers in Environment can be perplexing because both address the influence of external entities on organizational technology strategies, yet they are meant to be analyzed separately.

The most significant overlap occurs between Cyber Attacks and Cyber Threats in Environment and Cyber Risk and Cyber Vulnerability in Cyber Catalysts. Here, the external threats and internal readiness to address these threats are closely intertwined. This overlap made it difficult to separate the analysis of external cyber threats from internal risk management strategies.

This overlapping made the data categorization and analysis trickier and it may cause confusion in distinguishing the variables between technological readiness, organizational strategies or environmental pressures. This can cause the framework to lose its value and may require an addition of the layers of interpretation or adjustment of the framework.

Nevertheless, although the Extended TOE Framework has been designed to be a general model for understanding the adoption of cyber security, the overlapping dimensions of cyber security adoption could be made more clear or more integrated approach of categorization. Wallace et al. (2020) does highlight that the dimensions can affect each other, however, we believe it would still benefit from more clarity regarding certain factors and dimensions.

6 Conclusion

In this chapter, we present our conclusion to the research question, Furthermore, we highlight the theoretical and practical contributions of the thesis. Additionally, we discuss the shortcomings of our thesis and give recommendations for future research.

6.1 Conclusion

The aim of this study was to examine how decision influencers in big Swedish companies consider the implementation of AI-driven cybersecurity. The results show a picture that is mixed as to the level of adoption and perception of AI's role in improving cybersecurity.

Overall, the maturity level regarding AI in cybersecurity seems to be quite low in the companies we interviewed. However, the findings indicate a gradual but increasing acceptance of AI-driven solutions. While there is an interest in this solution, it is balanced by the complexity of the process of integrating AI with the current data models and IT infrastructure. R1's and R4's discussions clearly indicate that there is a big need for a strong and well-built IT infrastructure to achieve AI capabilities fully.

Furthermore, the results underpin the importance of the cybersecurity fundamentals. R1 and other respondents emphasize a point that the company should first ensure that the basic security and awareness is there before an eventual AI integration. This was also repeated by R2 who mentioned that they do not have much or no AI usage at present, but they do acknowledge the fact that AI can make their security measures better if the foundational building blocks are in place.

Moreover, the interviews revealed a complex perspective on AI's possible risks and advantages. R3 and R4 made the point that AI can enhance and strengthen cybersecurity methods, but they also expressed a visible concern about how AI technologies can be exploited, either by hacking or internal risks within the organization. This duality hence implies that a careful approach to AI adoption is needed, which involves strategic planning and risk management.

Lastly, there is no doubt among the decision influencers that AI can be an effective complement in cybersecurity but the journey to its implementation is complex and has many aspects. It comprises not only the technology adoption but also the major changes in the organizational culture, infrastructure readiness, and strategic risk analysis. Generally, our findings show a rather cautious approach to AI itself which in turn extends to AI in cybersecurity. The way forward for these companies will probably be a balanced approach which addresses all the dimensions simultaneously while gradually shifting to more AI-integrated cybersecurity solutions.

6.2 Contributions

Our bachelor's thesis research contributes to filling a significant research gap regarding the factors that influence the decision-making process for AI implementation in cybersecurity. This study broadens the understanding of how decision influencers in large Swedish companies and organizations consider AI-driven cybersecurity. Our research provides valuable knowledge and insights for companies across various sectors that are considering implementing AI-driven solutions.

6.3 Shortcomings

A shortcoming of this study is related to who we chose to interview. Although our research mainly focused on people in management roles, we also included a senior systems developer in our group of respondents. This choice might have influenced the overall results because the developer's perspectives could differ from those in management. Essentially, having someone from a technical role in the mix might make our findings less clear or less directly applicable to management practices. In the future, choosing only managers as respondents could help to get clearer insights that are more relevant in a decision process focus.

6.4 Future Research

Future research should continue to address the gap in understanding AI-driven cybersecurity, focusing on the decision-making processes within companies. We believe a good future research topic would be for researchers to research how industry-specific factors influence the adoption and effectiveness of AI-driven cybersecurity. For example, this could include comparing different sectors such as finance, healthcare, or manufacturing- sectors we were unable to research due to the timeframe for this bachelor thesis. This could identify unique challenges and shed some light on what the other practices in different sectors would be. Additionally, future studies could replicate and expand our research by deepening and broadening the scope to include more interview subjects, thereby deepening the insight into how AI is considered and implemented across various sectors and organisations.

Appendix A - Consent Form

Title of the Study:

"Fighting AI with AI: A Qualitative Study on Factors Affecting the Implementation of AI-driven Cybersecurity in Large Swedish Companies"

Researchers:

Hendrik von Krusenstierna, Bachelor Student, he6808vo-s@student.lu.se

Tim Brinkhagen, Bachelor Student, ti3538br-s@student.lu.se

Purpose of the Study:

The purpose of this bachelor's thesis research is to explore which factors affect the implementation of AI-driven cybersecurity and how they impact adoption decisions.

Procedures:

You will be asked to participate in a semi-structured interview that will last approximately 30 minutes. The interview will be conducted by Hendrik von Krusenstierna and Tim Brinkhagen. The interview will be recorded for transcription purposes, and the recording will be stored securely and confidentially.

Risks:

There are no known risks associated with participating in this study.

Benefits:

Your participation in this study will provide valuable insights into the factors affecting implementation of AI-driven cybersecurity. This research aims to contribute to the broader knowledge of AI-driven cybersecurity, potentially influencing future cybersecurity decisions.

Confidentiality:

Your participation in this study is strictly voluntary and confidential. All information collected during the study will be kept strictly confidential and will only be used for research purposes. Your name and/or the name of your company will not be exposed.

Voluntary Participation:

Participation in this study is completely voluntary, and you may choose to withdraw your participation at any time. If you choose to withdraw, any information collected up to that point will be destroyed.

Contact Information:

If you have any questions or concerns about this study, you may contact the Researchers at any of their given contact information.

Consent:

By agreeing to participate in this study, you are indicating that you have read and understood the information provided above, and that you voluntarily agree to participate in this study.

Appendix B - Interview Guide

Bakgrund

- Kan du beskriva din roll och dina ansvarsområden inom företaget?
- När du hör termen artificiell intelligens, vad tänker du på då?
- När du hör termen cybersäkerhet, vad tänker du på då?

Vi förklarar vår definition av AI-driven cybersäkerhet

Teknologi

- Använder ni er idag utav AI i cybersäkerhet?
- Hur integreras AI i er cybersäkerhetsstrategi och vilka specifika områden inom cybersäkerhet ser ni störst potential i för AI-användning?
- Berätta om några utmaningar ni stött på när ni anpassar AI-teknologier till er befintliga cybersäkerhetsinfrastruktur och hur ni har överkommit dessa.

Organisation

- Hur påverkar organisationens storlek och struktur era beslut och förmåga att anta AI-drivna cybersäkerhetslösningar?
- Hur ser ledningen på AI inom cybersäkerhet och vilken roll spelar utbildning för att förbereda er personal för dessa teknologier?

Environment

- Hur har marknadskonkurrens påverkat ert beslut att implementera AI i er cybersäkerhetsstrategi?
- Är det några regulatoriska aspekter som påverkat eller kan komma att påverka?

Cyberkatalysatorer

- Kan ni ge exempel på hur specifika cyberhot eller incidenter har fungerat som katalysatorer för innovation inom er cybersäkerhetsstrategi, särskilt med avseende på AI?

Praxis

- Hur balanserar ni juridiska och etiska överväganden i er AI-driven cybersäkerhetspraxis? Finns det några standarder eller riktlinjer ni strävar efter att följa?

Extrafråga

- Vilka är de mest spännande möjligheterna och framstegen ni ser med AI inom cybersäkerhet framåt?

Interview Transcripts Redacted (Appendix C-F)

Appendix G - AI-contribution Statement

AI-tools used: ChatGPT, Whisper

ChatGPT: ChatGPT was utilized to analyse literature (chapter 1 and 2), brainstorm ideas (chapter 1), and to support us with grammar at times (all chapters).

Whisper: We have used Whisper to transcribe our interview recordings for a first draft (Appendix C, D, E, F).

References

AL-Dosari, K., Fetais, M., & Kucukvar, M. (2024). Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. *Cybernetics & Systems*, vol. 55, no. 2, pp.302-330, https://doi.org/10.1080/01969722.2022.2112539

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cybersecurity. ICCC 2018 Proceedings, Paper 19. https://doi.org/10.23919/CYCON.2018.8405026. [Accessed 20 March 2024]

Bolagsverket. (2019). Vilka företag räknas som större och mindre?, Bolagsverket [Accessed 15 April 2024]

Braun, V., Clarke, V. (2006). Using thematic analysis in psychology, *Qualitative Research in Psychology*, vol. 3, no. 2, pp.77-101, http://doi.org/10.1191/1478088706qp063oa

Bryman, A. (2016). Social Research Methods (5th ed.), London: Oxford University Press

Chang, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Min, D., & Cao, R. (2019). Survey of AI in Cybersecurity for Information Technology Management. TEMSCON 2019 Proceedings. https://doi.org/10.1109/TEMSCON.2019.8813605

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, vol. 4, no. 10, pp.13-21, https://doi.org/10.22215/timreview/835.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. In L. G. Tornatzky & M. Fleischer (Ed.), The processes of technological innovation, pp. 151-175, Lexington, MA: Lexington Books

Gerlach, J., Werth, O., Breitner, M. H. (2022) Artificial Intelligence for Cybersecurity: Towards Taxonomy-based Archetypes and Decision Support. ICIS 2022 Proceedings, Paper 10. https://aisel-aisnet-org.ludwig.lub.lu.se/icis2022/security/security/10 [Accessed 29 April 2024]

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, vol. 3, no. 5, https://doi.org/10.1007/s43546-023-00477-6

Herrmann, D. & Pridöhl, H. (2020). Basic Concepts and Models of Cybersecurity, in M. Christen & B. Gordijn, *The Ethics of Cybersecurity,* Switzerland: Springer Open, pp. 11-44, http://dx.doi.org/10.1007/978-3-030-29053-5_2

IBM. (2024). What is ransomware?, https://www.ibm.com/topics/ransomware [Accessed 6 May 2024]

IBM Security. (2023). Cost of a Data Breach Report 2023 [pdf], https://www.ibm.com/downloads/cas/E3G5JMBP

Jackson, B. W. (2019). Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulations and Autonomous Network Defense. *Minnesota Journal of Law*, Science & Technology, vol. 21, no. 1, https://scholarship.law.umn.edu/mjlst/vol21/iss1/6

Lourens, M., Dabral, A. P., Gangodkar, D., Rathour, N., Tida, C. N., & Chadha, A. (2022). Integration of AI within the Cybersecurity: A detailed Systematic review with the practical issues and challenges. IC3I 2022 Proceedings, pp.1290-1295. https://doi.org/10.1109/IC3I56241.2022.10073040 [Accessed 3 April 2024]

Merhi, M. I. (2023). An evaluation of the critical success factors impacting artificial intelligence implementation. *International Journal of Information Management*, vol. 69, https://doi-org.ludwig.lub.lu.se/10.1016/j.ijinfomgt.2022.102545

Microsoft. (2023). Microsoft Digital Defense Report 2023, Microsoft Digital Defense Report 2023 [Accessed 22 March 2024]

Microsoft. (2024). Navigating cyberthreats and strengthening defenses in the era of AI [pdf], Navigating cyberthreats and strengthening defenses in the era of AI

Oates. (2006). Researching Information Systems and Computing, Los Angeles: SAGE

120 myndigheter drabbade av it-attack – tiotusentals anställda påverkade, SVT, 22 January 2024, SVT[Accessed 19 March 2024]

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modelling and Research Directions. *SN Computer Science*, vol. 2, no. 3, article. 173, https://doi.org/10.1007/s42979-021-00557-0

U.S. House of Representatives Committee on Oversight and Government Reform. (2018). The Equifax Data Breach [pdf], https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Varma, A.J. et al. (2023). A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence. In: Alshurideh, M., Al Kurdi , B.H., Masa'deh, R., Alzoubi , H.M., Salloum, S. (eds) The Effect of Information Technology on Business and Marketing Intelligence Systems. Studies in Computational Intelligence, vol. 1056. Springer: Cham. https://doi-org.ludwig.lub.lu.se/10.1007/978-3-031-12382-5_105

Wallace, S., Green, K. Y., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An Extended TOE Framework for Cybersecurity-adoptions Decisions. Communications of the Association for Information Systems, vol. 47, pp.338-363, https://doi-org.ludwig.lub.lu.se/10.17705/1CAIS.04716

von Solms, R. & van Niekerk, J. (2013). From Information Security to Cyber Security, *Computers & Security*, vol. 38, pp.97–102, https://doi.org/10.1016/j.cose.2013.04.004