Degree project

CYBERSECURITY LEADERSHIP COMPETENCIES IN RESPONSE MODE

Bachelor Degree Project in Informatics

First Cycle 30 credits

Spring term 2023

Student: Michael Zaniewski

Supervisor: Martin Lundgren

Examiner: Ali Padyab

ABSTRACT

Due to the sophistication of cyber threats, organizations need to be defended on a strategic level, leading to the emergence of the cybersecurity leader role. However, the necessary competencies required for successful response are not fully understood due to the unique demands of the role. To bridge this gap, it is crucial to explore how these competencies manifest in practice. Data were collected through interviews and open ended surveys of cybersecurity leaders, which were analyzed using the method of thematic analysis. Four key themes related to necessary competencies were identified: one on knowledge, two on skills, and one on attitudes. The study found that cybersecurity leaders emphasize the importance of having knowledge about the organizational architecture, skills to simplify incident handling procedures, and the ability to convince management to invest in better incident preparedness. They also highlighted the need for a supportive and approachable environment to facilitate optimal cybersecurity incident handling.

Keywords: Cybersecurity Leadership, Competencies, Response Mode, Cybersecurity

Table of Contents

1 Introduction 1
2 Background 2
2.1 Introduction to Cybersecurity Leadership 2
2.2 The Role of Cybersecurity Leaders in Response Mode 2
2.3 The Emergence of the CISO Role 3
2.4 Understanding Response Paradigm in Cybersecurity 3
2.5 Importance of Soft Skills in Cybersecurity Leadership 4
2.6 The Competency Model: A Holistic Approach to Professional Competence 4
2.7 Competencies of Cybersecurity Leaders in Leading Incident Response 5
2.8 Consequences of Inadequate Cybersecurity Leadership 5
3 Problem Statement 6
4 Method 7
4.1 Qualitative Approach 7
4.2 Data Collection 7
4.3 Participant Selection 7
4.4 Thematic Analysis Method 8
4.5 Validity Threats 9
5 Results 10
5.1 Understanding Organizational Architecture 11
5.2 Efficient and Effective Incident Handling Through Simplified Procedures and Tailored Playbooks 12
5.3 Using Marketing Skills and Real-World Examples to Effectively Persuade Management to Invest in Incident Handling Preparedness 13
5.4 Fostering a Supportive and Approachable Culture for Effective Cybersecurity Incident Handling 14
6 Discussion 16
6.1 Method Discussion 16
6.2 Ethical and Societal Aspects 17
6.3 Future Work 18
7 Conclusion 19

1 Introduction

In today's cybersecurity landscape, organizations face escalating threats and a rising number of sophisticated attacks and breaches. The potential consequences of these breaches, such as financial loss, reputational damage, and legal implications, underscore the critical role of competent cybersecurity leaders. Their ability to respond effectively to incidents becomes crucial, as organizations are bound to face cyber-attacks sooner or later. These leaders play a pivotal role in minimizing damage and safeguarding the organization's security and resilience.

The presence of sophisticated cyber threats, including state-sponsored actors and organized cybercrime groups, has made the cybercrime landscape increasingly complex, with organizations becoming targets for various reasons (Ahmad et al., 2021). Consequently, organizations are relying more on cybersecurity leaders, such as CISOs, directors of cybersecurity, and information security managers, to spearhead efforts in safeguarding their information resources (Anderson et al., 2022). These leaders also enable the broader business by protecting data, information, and knowledge, which fosters innovation and ensures operational continuity.

Professionals aspiring to become cybersecurity leaders often face challenges in finding suitable leadership education tailored to their specific needs. Existing cybersecurity knowledge frameworks primarily prioritize technical aspects, overlooking the development of essential leadership skills (Anderson et al., 2022). While this overemphasis on technical skills presents a significant hurdle, there is an additional issue that needs to be addressed: the lack of focus on the response mode paradigm in cybersecurity leadership. The increasing sophistication of cyber-attacks calls for a re-evaluation of the balance between prevention and response strategies (Baskerville et al., 2014). It is crucial to acknowledge that the prevailing research view of cybersecurity leaders tends to overemphasize the prevention paradigm, neglecting the importance of incorporating robust response capabilities (Anderson et al., 2022).

To address the disproportionate emphasis on prevention over response, this study adopts a qualitative approach, combining interviews and open-ended surveys. Its primary objective is to examine the competencies necessary for cybersecurity leaders, particularly in the response mode. While previous studies have identified a limited number of competencies, there is a need to expand the existing list and provide concrete examples of their application in response scenarios. By focusing on the response mode, this research sheds light on the knowledge, skills, and attitudes that enable cybersecurity leaders to effectively navigate and mitigate the impact of security incidents. Emphasizing the importance of response capabilities, this study contributes to a more balanced and comprehensive understanding of the competencies required for effective cybersecurity leadership in today's threat landscape.

2 Background

The background section of this study serves to provide crucial context for understanding the topic at hand. It starts by examining the role of leadership within the realm of cybersecurity, specifically focusing on the emergence of the Chief Information Security Officer (CISO) position. The section then delves into the two paradigms of prevention and response in cybersecurity, underscoring the need to strike a balance between these approaches. Additionally, it highlights the concept of competency through a competency model, which serves as the foundation for identifying the essential knowledge, skills, and attitudes required for effective cybersecurity leadership. Soft skills will be defined, and their significance in effective leadership within the cybersecurity domain will be highlighted. By including these elements, the background section sets the stage for exploring the consequences of inadequate cybersecurity leadership, as previously discussed, in a dedicated subsection.

2.1 Introduction to Cybersecurity Leadership

According to Tubbs and Schulz (2006), leadership refers to individuals who have the ability to influence others towards achieving the goals of an organization. Leadership is a crucial aspect of any organization's success, as without it, companies would not be able to fulfil their objectives of delivering products and services to their customers.

In the context of cybersecurity leadership, it is essential for leaders to strike a balance between risk controls and innovation. While the primary role of cybersecurity leaders is to protect information resources, adopting an overly cautious approach that avoids all risks can hinder innovation within organizations (Baskerville et al., 2014). Cybersecurity leaders face the challenge of balancing information protection and information sharing. At the operational level, they must establish barriers to safeguard sensitive information. However, at the strategic level, they must build bridges with business leaders, the cybersecurity team, and other departments within the organization. In addition, they need to cultivate information-sharing networks externally with vendors, clients, regulators, and even competitors (Hooper & McKissack, 2016; Gupta, 2021; Lanz, 2017).

2.2 The Role of Cybersecurity Leaders in Response Mode

Cybersecurity leaders must effectively balance their efforts and resources between prevention mode and response mode (Baskerville et al., 2014). While regulatory compliance demands considerable attention, allocating resources to proactively address unexpected threats is crucial. Neglecting response mode entirely can have catastrophic consequences, depending on the organization's industry, location, or clientele (Lovejoy et al., 2021). Achieving a balance between prevention and response is essential for effective cybersecurity leadership.

According to Cleveland et al. (2018), the effective handling of cyberattacks necessitates leadership awareness and response guided by a set of best practices for immediate solutions. Preventative measures alone prove insufficient once a cyberattack has occurred. Even with robust and resilient controls in place, the response to a cyberattack extends beyond technological considerations due to the global nature of information technology systems. Therefore, leadership's response must encompass a comprehensive understanding of a broad scope of factors, including behaviour, culture, socioeconomic context, and the impact on individual organizations or across multiple organizations. Auffret et al. (2017) argued that

these factors have contributed significantly to the creation of the Chief Information Security Officer (CISO) role in organizations.

2.3 The Emergence of the CISO Role

Traditionally, IT security in organizations was overseen by the IT security manager or the risk manager, with the role being viewed as an extension of IT. This often meant that IT security was placed within the IT department, under the CIO or similar role, leading to a lack of attention, reporting, and budget allocation. As a result, the executive/board's reporting on security was also diluted, with security having a low profile unless there was a significant breach. The CISO position has emerged in security-conscious organizations such as government departments and banks to address the potential danger of security breaches. The CISO is responsible for the protection and security of information assets and IT systems at a strategic level, aligning with the organization's strategic direction (Hooper & McKissack, 2016).

The role of a cybersecurity leader, such as a CISO, is distinct from traditional operational roles in cybersecurity. While operational roles focus on implementing and maintaining technical controls to protect information resources, cybersecurity leaders have a strategic, business-oriented role that requires collaboration, situational awareness against active adversaries, and a focus on innovation while balancing risk controls (Anderson et al., 2022).

According to Anderson et al. (2022), a comprehensive list of roles and responsibilities that a Chief Information Security Officer (CISO) can assume in spearheading cybersecurity within an organization has been identified. These roles encompass partnering with business leaders, leading the cybersecurity team, directing cybersecurity strategy, governance and policy, overseeing the SETA program, managing cybersecurity risk, and taking the lead in incident response. It is worth noting that the individual fulfilling these responsibilities may not necessarily hold the official title of CISO. Other titles such as Security Director, Security Manager, or Information Security Officer may also be used to denote the role" (Fitzgerald, 2007).

Ahmad et al. (2021) stated that there is a misunderstanding about the necessary competencies for a Chief Information Security Officer (CISO) to be successful in their role. They argued that the role of CISO is often conceptualized as a senior technical role, rather than a strategic and business-oriented role. This suggests that many organizations may not fully appreciate the importance of strategic thinking and business acumen in a CISO, and may instead focus too much on technical skills.

2.4 Understanding Response Paradigm in Cybersecurity

According to Baskerville et al. (2014), information security strategies encompass principles and practices based on both prevention and response paradigms. The prevention paradigm refers to the measures implemented by organizations to prevent security incidents, while the response paradigm focuses on addressing ongoing or occurred security incidents. Although interconnected, these paradigms represent distinct approaches to security management. Consequently, cybersecurity leaders must effectively balance their efforts and resource allocation between prevention and response modes. Furthermore, Baskerville et al. (2014) argue that the increasing complexity of cyber-attacks necessitates organizations to reassess the equilibrium between prevention and response strategies. While a prevention-focused approach

may suffice for repetitive and less sophisticated attacks, the escalating sophistication of threats demands an augmented emphasis on the response paradigm. Managers who comprehend the incident-centered model and operate within an environment influenced by the growing sophistication of attacks will recognize the importance of prioritizing activities aligned with the organization's response paradigm.

2.5 Importance of Soft Skills in Cybersecurity Leadership

Goleman (1995) defines soft skills as "emotional intelligence" in his book "Emotional Intelligence." He contends that the possession and effective use of soft skills have a more significant influence on an individual's overall success or failure compared to technical skills or intelligence.

Previous research conducted by van Yperen Hagedoorn et al. (2021) identified key soft skills that positively influence the leadership positions of Chief Information Security Officers (CISOs) in Dutch organizations. These skills include effective communication, leadership abilities, interpersonal skills, professionalism, integrity, work ethic, responsibility, teamwork, positive attitude, flexibility, and courtesy. The study highlights the need for job descriptions to clearly articulate the required soft skills for cybersecurity leaders. Better descriptions can improve the selection process, which in turn can improve alignment between the tasks and responsibilities of a CISO and the demand from the business. This improved alignment enhances the effectiveness and productivity of CISOs in meeting organizational needs. Additionally, the study emphasizes the importance of educational programs and personal development frameworks that prioritize the development of these essential soft skills.

2.6 The Competency Model: A Holistic Approach to Professional Competence

This study incorporates the competency model by Gonczi et al. (1990) and the concept of the reflective practitioner proposed by Schön (1983) and developed by Eraut (1994) to describe a particular role. Gonczi et al. (1990) introduced an integrated approach to professional competence, moving away from earlier models that focused on either roles and tasks or attributes such as knowledge, skills, and attitudes. The integrated approach considers these four components together, providing a more comprehensive understanding of competence and addressing the limitations of a narrow focus on individual elements.

- ***Knowledge***: Refers to an understanding of concepts, principles, rules, and procedures.
- ***Skills***: Refers to abilities as applied in practice.
- ***Attitudes***: Refers to desires and values.
- ***Roles***: Refers to the specific areas of practice to which knowledge, skills, and attitudes are applied, these roles can also be referred to as domains or functions (Gonczi et al., 1990).

2.7 Competencies of Cybersecurity Leaders in Leading Incident Response

In their study, Anderson et al. (2022) conducted a systematic literature review with the aim of identifying the competencies required by cybersecurity leaders. The study highlighted the role of leading incident response, which was found to predominantly operate in the response mode as predicted by Baskerville et al. (2014). This role requires cybersecurity leaders to possess specific knowledge, skills, and attitudes. In terms of knowledge, it is important for leaders to have a deep understanding of strategy and adversarial thinking, as well as knowledge of investigation and reporting principles. Skills essential for leading incident response include proficiency in planning incident response strategies, the ability to effectively lead response and recovery efforts, and competence in conducting thorough incident investigations. Attitudes that are crucial in this role include a willingness to invest effort in planning incident response strategies, the capacity to respond effectively during emergencies, and dedication to conducting comprehensive incident investigations.

Additionally, Anderson et al. (2022) emphasized the importance of continuing research in this area to further understand and capture the complete set of competencies required for cybersecurity leadership roles in response mode. They suggested that future studies should consider employing empirical data gathering methods and conducting interviews with industry experts to gain deeper insights into the specific competencies that contribute to effective leadership in the field, with a specific focus on response mode scenarios.

2.8 Consequences of Inadequate Cybersecurity Leadership

When cybersecurity leaders are unwilling to familiarize themselves with the organization's overall strategy, invest time and effort in collaboration, and strategically embrace some risks, it can lead to detrimental consequences. This includes damaging their relationship with the broader business, losing influence in the boardroom, and being excluded from important decision-making processes (Aguas et al., 2016).

The catastrophic consequences of incompetent cybersecurity leadership are evident in various real-world scenarios. One notable example is the Equifax data breach in 2017, where hackers were able to gain unauthorized access to sensitive data of approximately 145 million Americans. The sensitive information leak at Equifax, which could have been completely avoided, was further exacerbated by the disorganized and delayed response from the company. According to the former CEO of Equifax, the breach was a result of both human error and technology failures. However, it is evident that inadequate leadership and a corporate under-emphasis on security also played significant roles (Berghel, 2017).

3 Problem Statement

In the realm of cybersecurity, leadership roles such as the Chief Information Security Officer (CISO) are crucial for ensuring effective security practices within organizations. However, there is still a degree of uncertainty surrounding the competencies required for success in these executive positions. Prior research has acknowledged the existence of competencies for cybersecurity leaders, but a comprehensive and specific list tailored to their unique needs is yet to be generated (Anderson et al., 2022). While existing research has shown a noticeable emphasis on the preventive aspect of cybersecurity leadership, the response aspect remains relatively understudied (Ahmad et al., 2021).

The current body of research on cybersecurity leadership competencies has acknowledged the importance of various skills and knowledge areas. However, one notable gap in the existing literature is the lack of concrete and practical examples that demonstrate how these competencies manifest in real-world scenarios.

This study aims to expand our understanding of cybersecurity leadership competencies in the context of response mode. Additionally, the study seeks to gain insights into how these competencies manifest in practice through interviews with cybersecurity leaders.

Research question

What are the practical manifestations of cybersecurity leadership competencies in response mode?

4 Method

4.1 Qualitative Approach

This research employs a qualitative methodology to investigate the competencies that cybersecurity leaders perceive as crucial for success in the response mode, as well as how these competencies manifest in real-world situations. Qualitative research is highly suitable for gathering non-numerical data, including opinions, attitudes, and experiences. Through qualitative interviews, this study provides an opportunity for cybersecurity leaders to express their perspectives on the significant competencies based on their own experiences. This approach proves advantageous in collecting data about competencies based on the experiences of cybersecurity leaders because it facilitates in-depth exploration and understanding. By using open-ended questions and encouraging participants to freely express themselves, the study aims to gather rich and detailed insights into the competencies that leaders deem essential for effectively handling security incidents. Moreover, the qualitative approach enables the examination of contextual factors, such as organizational dynamics and situational challenges, which significantly influence how these competencies manifest in real-life scenarios.

4.2 Data Collection

Data collection was conducted through live interviews via telephone or video conferencing software, and for those unable to participate in a live interview, a survey with open-ended questions was offered. The interviews conducted through Microsoft Teams had their sound recorded for transcription purposes. The interviews were not video recorded to respect the participants' privacy and maintain confidentiality. Similarly, the phone interviews were recorded for transcription into text form for analysis. For those who were unable to participate in a live interview, an alternative method of data collection was offered in the form of a survey with open-ended questions. The participants who chose to complete the survey were able to provide their responses through pre-prepared questions, which were immediately ready for analysis upon submission.

All participants in this study were guaranteed full anonymity when participating, which means that their identities have been completely removed to protect their privacy. To further ensure confidentiality, the recorded interviews were immediately removed upon being transcribed, and the author did not write down the names of the participants in any way that could be correlated to their answers. This was done to ensure that the participants could speak freely without fear of any potential negative consequences, and to uphold the ethical standards of the research.

4.3 Participant Selection

Participants in this study were sought based on specific criteria: they needed to have a leadership role in cybersecurity and possess experience with incident-related tasks in their current or prior job roles. To ensure a diverse pool of participants, recruitment efforts included contacting individuals through social media platforms like LinkedIn, as well as sending requests for participation via email to municipalities across Sweden.

4.4 Thematic Analysis Method

The text was analyzed using the thematic analysis method developed by Braun and Clarke (2006). This approach facilitated the identification of common patterns in participant responses by extracting and grouping codes into themes. The author also adopted a deductive approach, using pre-existing categories based on the competency framework by Gonczi et al. (1990) to categorize codes into knowledge, skills, and attitudes.

1. Familiarizing yourself with your data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes

1. In the first step, the author familiarized themselves with the data by thoroughly reading the transcribed interviews multiple times. This allowed them to gain a comprehensive understanding of the content.

2. The second step involved extracting relevant codes. The author achieved this by identifying commonalities among participants and selecting codes that fell into three distinct categories: knowledge, skill, and attitude.

3. After extracting the codes for these categories, the author proceeded to search for themes. They identified themes either by looking for codes mentioned by at least one-third of the participants or by identifying correlations between different codes mentioned by different participants.

4. To ensure accuracy, the author reviewed the themes and validated them by making sure that the extracted codes truly reflected the participants' intended meaning and were contextualized appropriately. The author also ensured that there were a sufficient number of codes to support the validity of each theme.

5. Finally, in the last step, the author established appropriate names for each theme, which effectively captured the essence and content of the theme.

4.5 Validity Threats

The number of participants can have a significant impact on the validity of conclusions drawn from a study. In this study, efforts were made to reach out to as many participants as possible through social media platforms, including LinkedIn. Additionally, emails were sent to numerous Swedish municipalities to maximize outreach and engagement. However, the potential for a small sample size remains a validity threat, as the number of participants may not be sufficient to draw meaningful conclusions or identify patterns that accurately represent the population. To ensure enough participants, the author provided participants with several methods of gathering data, including open-ended surveys and various interviewing methods, to ensure participant availability and convenience.

One validity threat to consider in thematic analysis is the subjectivity of the author's interpretation of the transcribed text. As with any qualitative research method, different individuals may interpret the same text differently based on their personal biases, experiences, and knowledge. This subjectivity can affect the validity of the conclusions drawn from the analysis, as different authors may identify different patterns and themes in the data. However, in this study, the author did strive to stay neutral and minimize the impact of their own biases on the analysis. It is important to note that the conclusions drawn from this study are based on patterns identified among several participants to ensure that they are not biased or incomplete.

5 Results

The study involved interviewing 11 participants who all had experience working in response mode. Of the 11 participants, 9 were Chief Information Security Officers (CISOs), 1 was an Incident Response Manager, and 1 was an IT Unit Manager. These participants shared valuable insights into how they prepare for potential security incidents, as well as how they act during and after incidents occur.

During the analysis of transcribed responses in the study, a thematic exploration revealed four crucial themes that shed light on the competencies required for cybersecurity leaders in response mode. These themes encompassed the areas of knowledge, skills, and attitudes, providing a comprehensive understanding of the essential competencies needed to navigate and excel in response mode.

The first theme is "Understanding Organizational Architecture." This highlights the significance of having a deep understanding of the organizational structure and dynamics to navigate incidents efficiently. The second theme is "Efficient and Effective Incident Handling through Simplified Procedures and Tailored Playbooks." This emphasizes the importance of streamlining incident handling procedures and creating customized playbooks to optimize response capabilities. The third theme is "Utilizing Marketing Skills and Real-World Examples for Effective Persuasion." It underscores the value of leveraging marketing techniques and providing concrete examples to persuade stakeholders and management about the importance of investing in incident handling. The fourth theme is "Fostering a Supportive and Approachable Culture for Effective Incident Handling." This emphasizes the need to cultivate a workplace culture where employees feel supported, encouraged, and approachable, enabling effective collaboration during incident response.

Categories	**Knowledge**	**Skill**	**Attitude**
Themes	*Understanding Organizational Architecture*	*Efficient and Effective Incident Handling Through Simplified Procedures and Tailored Playbooks* *Using Marketing Skills and Real-World Examples to Effectively Persuade Management to Invest in Incident Handling Preparedness*	*Fostering a Supportive and Approachable Culture for Effective Cybersecurity Incident Handling*

5.1 Understanding Organizational Architecture

Through thematic analysis, the theme of understanding organizational architecture emerged, indicating the importance of comprehending the organization's structure and processes. Participants shared their perspectives, highlighting key areas of knowledge required to effectively manage and respond to cybersecurity incidents.

Participant 4 and Participant 8's perspectives align in their emphasis on the importance of understanding the organization's functioning, key assets, and risks. Participant 4 states, "Leaders that have to manage an organization during an incident need to have a very sound technical understanding, but also a great understanding of how the organization works and what are key assets and risks for the organization." Similarly, Participant 8 highlights the need to protect valuable information assets and maintain control over their location, stating, "Thus, the question is raised: How do we protect our most valuable information assets? Then, a follow-up question is asked: Do we know where the information is located?"

Building upon these insights, Participant 3 adds to the discussion by emphasizing the need for leaders to understand the threat landscape, the business, infrastructure, and the flow of information. They state, "An understanding of the threat landscape, the business, infrastructure, and the flow of information."

Participant 2 echoes the importance of organizational knowledge, highlighting the benefits of knowing the organization and its formal and informal functions. They state, "Knowing the organization and how it functions, both formally and informally in all its parts, is beneficial."

Participant 10 contributes a broader organizational perspective by emphasizing the need to understand various operations. They state, "One must be able to understand various operations. Municipal operations involve an incredible breadth of activities, and it is necessary to grasp the entirety of them."

Lastly, Participant 11 emphasizes the importance of a general understanding of technology, the organization's architecture, business processes, customers or clients, suppliers and partners, and regulatory impact. They state, "A general understanding of technology and the business's architecture. A general understanding of the business processes. A full understanding of the regulatory impact and the necessary communications to each respective body."

5.2 Efficient and Effective Incident Handling Through Simplified Procedures and Tailored Playbooks

The second prominent theme that emerged from the thematic analysis was the significance of efficient and effective incident handling through simplified procedures and tailored playbooks. Participants highlighted the need for streamlined and accessible processes that enable prompt and efficient actions.

Participant 4 emphasizes the importance of policies and plans that provide a framework for incident response teams to execute without roadblocks. They state, "The policies & plans need to set the right framework for the incident response teams to be able to execute, without any roadblocks."

Participant 7 further adds to the discussion by emphasizing the significance of documenting responsibilities, communication protocols, and backup channels during incidents. They state, "The first thing is the process and responsibility surrounding the incident. It is important to document and clarify respective areas of responsibility, how to communicate during incidents, how to handle situations where normal communication channels are down."

Participant 5 and Participant 9 share valuable insights on the importance of simplifying incident procedures to make them easy to understand and follow. Participant 9 brings attention to the importance of simplicity and ease of implementation in incident handling. They state, "If we look at everything from everyday work to continuity plans, we must remember that it should be easy to do the right thing in these types of situations."

Similarly, Participant 5 underscores the significance of ensuring that everyone understands the procedures and playbooks. They emphasize the importance of simplifying the language and content to a basic level that is accessible to all individuals involved. Participant 5 states, "The most important thing is to put it on such a basic level that everyone understands it. Otherwise, it serves no purpose other than looking professional."

Participant 5 shares examples of how incident procedures were simplified, building upon their earlier emphasis on the importance of this approach. They provide concrete instances where the company's "Ledningssystem för informationssäkerhet" (LIS) was translated into employees' native language to ensure clear understanding during cybersecurity incidents. In Participant 5's own words, "I have chosen to write our LIS in Swedish even though we have them ready in English just because I want everyone to understand."

5.3 Using Marketing Skills and Real-World Examples to Effectively Persuade Management to Invest in Incident Handling Preparedness

The third significant theme that emerged from the thematic analysis focused on the importance of utilizing marketing skills and real-world examples to effectively persuade management to invest in incident handling preparedness. Participants emphasized the need to communicate the value of investing in incident handling and the potential consequences of inadequate preparedness.

Participants 5, 7, and 8 all share their experiences in facing challenges when trying to persuade management to invest in better incident handling preparedness. Participant 8 draws from their own experiences and highlights the difficulty of obtaining financial support for incident handling. They emphasize that while everyone acknowledges the importance of incident handling, persuading management to allocate resources remains a significant hurdle. Participant 8 explains, "That's the reality, everyone says how important it is but no one understands, and no one wants to invest money in it. Soft skills are incredibly important because the first task is to explain to the management why this needs to cost money. But there is always a demand that you should be prepared, you should be able to handle incidents, you should raise security, you should raise maturity but you don't get any money."

Participant 5 shares a real-world example from their previous company where the understanding of information security was low. They encountered challenges in requesting a budget for security investments, as management prioritized other physical infrastructure needs. Participant 5 recounts, "I worked at a company that handles explosives, and the understanding of information security was so low that when asked for a budget to invest in security, they said they needed to invest in a new gate instead. I had to explain that a new gate won't protect them from cyber-attacks."

Participant 7, like other participants, acknowledges the challenge of skepticism when it comes to investing in incident handling. They specifically emphasize the importance of conducting a risk analysis and using it as evidence to address the skepticism of stakeholders. Participant 7 highlights that there are strong forces that question the functionality and necessity of such investments. To overcome this skepticism, they assert that having a robust risk analysis and being able to present its findings is crucial. Participant 7 explains, "There are strong forces that look down on functionality and constantly question why. That's when it's important to have a risk analysis and be able to demonstrate it. Otherwise, it can be difficult to convince them. As a CISO, one needs to be aware of the responsibility one has and be able to ensure that there is a basis for building security."

Participant 10, reflecting on their own encounters, highlights the need to approach incident handling preparedness as a marketing endeavor. They stress the importance of understanding sales-oriented marketing principles and effectively articulating the reasons for investing in incident handling. Participant 10 states, "You need to be able to sell this, so maybe you need to know a little bit about marketing. Sales-oriented marketing, you need to be able to market it. Why do we need to work with this? Then you should be able to say why we need to work with this." They further emphasize the significance of providing concrete examples to support the importance of incident handling, stating, "If it's the student health service and you need to

request a report for concern and you don't have access to those systems, what do you do then? Then they reply, 'Well, this is really serious, there might be a school incident.'"

Similarly, Participant 8 presents concrete examples of incident scenarios to make management understand the implications of poor incident handling preparedness. They demonstrate the potential consequences of a loss of availability, such as production problems in the case of a system containing recipes. Participant 8 explains, "This issue of loss of availability, the system where we have the recipes, will there be any relevant consequences if the information is not available? Yes, then we will have problems with production. That's when we started a dialogue with management in a completely different way." Both Participant 10 and Participant 8 emphasize the importance of using concrete examples to provide tangible evidence and create a compelling case for investing in incident handling preparedness.

5.4 Fostering a Supportive and Approachable Culture for Effective Cybersecurity Incident Handling

Through the thematic analysis, the fourth theme that emerged was the importance of fostering a supportive and approachable culture for effective cybersecurity incident handling. Participants emphasized the significance of creating an environment where individuals feel comfortable reporting incidents and seeking guidance from cybersecurity leaders.

Participant 5 and Participant 9 both address the challenges associated with uncertainty and fear within organizations. Participant 5 shared an anecdote about employees being afraid to approach the CISO in a previous organization. They emphasized the importance of meeting individuals with praise instead of irritation when they report incidents, empowering them to come forward and build trust. Participant 5 explained, "I have been at large companies before where people are afraid to talk to a CISO. Something happens, and they respond with: 'We'll solve this ourselves instead.' I reached out to people, and they used to be terrified. 'I haven't done anything wrong.' 'No, but it's not about that.'

Similarly, Participant 9 stressed the significance of creating an environment where individuals feel safe expressing their understanding or lack thereof. They stated, "There is a tendency for those who do not understand a sentence to not dare to say that they do not understand. Additionally, what are the implications of this for the business?"

Additionally, Participant 5 also shares the importance of being both technical and social as a CISO. They emphasize the need to communicate with everyone, regardless of their position, and ensure that individuals feel comfortable asking questions. Participant 5 states, "As a CISO, it's good to be technical but also social, to be able to talk to everyone, lift everyone up and make sure people feel comfortable asking you questions. I treat everyone equally, whether it's the CEO or a technician. I talk to everyone in the same way."

When it comes to approaching incidents, both Participant 1 and Participant 5 share a similar viewpoint on the attitude leaders should adopt. Participant 1 emphasizes the importance of understanding and empathy, stating, "Show understanding to customers and clients, creating a sense of security and reducing stress when communicating during an incident."

Participant 5 echoes this sentiment by highlighting the significance of meeting individuals with praise instead of irritation when incidents are reported. They explain, "When someone reports an incident, meeting them with praise instead of some kind of irritation. For example:

'I have leaked our customer database on Reddit,' 'Great that you're reaching out!' If instead, I were to get angry and say, 'What the hell are you doing?' Then you wouldn't dare to reach out again. 'Empower the staff.'"

Building upon this notion, Participant 5 also shared their approach to creating a more relaxed work environment to counter the tension. They explained, "I allow the staff to play games on the computers. I have written a policy that is rigorous enough. If Counter Strike is installed from Steam, I do not see it as a security risk. However, if you download software from other places that are not classified as safe, it can lead to something negative. You can be a cool person but still be safe." By introducing a policy that allows employees to engage in online computer games, provided they are downloaded and installed from trusted sources like Steam, Participant 5 aims to create a more enjoyable and stress-relieving atmosphere while maintaining a focus on cybersecurity.

6 Discussion

The primary goal of this study was to expand the understanding of competencies for cybersecurity leaders in response mode beyond what prior studies have explored. The findings of this research strongly support this objective by providing real-world examples that illustrate the practical application of these competencies. In this study, the application of the competency model went beyond the traditional focus on technical skills and expanded the perspective of competency to include essential soft skills. This broader perspective was particularly evident in the attitude theme that emerged from the analysis.

It is important to acknowledge the findings from previous studies that have emphasized the significance of communication skills for cybersecurity leaders (Haqaf & Koyuncu, 2018; van Yperen Hagedoorn et al., 2021; Anderson et al., 2022; Sohime et al., 2020). These studies recognize communication skills as important competencies for cybersecurity leaders. However, they often lack practical examples of how these competencies manifest in real-life scenarios within the context of the response mode. Thus, this current study adds value by expanding on existing research and providing detailed insights into a broader range of competencies, including communication skills, and their practical manifestations in response mode scenarios. This study uncovered the practical manifestation of communication skills within the response mode for cybersecurity leaders. Through participant responses, the theme of using marketing skills and real-life scenarios emerged, illustrating how effective communication can be utilized to persuade management to invest in incident handling preparedness.

In the specific context of incident handling, a positive attitude plays a crucial role in creating an environment where individuals feel comfortable reporting incidents and seeking guidance from cybersecurity leaders. Prior studies, such as the work of van Yperen Hagedoorn et al. (2021), have recognized the significance of a positive attitude in cybersecurity leadership. In our study, one participant emphasized the importance of responding to incident reports with praise rather than criticism.

6.1 Method Discussion

Initially, the plan for this study was to conduct in-depth interviews with cybersecurity leaders to gather insights on the competencies required for effective cybersecurity incident handling. However, due to the busy schedules and time constraints of these leaders, it became challenging to secure their participation. To overcome this issue and ensure sufficient data collection, an alternative method in the form of an open-ended survey was incorporated. The inclusion of the open-ended survey allowed cybersecurity leaders to share their experiences and insights on their own time, providing flexibility and convenience. This approach also enabled a larger sample size, enhancing the richness and diversity of the data collected. However, it is important to acknowledge that the survey format may have limited the depth and nuance that could have been captured through direct interviews. Written responses may lack real-time interaction and the opportunity for further exploration. Additionally, time constraints impacted the study, resulting in a smaller sample size and limited depth of analysis. Despite these limitations, the study aimed to provide valuable insights within its scope and contribute to the understanding of competencies in cybersecurity incident handling.

6.2 Ethical and Societal Aspects

Implementing the four identified themes holds the potential for significant societal benefits while also raising important ethical considerations. Understanding organizational architecture empowers cybersecurity leaders to adeptly handle incidents, minimizing damage to organizations. By efficiently allocating resources and coordinating responses, leaders protect organizations, municipalities, and their sensitive data. This approach safeguards human well-being, as attacks on organizations and infrastructure can have broad societal impact. However, the ethical landscape is nuanced. The acquisition of in-depth organizational knowledge must align with principles of privacy and data protection. Leaders should ensure that their understanding doesn't infringe upon individual privacy rights or compromise confidential information.

By adopting simplified procedures and tailored playbooks in incident handling, cybersecurity leaders contribute to fostering a broader understanding of incident procedures on a collective level. This strategic approach goes beyond its inherent societal impact, underscoring the power of involving a wider range of individuals who can comprehend these procedures. This not only promotes inclusivity but also amplifies the effectiveness of incident handling. However, there are ethical caveats. Oversimplification might trivialize the severity of potential cyber threats, leading to inadequate responses.

Through the strategic application of marketing techniques and the use of real-world instances, cybersecurity leaders can effectively persuade management to increase their investment in incident preparedness. With these enhanced resources, cybersecurity leaders can better equip organizations and municipalities to respond to potential cyber incidents. Ethically, cybersecurity leaders must prioritize transparent communication. Persuasion is meaningful when based on accurate information. However, employing manipulative tactics for persuasion undermines trust and transparency, potentially leading to misguided decisions. Misleading stakeholders about threat severity erodes integrity and disrupts the relationship between cybersecurity professionals and management.

Implementing a supportive and approachable culture for effective cybersecurity incident handling could lead to improved incident reporting, increased trust and collaboration, reduced fear and stigma, a positive work environment, empowered employees, resilience against cyber threats, and a stronger societal cybersecurity posture. Ethically, fostering a supportive culture for effective cybersecurity incident handling brings forth concerns. A potential pitfall is the emergence of a false sense of security, where employees perceive invulnerability due to the supportive atmosphere, leading to lax security measures. Moreover, an excessive emphasis on support could blur lines of accountability, hindering incident attribution to specific individuals or teams.

The findings of this study demonstrate potential alignment with Goal 9 (Industry, Innovation, and Infrastructure). Effective incident handling practices can contribute to the development of resilient and secure digital infrastructures, promoting sustainable technological advancements.

This study did not collect any identifiable personal information from participants. Therefore, the General Data Protection Regulation (GDPR) was not applicable to this research. However, privacy and ethical considerations were still prioritized to ensure the confidentiality and anonymity of the participants. The study aimed to uphold ethical principles by minimizing potential risks and respecting individuals' privacy throughout the research process.

6.3 Future Work

Cybersecurity is a rapidly evolving domain that requires competent leaders to guide organizations on a strategic level. As cyber threats become more sophisticated, it's increasingly important for organizations to have skilled cybersecurity professionals who can adapt to the changing landscape and implement effective security measures. The present study provided valuable insights into the perspectives of a small group of participants, but due to time constraints, the number of participants was limited. To build on these findings and gain a more comprehensive understanding of the challenges and opportunities in cybersecurity leadership, future studies could expand the number of participants or explore additional research questions.

7 Conclusion

In conclusion, this study has explored and expanded upon the existing list of competencies necessary for cybersecurity leaders to succeed in response mode, shedding light on their manifestation in real-life scenarios. Through in-depth interviews with cybersecurity leaders, several key themes have emerged, providing valuable insights into the competencies required for effective cybersecurity incident handling.

The first theme that emerged from the study highlights the critical role of understanding organizational architecture in effective incident handling. Cybersecurity leaders who possess a comprehensive understanding of the technical intricacies of their organization, along with the key assets and associated risks, are better equipped to handle incidents with confidence and efficiency. By understanding the processes and interconnections within the organizational architecture, cybersecurity leaders can effectively protect key assets and the overall infrastructure during incidents.

The second theme that emerged from the study focuses on the skill of efficient and effective incident handling through the use of simplified procedures and tailored playbooks. Participants highlighted the importance of developing clear policies, plans, and playbooks that eliminate complexities and provide a structured framework for incident response. By simplifying processes and customizing playbooks to specific organizational needs, cybersecurity leaders can enhance their team's ability to respond swiftly and effectively to incidents.

The third theme that emerged from the study highlights the importance of leveraging marketing skills and illustrating real-world examples to help management better comprehend the consequences of incidents. Cybersecurity leaders face the challenge of being underinvested, which hampers their ability to effectively handle incidents. By presenting concrete examples from actual situations, these leaders can provide tangible evidence that vividly portrays the impact and implications of incidents.

These examples serve as powerful tools to facilitate management's understanding and appreciation of the gravity of incident handling. This, in turn, underscores the critical need for increased investment in incident handling preparedness. Through effective communication and relatable illustrations, cybersecurity leaders can advocate for the necessary resources and support to ensure a robust and comprehensive incident response capability.

The fourth theme emphasizes the critical attitude of fostering a supportive and approachable culture for effective cybersecurity incident handling. Building a culture where employees feel comfortable reporting incidents and seeking guidance from cybersecurity leaders is crucial for timely detection, response, and resolution. The study's findings provide examples of how cybersecurity leaders have created an environment of trust and open communication, encouraging employees to actively participate in incident handling efforts.

References

Aguas, T., Kark, K., & François, M. (2016). The new CISO: Leading the strategic security organization. Deloitte Insights. Retrieved August 13, 2023, from https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security, 101, 102122.

Anderson, A. B., Ahmad, A., & Chang, S. (2022). Competencies of cybersecurity leaders: A review and research agenda.

Auffret, J. P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., ... & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. Journal of Interconnection Networks, 17(01), 1740001.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & management, 51(1), 138-151.

Berghel, H. (2017). Equifax and the latest round of identity theft roulette. Computer, 50(12), 72-76.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Cleveland, S., & Cleveland, M. (2018, May). Toward cybersecurity leadership framework. In Proceedings of the Thirteenth Midwest Association for Information Systems Conference.

Eraut, M. (1994). Developing professional knowledge and competence. Psychology Press.

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. Information Systems Security, 16(5), 257-263.

Goleman, D. (1995). Emotional Intelligence. Bantam Books.

Gonczi, A., Hager, P., & Oliver, L. (1990). Establishing competency-based standards in the professions. Canberra: Australian Government Publishing Service.

Gupta, D. (2021, August 17). The Role Of A CISO In Building A Modern Cybersecurity Culture. Forbes. Retrieved August 12, 2023, from https://www.forbes.com/sites/forbestechcouncil/2021/08/17/the-role-of-a-ciso-in-building-a-modern-cybersecurity-culture/?sh=9e6e5ab25e3b

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. International Journal of Information Management, 43, 165-172.

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. Business Horizons, 59(6), 585-591.

Lanz, J. (2017). The Chief Information Security Officer: The New CFO of Information Security. CPA Journal, 87(6), 52–57.

Lovejoy, K., Burg, D., Maddison, M., & Watson, R. (2021). Cybersecurity: How do you rise above the waves of a perfect storm? Ernst & Young. Retrieved August 12, 2023, from https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

Schön Donald A. (1983). The reflective practitioner: how professionals think in action. Basic Books.

Sohime, F. H., Ramli, R., Rahim, F. A., & Bakar, A. A. (2020, August). Exploration study of skillsets needed in cyber security field. In 2020 8th International Conference on Information Technology and Multimedia (ICIMU) (pp. 68-72). IEEE.

Tubbs, S. L., & Schulz, E. (2006). Exploring a taxonomy of global leadership competencies and meta-competencies. Journal of American Academy of Business, 8(2), 29-34.

van Yperen Hagedoorn, J. M., Smit, R., Versteeg, P., & Ravesteyn, P. (2021). Soft Skills of The Chief Information Security Officer.

Appendix A Interview letter

Dear [Name],

I hope this message finds you well. I am currently conducting a study for my thesis that aims to identify important competencies required for individuals working in cybersecurity at the leadership, executive, or management level, particularly with experience in leading organizations in response to incidents.

If you have the time and willingness to participate, I would greatly appreciate your input on this matter. Your insights and experiences would be valuable in contributing to the success of this study. Thank you for your consideration.

Kind regards,

Michael

Appendix B Interview questions

1. What is your present position in cybersecurity leadership, and could you briefly describe your specific duties in your current position?

2. Have you handled cybersecurity incidents in real-time, such as data breaches or cyber attacks? If so, could you briefly describe your experience?

3. What **knowledge** is necessary for developing and adhering to response-mode focused policies, plans, and procedures?

4. What specific **knowledge** areas are essential for a cybersecurity leader to possess in order to effectively lead their organization's response to various types of cybersecurity incidents?

5. What specific **skills** are important for shifting the focus of policies, plans, and procedures towards response-mode dimensions?

6. What **skills** are necessary for developing and adhering to response-mode focused policies, plans, and procedures?

7. What specific **skills** must a cybersecurity leader possess to effectively lead their organization's response to various types of cybersecurity incidents?

8. What specific **attitudes** are important for shifting the focus of policies, plans, and procedures towards response-mode dimensions?

9. What specific **attitudes** are important for developing and adhering to response-mode focused policies, plans, and procedures?

10. What specific **attitudes** must a cybersecurity leader possess to effectively lead their organization's response to various types of cybersecurity incidents?