The CISO Role: a Mediator between Cybersecurity and Top Management

Håkon Sjøberg Sveen [1][0000-0001-9144-3760]
Filip Østrem[2][0000-0001-6247-092X]
Jaziar Radianti [3] [0000-0001-6860-1652]
Bjørn Erik Munkvold[3][0000-0002-3629-419X]

[1] Sopra Steria, Oslo
[2] Netsecurity AS
[3] Dept. Of Information Systems, University of Agder, Kristiansand, Norway
bjorn.e.munkvold@uia.no

Abstract. As organizations increasingly rely on digital solutions, they also become more exposed to cybersecurity threats. Thus, cybersecurity is becoming a strategic concern for the organizations rather than merely a technological issue. However, many organizations are still not sufficiently aware of the cybersecurity risks and their mitigation. This article studies how to engage the top management more in cybersecurity in order to mitigate the risk of cybersecurity threats. In particular, we focus on the role of the Chief Information Security Officer (CISO) as part of the organization's cybersecurity strategy. We conducted qualitative interviews with nine cybersecurity professionals, including four CISOs, two CEOs, one information security leader and two information security experts. Our study shows that the CISO role is acknowledged as important for facilitating communication between the technical staff and the top management, and for making top management understand the importance of their involvement in cybersecurity. In this sense, the CISO may serve the role as a mediator related to security aspects of the organization. Further, our findings support previous research on the importance for top management to engage actively in cybersecurity matters, including operational risk management, identifying critical assets and data, and defining necessary cybersecurity controls (physical, technical and administrative).

Keywords: CISO Role, Cybersecurity Management, Cybersecurity Strategy.

1 Introduction

In the last decades, we have noticed rapid growth of digitalization across all sectors in public and private organizations. New technologies introduce new challenges that force organizations to adapt their business strategies to cope with the digitalization and change, and not to mention the cybersecurity incidents that are rapidly growing. However, many organizations today are not aware of what risks their organization faces in the cybersecurity domain, nor do they know how to mitigate risks threatening their company [1]. Further, there is uncertainty on who is responsible for an organization's cybersecurity. In a recent poll conducted by The CyberSecurity Hub (2022), 47%

responded that the Chief Information Security Officer (CISO) is ultimately responsible for cybersecurity, while the board members and CEO only received 23% and 21% of the votes.

Taking Norway as an example, the country has embraced an extensive digitalization in public and private organizations, and 96% of all Norwegians are online. Despite this high number, only 6 out of 10 feel capable of judging what is safe online, and cyber-crime costs in Norway is over 19 billion NOK annually [2]. One step to improve the cyber risk awareness for organizations is to involve all parts of the organization, i.e., all employees up to the top management. The board and top management need to be aware of all cyber risks so that measures for cybersecurity are funded and prioritized. If there is an incident, it is likely that the organization's reputation is on the line affecting the organization as a whole [3]. According to Berit Svendsen, former director of a widely used payment service in Norway and a leading telecommunications operator, “Top management in Norwegian companies is not sufficiently concerned with the risk of computer attacks.” [4]. In this article she argues that top management and leaders should ask themselves if the board has the necessary competence to assess the total picture of risk that cyberthreats pose.

The role of the CISO has recently become more relevant as a senior-level executive responsible for the organization’s cybersecurity strategy. In this article we look into the placement of the CISO role in the organizational structure, and how this role can influence the top management to get a better overview of cybersecurity threats and make appropriate cybersecurity-related decisions. We here refer to the top management as defined in ISO 9000:2015 [4], i.e., «the person or group of people who directs and controls an organization at the highest level”.

Our study was motivated by initial discussions with cybersecurity professionals on risk awareness in top management, indicating that the board and top management in many Norwegian organizations are not aware of the benefits of cyber risk awareness in the top management. The discussion also pointed out that the CISO role was often not seen as a top management role, and often had little to no involvement with the top management. Thus, we were interested in exploring, why many organizations operate this way and what could be the possible role of the CISO in the organization’s cybersecurity management. On this background we defined the following research questions (RQs) guiding our study: RQ1: To what extent should the top management be involved in cybersecurity?; RQ2: Who should have the overall responsibility of cybersecurity in an organization?; RQ3: How can a CISO help improve an organization's cybersecurity overall and what should be the CISO’s responsibilities?; RQ4: Where in the organizational structure should the CISO be placed?

The contribution of this article lies in providing insight and highlighting key aspects of the CISO role and its importance in the overall cybersecurity structure of an organization. The rest of the article is organized into 5 sections. In the following section we review related work on the CISO role in organizations. Section 3 describes the methodology used in this study. Section 4 reports the findings, which are discussed in Section 5. Section 6 presents our conclusions.

2 Related Literature

The increased need for boards of directors and executive management to review, monitor and govern organizational information security is discussed in the information systems literature under the topic of information security governance (ISG). This has been defined as “oversight and execution of information security functions, and the establishment of a control environment where policies and procedures which define the role and responsibilities are implemented” [5]. Von Solms and von Solms [6] suggest to also include information security strategy, objectives, organizational structure, risk management and the monitoring of performance. However, the CISO role is not explicitly included in ISG theories or frameworks. Further, related theory on IT and corporate governance rarely focuses on ISG [5]. Moreover, we found limited previous empirical research on the role and responsibility of the CISO, especially related to improving cybersecurity.

Hooper and Mckissack [7] examine the CISO role and organization´s expectation from the role, including the CISO´s responsibility. One of the main focuses of their article is the importance of a CISO that can communicate well. The authors consider that technical expertise is not the only key competence of a CISO. In addition, the CISO should have the following properties: excel in communication skills, possess adequate business knowledge, and having interpersonal skills. These skillsets facilitate the CISO’s effective communication on the cybersecurity challenges with the board and executives [7].

Monzelo and Nunes [8] analyze the CISO role with the aim of trying to understand where the CISO role should be positioned within an organization. The research is based on the case of Portuguese organizations’ maturity towards cybersecurity. They argue that unlike the roles of the CEO and the CIO that are easier to understand, the CISO role is still under evolution. They also contend that earlier, the CISO role has been seen more as a technical role defining security standards and policies, while recently it has become more recognized as a core element of the organization's cybersecurity strategy. As stated in their study: “*In organizations where there is less maturity for security issues, the person in charge of this area is typically under the IT department. In organizations where the board of directors are more aware of information security risks and their impact on business operations, organizational strategy, and reputation, the CISO has a greater proximity and independence with them*.” [8, p.12].

A review study conducted by Onibere et al. [9] explores the necessary competencies required by a CISO to become an effective strategist by doing a review of both security literature as well as strategic management literature. The authors assert the need for a security campaign that highlights the CISO as a “strategist” who is capable of crafting organizational-level security strategies that can be orchestrated and can facilitate the fulfillment of organizations’ goals and objectives [7]. By examining strategic management literature, they were able to identify qualities and characteristics and create five dimensions (i.e., Thought, Contextualization, Execution, Response and Advocacy) of how the CISO can effectively function as a strategist and overcome challenges faced by security management. Furthermore, Maynard et al. [10] use the previous research paper to look into the CISO role as a strategist and point out that “security management within organizations faces a number of strategic challenges that detract from the overall effective security posture of the organizations." [10, p. 9]. The authors also observe the lack of a strategic perspective in security literature where the CISOs were not positioned as strategists.

A study conducted by Karanja [11] aimed to research the position of the CISO by looking at the role of CISOs before and after an IT security breach. One of the results was that 6 out of 13 organizations did not have a CISO in their company before experiencing a security breach, but after the security breach 5 of those 6 organizations hired a CISO. In the findings chapter, Karanja stated that IT security is still being seen as a more technical and specialist function and that CISOs still struggle to gain credibility from the management. On the other hand, the results are consistent with the findings of Ashenden and Sasse [12] in that IT security is still a specialist business function rather than a strategic firm resource and CISOs still struggle to gain credibility as depicted by their reporting structure [11].

A qualitative study conducted in Korea [13] focused on how organizations implemented security strategies and found considerable evidence from the organizations involved in the study that security strategy is driven bottom-up rather than top-down. The highest-ranking security role in the organization existed at a middle management level or lower. Moreover, this study found that every participant except one did not mention anything of driving strategy from organizational security policies or speaking to senior management on strategy related issues.

A recent article by Zwilling [14] focusing on trends regarding cyber risk looks into the CISO role and its level of cyber-related preparation to mitigate cyber threats. The findings show that the scientific literature is not heavily concerned with the lack of CISO knowledge and training and its effect on the CISO's ability to mitigate cyberthreats successfully. On the contrary, expert opinion columns clearly show that this concern should be considered seriously [14]. The study concludes that companies need to evaluate their CISO's knowledge of new cyber challenges and risk and consistently invest in both improving this knowledge and in new technological solutions that can help mitigate those risks.

The importance of good communication abilities for the CISO appears in several articles reviewed. For example, Hooper and Mckissack [7] point out that "[...] *the CISO should be an excellent communicator with business knowledge and interpersonal skills"* [7, p. 591]. The authors discuss in-depth the importance of the CISO being a good communicator that can translate his/her technical expertise to a more fitting language to make for example the top management understand the cybersecurity risk or solutions better. This was also identified by Maynard et al. [10] as one of the dimensions required for a CISO: a CISO needs the ability to negotiate, influence and communicate clearly as some of the important functions for the CISO to become a strategist [10].

The structural positioning of roles within cybersecurity was also a largely focused theme, i.e., where and who in an organization should be aware of and prioritize risks related to cybersecurity, as discussed by Monzelo and Nunes [8]. They claimed that in an organization where the board of directors are more aware of cyber risk, the CISO has a greater proximity and independence with the board [8]. While other studies focus more on information security becoming an organizational strategy that will help the organization in protecting their information system [10, 13].

3 Research Approach

3.1 Data Collection

We employed a qualitative approach with semi-structured interviews as the data gathering method. The inclusion criterion for selecting informants was that they should be cybersecurity professionals in public and private organizations with knowledge about the CISO role. A total of nine interviews were conducted with two CEOs, four CISOs, one Information Security Leader, and two Information Security Experts. We recorded all interviews, lasting between 30 to 60 minutes each. Table 1 provides an overview of the informants, with anonymized organization names.

Table 1. Overview of informants

No	Role	Org	Sector	Size	Type of business
R1	CEO	A-Sec	Private	Medium	Data collection / data handling
R2	CISO	B-Sec	Private	Large	Educational
R3	CEO	C-Sec	Private	Medium	Consultant firm
R4	CISO/IT & Operations manager	D-Sec	Private	Medium	Software company
R5	CISO	E-Sec	Private	Large	Commercial broadcasting enterprise
R6	Information Security Leader	F-Sec	Public	Large	IT provider
R7	CISO	G-Sec	Public	Large	Government agency
R8	Expert	H-Sec	Private	Medium	Managed Security Service Provider
R9	Expert	I-Sec	Private	Medium	Managed Security Service Provider

3.2 Data Analysis

We employed qualitative Thematic Content Analysis (TCA) for analyzing the interview transcripts. TCA is a suitable approach to use when the research is based on people’s views, opinions, knowledge, experiences or values from a set of qualitative data [15]. In practice, TCA can either be inductive or deductive. We adopted a deductive approach, because we already had some preconceived themes derived from the earlier literature findings, theory and existing knowledge that were expected to be reflected in the interviews.

There are various approaches to conduct TCA, but we followed the six-step process defined in [12], i.e., familiarization, coding, generating themes, reviewing themes, defining and naming themes, and lastly writing-up. First, in the *familiarization stage*, we aimed at getting to know our data to get a thorough overview of all the data that had been collected before we started analyzing individual items. This part involved transcribing audio, reading through the transcribed text and taking initial notes of interesting findings as well as going through the data. Second, in the *coding stage*, we coded our interviews, highlighted data and sections from the interview transcriptions and turned them into codes/labels. Eight out of nine interviews were conducted in Norwegian, and the code were translated to English. An example excerpt from the interview with R2 can be seen in Table 2 for illustration of the coding process.

Third, in the *generating theme stage*, we generated themes by analyzing the codes identified from each individual interview in interpretation sessions using sticky notes. The notes were then organized into an affinity diagram (Fig. 1). An affinity diagram consists of hierarchical groupings of structures and themes, built with post-it notes, using different colors to represent the different layers in the hierarchy. These groupings were then given names and categorized into main themes [16]. The themes first identified were Measures, CISO, Top Management, Opportunities and Others.

Table 2. Example of the coding process

Interview 2 extract	**Codes**
You cannot pinpoint just one thing. It's an array of things that you need to take care of [most important thing organizations need to do to secure itself or from cyber-attacks - author clarification] *Uh, number one is obviously the technological side of things, so you need to put technological controls in place.* *Uh, then you have the human aspect of things where you need to also make sure that you have enough awareness in your organization against the most obvious threat actors, like phishing emails and*	● Technological measures/controls ● Awareness ● Risk awareness ● Necessary measures ● Administrative measures/controls ○ Policies ○ Procedures

Fourth, in the *reviewing theme stage*, we conducted evaluation and refinement of the themes, and changed into more fitting themes where necessary. Some themes were too broad while others were too narrow or did not apply to our research problem. The color of the notes was also refined to make it more clear which themes related to each other. Figure 1 is an illustration of refined themes in affinity diagram form.

The *defining and naming theme stage* involved formulating what is exactly meant by each theme and figuring out how these themes can help in understanding the data. Our final, refined naming of the themes was: *Measures, CISO role, Mixed CISO role & Top management, Top management, Opportunities and Others*. The most relevant themes identified were *CISO role and Top Management* as these themes have a clear and direct connection to our RQs. The interviews also produced most data related to these two themes. Indeed, the remaining themes were also important in terms of enhancing our understanding of the complexity of the research problem and to give a broader insight to the research field as a whole. The sixth stage is *writing up*, which is presented in Section 4.

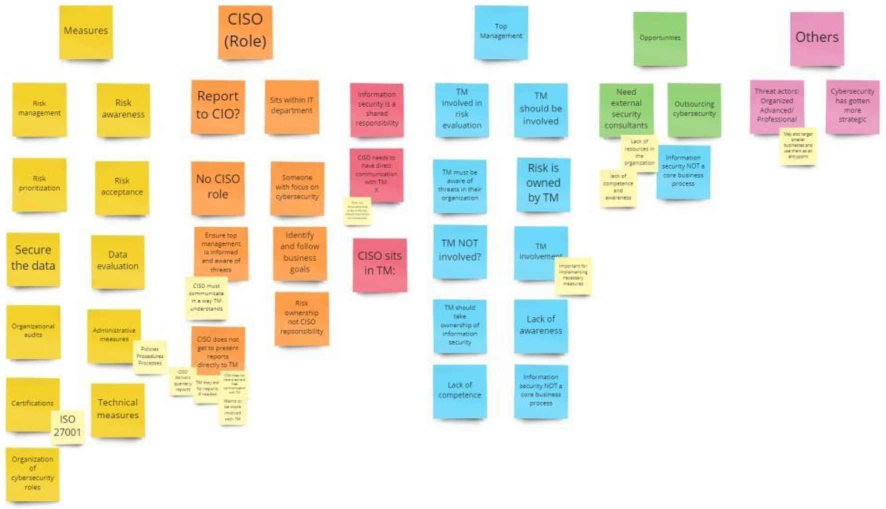
Measures
CISO (Role)
Top Management
Opportunities
Others
Risk management
Risk awareness
Report to CIO?
Sits within IT department
Information security is a shared responsibility
TM involved in risk evaluation
TM should be involved
Need external security consultants
Outsourcing cybersecurity
Threat actors: Organized Advanced/ Professional
Cybersecurity has gotten more strategic
May also target smaller businesses and use them as an entrypoint
Risk prioritization
Risk acceptance
No CISO role
Someone with focus on cybersecurity
CISO needs to have direct communication with TM: X
TM must be aware of threats in their organization
Risk is owned by TM
Lack of resources in the organization
lack of competence and awareness
Information security NOT a core business process
Secure the data
Data evaluation
Ensure top management is informed and aware of threats
Identify and follow business goals
CISO sits in TM:
TM NOT involved?
TM involvement
Important for implementing necessary measures
CISO must communicate in a way TM understands
Organizational audits
Administrative measures
Policies Procedures Processes
Risk ownership not CISO repsonsibility
TM should take ownership of information security
Lack of awareness
CISO does not get to present reports directly to TM
CISO delivers quarterly reports
TM may ask for reports if needed
Wants to be more involved with TM
Certifications
ISO 27001
Technical measures
Lack of competence
Information security NOT a core business process
Organization of cybersecurity roles

Figure 1 Refining themes after generating themes

4 Results

In this section we describe the research results, organized according to the research themes identified in the previous section.

Top Management Involvement in Cybersecurity. Our informants mostly agreed on the criticality of the involvement of the top management in cybersecurity-related work in organizations, despite some variation in their arguments behind this. The A-Sec CEO (R1) was clear that the top management was involved in most of the activities related to cybersecurity. This included risk evaluation, risk management, data analysis, data evaluation, deciding measures and revising them (technical and administrative), and also mitigation. At the time when we interviewed R1, s/he had some of the delegated CISO responsibility shared with a former employee that helped with cybersecurity. The A-Sec company did not have a CISO employed and was in the process of recruiting a CISO: «*.... We now have 120 employees, and we are evolving heavily. [...] We are currently in the process of recruiting for that now. [...] I think that if you don't have a CISO, because often you might not have that, you might have a CTO, but you should have someone with the focused responsibility of security…*». In brief, the CEO with cybersecurity responsibility comes rather as an enabler for the business. But cybersecurity is also not something everyone can handle as it requires special knowledge and proper training, thus the need for recruiting a CISO.

In contrast, the top management in the E-Sec organization admitted that s/he is less involved in the cybersecurity work or making cybersecurity-related decisions. As a CISO in E-Sec, R5´s responsibility includes creating quarterly reports, but ….”*the* *leader of Digital, the CDO (Chief Digital Officer) presents them.... If I could say one thing ... it would be that it was myself that got to present the reports for the board....".* The CISO further wished to have the possibility of more communication with the top management in general. Seemingly there was limited communication between R5 as the CEO of E-Sec with the top management. E-Sec is owned by another company that also has its own CISO. Thus, the CISO role was more on the administrative level and in direct communication with the parent company of E-Sec. The CISO in the parent company creates policies and requirements for security for both the parent and the subsidiary companies.

Instead of contrasting the role of the CISO vs. top management in the cybersecurity work, the expert from the H-Sec company (R8) rather observed in a more detail in what way the top management can contribute to facilitate the cybersecurity work and is critical, i.e. setting the tone, identifying the critical assets and data sets, mapping the top events that would impact business goals and providing support, mandate and backing for employees to execute on necessary cybersecurity controls including technical, awareness, mapping and continuous improvement. This opinion was confirmed by the expert R9 from I-Sec who pinpointed the critical role of the top management in terms of operational risk management, and risk related to cybersecurity. R9 emphasized that *"cybersecurity tech knowledge is not necessary for top management".* Apart from the issues of CISO structure and communication with the top management, the interviews showed that the informants concur strongly that the top management in an organization has a critical role to be more involved in the cybersecurity work.

Perceived Cybersecurity Ownership and Awareness. Most of our interviewees considered that risk and cybersecurity is owned by top management. Several of the informants shared the same opinion, and the CISO from B-Sec (R2) explained these thoughts in a good way: *"I feel that risk is owned by the top leadership. It's not my responsibility. Infosec is not my responsibility. It has been delegated to me from the top level management, so it's my responsibility to let them know that these are their business risks. I can help you in mitigating them, but you should at least know and if you want me to prioritize some of them more than the other, because I might see it in a different way."* Both expert informants (R8 and R9) also agreed that the responsibility of cybersecurity lies with the CEO and the top management in an organization. The expert from H-Sec (R8) stated the following about cybersecurity ownership: *"The CEO should know that s/he is responsible for cybersecurity in the organization. Even board members can be fined or go to jail over lapses in cybersecurity."*

Moreover, R9 from I-Sec considered that while cybersecurity is owned by the top management, the responsibility for daily security operations should be delegated to a role with sufficient competence within the area, such as a CISO. R9 further stated that it is too much specialization in the cybersecurity field for an ordinary board member: "[...] *However a person with expertise and dedication should be nominated to own the management system for information security, there is too much specialization and changes happening for a person on the board or the CEO to operate this on a daily basis. Top management should be involved in risk assessments, strategic decisions and encourage delivery and improvements to cybersecurity through Key performance indicators and regular meetings with the cybersecurity leader and staff*."

In brief, our interviewees deemed that the responsibility of cybersecurity lies in the hands of the CEO together with the top management. Thus, they should be aware of this responsibility, and that they can get fined or even go to jail if they do not implement cybersecurity in their organization. A person with sufficient cybersecurity expertise should be nominated to help the CEO and top management in managing cybersecurity.

Perceived Role and Responsibilities of the CISO. We asked our informants on the most important tasks and responsibilities of a CISO. The respondents had different answers to this question. The CEO from A-Sec (R1) suggested that the CISO owns the whole “umbrella” for information security, and thus has responsibility for cybersecurity activities and for prioritizing these. The CISO from B-Sec (R2) argued that the CISO’s responsibility is to identify business goals and activities and align these goals with cybersecurity goals. The C-Sec CISO (R3) illustrated that their job is a kind of a control function and s/he worked mostly with creating and writing policies, the distribution of policies, and following up security measures and demands. The CISOs R4 and R7 explained that they coordinate the cybersecurity work across the organization, making sure everyone has a good understanding of the cybersecurity risks and also ensuring organizational compliance to the committed norms, agreement, and certifications. R3 mentioned that the CISO is responsible to get an overview of the security and define everything from security policies to routines. The CISO R7 concurred with R2 on the importance for CISOs to understand the business of the organization.

The F-Sec information security leader (R6) said that the CISO’s responsibility often related to and evolved around communication. R6 deemed that the most important job of the CISO often was to communicate what might be a little more technically demanding for the leaders to understand, using correct, proper, and understandable business terminology and language. R6 emphasized the knowledge of the “business language” to enhance the top management´s understanding on cybersecurity issues. There was almost no disagreement among the interviewees on the capability of communication with top management being a part of the skillset required for a CISO. To conclude, the interviews identified the perceived role and responsibilities of the CISO to include the following: 1) Excel the business goals and strategies; 2) Communicate with the top management and learn about the organization´s important assets; 3) Define appropriate/necessary measures, i.e. technical and strategic controls; and 4) Being a good communicator and security adviser, and being able to propose appropriate measures to the top management in an understandable way.

Other Findings. We also identified several other issues relevant for the CISO role:

- *The need for understanding of the threat actors*. Recently the threat actors have become much more organized, advanced and professional, especially the APTs (Advanced Persistent Threats). They may even target smaller businesses and use them as an entry-point to larger organizations and business partners.
- *Core business dilemma and outsourcing*. Cybersecurity is usually not a part of the core business for most organizations. The companies are completely dependent on good partners, both the IT manager and the IT organization. Some interviewees pointed out that they needed to use help from external cybersecurity partners and consultants, even the largest companies with over 1600+ employees. Smaller businesses with smaller budget also have the possibility of hiring CISO consultants

for shorter periods instead of hiring a full-time CISO, as expressed by R7: *"For organizations that do not have the money to hire a CISO, I always recommend that they hire or "rent" a virtual CISO or CISO consultant for hire."*

Placement of the CISO in the Organization. We found two different opinions on this issue from the interviews. While some informants advocated the incorporation of the CISO in the top management structure, some informants considered it unnecessary to place the CISO in the top management as long as there was a good communication between them.

Examples of the proponents of the first idea were R2 and R7 who suggested that the CISO should sit together with the top management and be included in strategic planning, and be expected to deliver metrics, support key business goals, vision and mission of the companies. Changes in the business or the cybersecurity landscape will impact the information security management system of the company and possibly business plans. However, R2 and R7 emphasized that the CISO's placement might depend on the background of the individual CISO. If the CISO comes from the business side, the CISO should be in management team. If the CISO has a strong technical background, the cybersecurity report should be addressed through the CTO or the CIO. An example of the proponent of the second idea was R9 who considered the CISO´s work should cover the handling of operational risk related to the digital solutions to support the organizational goals. In fact, most of the top management agenda is not related to cybersecurity. R9 did not think the CISO should be placed in the top management, but acknowledged the importance of the CISO to regularly inform the top management on the status of the cybersecurity in the organization.

To sum up, it is difficult to suggest a single viewpoint on the placement of the CISO role in an organization, as the interview results suggest that it also depends on the CISO´s background and the organizational culture in general. However, regardless of the placement of the CISO, the informants agreed that to be successful the CISO or the person responsible for cybersecurity should have frequent and direct communication with the top management.

5 Discussion

This section discusses the findings derived from our thematic content analysis The discussion and interpretation of the findings are important to help answer the research questions for our study.

Involvement of top management. In RQ1 we ask to what extent the top management should be involved in cybersecurity. Our findings suggest that the top management needs to be involved in the organization's work with cybersecurity, thus also supporting former research. For example, Ahmad et al. [13] underline that a low level of involvement from senior management can hinder the development of security strategies in organizations. They point to the senior managers' perceived limited role in shaping security strategy, lack of commitment to the security strategy function, and the low-level of involvement in strategizing as factors that hinder the development of security strategy within organizations. [13].

Based on our findings there was a vagueness on *how much* the top management needs to be involved. However, most of the CEO/CISOs interviewed in this study agreed that the involvement of top management is critical, and it was expressed that the top management needs to be more actively involved in work related to cybersecurity. Here they specified the following tasks: 1) Identifying critical assets and data; 2) Operational risk management; 3) Decide necessary cybersecurity controls, including physical, technical and administrative controls. While examining frameworks for enterprise security architecture is beyond the scope of this article, it is worth mentioning that there are well developed best practices, standards and frameworks that can help the organizations in managing their cybersecurity strategies or align business and cybersecurity goals, such as the SABSA Framework [17, 18].

Hooper and Mckissack [7], who support the notion of higher engagement of top management in cybersecurity, also argue that there is no way every board member needs to act as a security expert But raising their awareness of what CISOs see as critical is important and a way to begin communication on the topic [7]. Findings from Bongiovanni et al.´s study [19] confirm the need for enhancing the top management´s knowledge on cybersecurity risks and provide a set of practical recommendations on how to achieve this.

Responsibility of Cybersecurity. In RQ2, we ask who should have the overall responsibility of cybersecurity in an organization. As explained in Section 4 our expert informants agreed that the cybersecurity responsibilities are owned by the CEO and the top management who have the authorities to make decisions across organizations. Admittedly, they still need a person with the delegated responsibility to manage information security. While a CISO can do this job perfectly, their involvement with top management is essential to prevent situations where the CISO has to struggle to gain credibility, getting funding for necessary measures, and getting overview of organizational assets to be protected. Besides, everyone in an organization, all the way from the top leaders to the employees at the bottom of the organization should be aware of threats and take part in cybersecurity. This finding is in line with e.g. Rothrock et al. [20] who argue that cybersecurity should not only engage all elements within the organization, but also goes beyond the boundaries of a single organization. That is, it should reflect interactions with suppliers, customers and vendors that increasingly are taking place in the cyberspace, thus even strengthening the requirements for everyone to take part and be responsible for preventing cybersecurity risks to happen.

CISO’s Influence and Responsibilities in Organizations. In RQ3 we ask how a CISO can help improve an organization's cybersecurity overall. Our study shows that skills are needed for communicating cybersecurity to everyone in an understandable way, regardless of their background. When the top management involves themselves in cybersecurity and has direct communication with a CISO that knows how to communicate in a good way, this might help in enabling the CISO’s abilities to work on a more strategic level, and by doing so also improve the organization’s cybersecurity overall. This is also discussed in the article by Karanja [9, p. 318]: *“By hiring a CISO (IT security leadership) and having a clear reporting structure (organizational structures) whereby the CISO reports either to the CEO or a CIO, who in turn reports to the CEO, the firms are affirming and communicating, both to the internal and* *external stakeholders, that they are committed to guaranteeing the confidentiality, integrity and availability of IT resources."*

As to CISO responsibilities, we found variations between each organization, but based on the interview findings it is clear that the main responsibilities of a CISO and much of the CISO's function often revolve around knowing the business, knowing the assets the organization possesses and communicating the status with necessary measures to the rest of the organization. The communication responsibilities of the CISO have been emphasized in the literature such as Maynard at al. [8] who argue how important it is that the CISO is able to communicate strategies clearly in order to motivate and influence the relevant stakeholders and inspire towards a shared vision of information security: *"CISOs operating as strategists within the dimension of advocacy are thus required to possess the communication skills to clearly communicate security strategy in understandable terms to senior management in order to secure buy-in for security initiatives*." [9, 10].

They further explain that CISOs should be able to bridge existing communication gaps, overcome people's resistance to change, and also facilitate the organizational transformation by inspiring shared vision of security across the organization [9]. In fact, very often CISOs or people within the field of IT use very technical language that may be difficult to grasp, unless the CISO has good communication skills. Without denying the importance of technical expertise, Hooper and Mckissack [7] emphasize that the CISO should be an excellent communicator with business knowledge and interpersonal skills rather than just being a technical expert. Moreover, they suggest that the CISO is a senior-level executive and that the CISO should therefore be performing strategic-level tasks rather than daily operational ones [7]. They also investigated the job descriptions of the CISO and found that some of these contained elements of business knowledge and understanding, but that the main and primary focus and importance of the job description was more technical and security focused and that the candidate had technical security expertise [7]. This shows that very often when people are discussing ways of securing organizations they might first think of more technical measures and get hung up in only thinking of the more technical bit of cybersecurity. The authors agree that the technical bit of cybersecurity is important, but often the strategic measures are just as important to discuss when it comes to cybersecurity and securing organizations.

Placement of the CISO. In RQ 4 we asked where in the organizational structure the CISO should be placed. This is the only question where the experts had slightly different opinions on the matter, which is also reported in previous studies. For example, a study by Monzelo and Nunes [8] explains that only the expert consultants they interviewed shared the view that the CISO should have a position with the board of directors. The authors also expressed the challenge of verifying this reality in any organizations under study [8]. This is similar to our study, as the findings from our interviews were not able to verify if the CISO actually should sit together with the top management or not as the placement of the CISO was different between the organizations. The opinions on this matter also differed from interview to interview. It should be noted here that the study by Monzelo and Nunes [8] looked into if the CISO should be placed among the board of directors, and not if the CISO should sit in the top management as is the focus in our study.

While several of the respondents expressed that the CISO should be placed together with the top management there were also several who were unsure if this was necessary. As long as the CISO had direct communication with the top management and the possibility of giving them regular updates on the status of cybersecurity, the CISO did not have to sit in the top management. Some informants also mentioned that the placement of the CISO might depend on his/her background and that this may also affect the way CISOs make decisions in a company. Depending on whether the CISO comes from a technical or a more strategic background might for example affect what the CISO sees as critical assets. One more thing that might affect the placement of the CISO could be the size of the organization. However, we could not identify any data pointing to this in our research. The placement of the CISO in the organization is thus hard to determine and is something that should be focused in further research.

6 Conclusion

Our study aimed at investigating if it is crucial that the top management in private and public sector gets involved in cybersecurity in order to properly secure an organization. Our study shows that the top management needs to be included or involve themselves actively in cybersecurity matters and proposes some strategic activities that will help improving overall organizational security. For example, to identify critical assets and data, operational risk management and provide backing for necessary cybersecurity controls including physical, technical, and administrative controls.

The study also investigates who should have the overall responsibility of cybersecurity in an organization, which does not have a clear-cut answer. Our study shows that the CEO together with top management should hold the responsibility for cybersecurity, with the possibilities to delegate the tasks for daily operation to a role with sufficient competence and expertise.

Concerning the question on how a CISO can help improve an organization's cybersecurity overall, it can be concluded that the functions of the CISO may vary from organization to organization. The CISO responsibilities suggested by the informants included knowing the business, knowing the assets of the organization, and communicating this to the top management and to the rest of the organization. In essence, the CISO should take the role as a mediator between cybersecurity and top management. By taking such a role and being a good communicator of cybersecurity, the CISO can gain better credibility and raise cybersecurity awareness across the whole organization.

Lastly, regarding the question of where in the organizational structure the CISO should be placed, both the findings from the literature review and the interviews varied. However, they all agreed that frequent communication and status reports of cybersecurity between the CISO and top management is a necessity. Some informants also mentioned that the placement of the CISO and the decisions the CISO make might depend on the CISO’s background.

References

[1] Kitten, T.: Cybersecurity: The CEO's Responsibilities. Bank Info Security (2015). https://www.bankinfosecurity.com/interviews/durbin-from-london-i-2969, last accessed 2022/10/28.

[2] Malmedal, B., Røislien, H.E.: The Norwegian Cybersecurity Culture. Norwegian Centre for Information Security (NorSIS) (2016).

[3] Dunbar, T.: The First Steps to Managing Cyber-Risk. Risk Management 59(8), 20-25 (2012).

[4] Svendsen, B.: I sjefsstolen: Da hackerne slo til. *E24*. https://e24.no/karriere-og-ledelse/i/WjXbaK/da-hackerne-slo-til (2022), last accessed 2022/10/28.

[5] Wong, C.K., Maynard, S.B., Ahmad, A., Naseer, H.: Information security governance: a process model and pilot case study. ICIS 2020 Proceedings, 3 (2020).

[6] Von Solms, R., von Solms, S.B.: Information Security Governance: a model based on the direct–control cycle. Computers & Security, 25(6), 408-412 (2006).

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

[8] Monzelo, P., Nunes, S.: The Role of the Chief Information Security Officer (CISO) in Organizations. Presented at the 19.ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI'2019) (2019).

[9] Onibere, M., Ahmad, A., Maynard, S.: The Chief Information Security Officer and the Five Dimensions of a Strategist. PACIS 2017 Proceedings, 77 (2017).

[10] Maynard, S., Onibere, M., Ahmad, A.: Defining the strategic role of the chief information security officer. Pacific Asia Journal of the Association for Information Systems 10(3), 3 (2018).

[11] Karanja, E.: The role of the chief information security officer in the management of IT security. Information & Computer Security 25(3), 300-329 (2017).

[12] Ashenden, D., Sasse, A.: CISOs and organisational culture: their own worst enemy? Computers & Security 39(Part B), 396-405 (2013).

[13] Ahmad, A., Maynard, S.B., Park, S.: Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing 25(2), 357-370 (2014).

[14] Zwilling, M.: Trends and Challenges Regarding Cyber Risk Mitigation by CISOs - A Systematic Literature and Experts' Opinion Review Based on Text Analytics. Sustainability 14(3), 1311 (2022).

[15] Caulfield, J.: How to Do Thematic Analysis. Last accessed 2022/09/06. https://www.scribbr.com/methodology/thematic-analysis/ (2019).

[16] Lazar, J., Feng, J.H., Hochheiser, H.: Research methods in human-computer interaction. Morgan Kaufmann (2017).

[17] Burkett, J.S.: Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. Information Security Journal: A Global Perspective 21(1), 47-54 (2012).

[18] Sherwood, J., Clark, A., Lynas, D.: Enterprise security architecture whitepaper. SABSA Limited (2009).

[19] Gale, M., Bongiovanni, I., Slapnicar, S.: Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security* 121, 102840 (2022).

[20] Rothrock, R.A., Kaplan, J., Van Der Oord, F.: The board's role in managing cybersecurity risks. MIT Sloan Management Review 59(2), 12-15 (2018).