Alina Kyrölä

REPORTING CYBER SECURITY TO MANAGEMENT AND BOARD OF DIRECTORS

UNIVERSITY OF JYVÄSKYLÄ
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

ABSTRACT

Kyrölä, Alina
Reporting Cyber Security to Management and Board of Directors
Jyväskylä: University of Jyväskylä, 2022, 93 pp.
Information Systems Science, Master's Thesis
Supervisors: Siponen, Mikko & Ylhäisi, Teemu

The importance of cyber security reporting on board and management level has been and is still increasing constantly. Cyber security incidents are growing and evolving, while the common view is that the boards and management are not prepared for their role of ensuring cyber security in their organisations. There are recognised challenges with organisations having issues in reporting about cyber security to their boards and management efficiently. However, currently offered solutions, and the already existing reporting frameworks and models do not fit the needs of all organisations in this matter.

This Master's thesis studies board and management level cyber security reporting, including its history, current state, issues, and practices that are advocated for. The motivation for this study is the rising importance of board and management level cyber security reporting, and the fact that the level of it does not generally meet the needs of organisations. This research aims to offer a solution on how to report cyber security to boards and management effectively.

There are recognised issues with reporting too rarely, reporting about topics that do not provide the boards and management with the information they need, and communicating ineffectively. The topics reported are often too focused on overly technical data, and metrics that are not necessarily based on evidence. The ineffective communication is commonly related to the lack of visuality, or using it wrong, or using language that is too technical for the audience. In this research paper the significance of visuality is studied, in addition to the general evolution of cyber security reporting on board and management level.

This thesis presents a process model for creating an effective reporting method for board and management level cyber security reporting. The model offers a new, iterative way to form an operating reporting method, and to keep it up to date.

Keywords: Cyber security reporting, Cyber security, Board of directors and management, Visuality

TIIVISTELMÄ

Kyrölä, Alina
Reporting Cyber Security to Management and Board of Directors
Jyväskylä: Jyväskylän yliopisto, 2022, 93 pp.
Tietojärjestelmätiede, Pro gradu -tutkielma
Ohjaajat: Siponen, Mikko & Ylhäisi, Teemu

Johto- ja hallitustason kyberturvaraportoinnin tärkeys on kasvanut ja kasvaa edelleen. Kyberturvahyökkäykset lisääntyvät ja kehittyvät, ja yleinen näkemys on, etteivät johto ja hallitukset ole valmistautuneita rooliinsa organisaationsa kyberturvallisuuden varmistamisessa. Haasteita kyberturvallisuuden tehokkaassa raportoinnissa johto- ja hallitustasolla on jo tunnistettu, mutta tällä hetkellä tarjotut ratkaisut, ja jo olemassa olevat viitekehykset ja mallit, eivät vastaa kaikkien organisaatioiden tarpeisiin.

Tämä Pro Gradu -tutkielma tutkii johto- ja hallitustason kyberturvaraportointia, mukaan lukien sen historiaa, nykytilannetta, ongelmia, ja puollettuja käytäntöjä. Tutkielman motivaatio on johdon ja hallituksen kyberturvaraportoinnin kasvava merkittävyys, ja realiteetti sen tason kyvyttömyydestä vastata organisaatioiden tarpeisiin. Tutkielman tarkoitus on pyrkiä tarjoamaan ratkaisu, joka mahdollistaa kyberturvallisuuden raportoinnin johdolle ja hallitukselle tehokkaasti.

Tunnistettuja johto- ja hallitustason kyberturvaraportoinnin ongelmia ovat muun muassa liian harvoin raportoiminen, aiheista raportoiminen, jotka eivät tarjoa kohderyhmälle heidän tarjoamaa informaatiota, sekä epätehokkaasti kommunikoiminen. Raportoidut aiheet keskittyvät usein liian tekniseen dataan, ja metriikoihin, jotka eivät ole evidenssiperusteisia. Epätehokas kommunikointi liittyy yleensä visuaalisuuden puutteeseen, tai sen vääränlaiseen käyttöön, sekä liian teknisen kielen käyttöön kohderyhmään nähden. Tässä tutkielmassa tarkastellaan myös visualisuuden merkittävyyttä johto- ja hallitustason kyberturvaraportoinnin yleisen kehityksen lisäksi.

Tässä tutkielmassa esitetään malli, jonka avulla voidaan luoda tehokas raportointimetodi johdon ja hallituksen kyberturvaraportoinnille. Esitetty malli tarjoaa uuden, iteratiivisen tavan toimivan raportointimetodin kehittämiseen, ja sen pitämiseen ajan tasalla.

Asiasanat: Kyberturvaraportointi, Kyberturvallisuus, Johto ja hallitus, Visuaalisuus

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Digitalization and advancing use of the Internet have been shaping the current world drastically. Internet is no longer only a research and communication tool, but it has been integrated in our everyday life and harnessed to provide convenience and efficiency in both individual and organizational level. Information systems and the Internet are part of governance and warfare, as well as they can be used by a single person to order groceries or to listen to music (Mir, Irshad & Bilal, 2018). At the same time security is becoming one of the most important topics in multiple areas of information technology (Schwab & Poujol, 2018).

Growing use of Internet using technology has increased the number of cyber security incidents worldwide(Mir, Irshad & Bilal, 2018), and it is believed that many companies are or will be compromised due to their poor cyber security reporting structure (Sharyo & Lin, 2019). The number of incidents is only expected to grow in the future; Cybercrime Magazine has stated that cybercrime is expected to cost the world 10.5 trillion US dollars annually by 2025 (Cybersecurity Ventures, 2020).

Cybercrime is developing and spreading to new areas, and different ways to attack known targets are being created constantly. The role of cyber security in organizations is becoming more and more relevant as cyber security measures need to be implanted to protect systems, devices, software, and data, and to ensure functionality of the business. (Shea, Gillis & Clark, 2021). To be able to maintain the cyber security of an organisation, it not only needs to be monitored and observed constantly, but also reported – the value of observation is lost if not communicated properly and used in decision making (Robinson, Jones, Janicke, Maglaras, 2018).

One has come to the realization that cybersecurity should and can no longer be the concern of just the IT department; everyone in the company needs to take part in it – including the management and the board. However, after multiple serious security breaches happening in the recent years, it became a common view that most boards are not prepared for the role of ensuring cybersecurity. The following question is, can an unprepared board be expected to determine the effectiveness of current and proposed cybersecurity strategies and know what to ask to make the right cybersecurity investment decisions? (Rothrock, Kaplan, Van der Oord, 2018)

Regardless of cyber security being an extremely important topic nowadays, it is still relatively rarely on the agenda of the board, while it should be brought up even briefly at every board meeting (Zeni, 2022) ~ (Deloitte, 2019). In addition, the topics reported to the boards and management often do not answer the questions the audience has, and do not prepare the boards and management for the actions they need to take (Cyentia Institute, 2018). Furthermore, there are often issues regarding communication on board and management level cyber security reporting: language used is too technical and visual tools are underrated, even when they are often what is needed to improve reporting (Vaught, 2022).

The motivation for this study comes from the recognised issue of reporting cyber security to boards and management in a way, that the report is understandable, interesting, has the right contents, is presented often enough, and prepares the boards and management for their role in the matter. This research is commissioned by OP Group, which is the largest finance group of Finland.

1.1 Research question and goals

The main research question of this study is based on the rising importance of reporting cyber security to boards and management, as well as on the recognised problem of reporting it ineffectively. In fact, according to a survey conducted by the Ponemon Institute, only 9% of security teams felt as they are highly effective in communicating security risks to the board and other C-suite executives. In addition, according to Sridhara (2020), it can also feel that it is impossible to effectively report and explain the workings and importance of the organisation's cyber risk program, when the audience views cybersecurity as a technical topic, that is difficult to understand. (Sridhara, 2020.) Based on the previous statements, the main research question of this study is:

- How can cyber security be reported effectively on board and management level?

In Addition, there are two sub-questions in this study, which are:

- What is the impact of visuality in board and management level cyber security reporting?

- How has cyber security reporting on board and management level evolved?

The first sub-question regarding the impact of visuality was chosen because visualisation is increasingly an essential element of business intelligence, and its significance in board and management level cyber security reporting has not been studied before (Eckerson, Hammond, 2011). The second research question was chosen to gain understanding of the life cycle of cyber security reporting on board and management level, and to form an idea of what it is now, and what it could be in the future.

The main goal of this study is to find a solution for the problem of reporting cyber security to boards and management ineffectively. To do so, this study aims to study how cyber security reporting to boards and management can be improved and made more effective. The methods and stages of the study are explained in the chapter **4 Research method**.

1.2 Scope and structure of thesis

In this thesis the main terminology is opened in the chapter 2, where cyber security reporting and management and board of directors are explained for this context. After this, the literature related to the subject is further opened. The literature is separated in the history of cyber security reporting on board and management level, and how it is done now. This should help to understand how cyber security reporting on board and management level has evolved to the state where it is now, and what are still generally recognised issues.

In chapter 4 the research method of the empirical part of this study is explained, divided in the sections data collection, data set, and data analysis. The data analysis explains in further details how the results and outcomes of this study have been formed.

The results are presented in chapter 5, where the interviews have been analysed and compared to literature. The results are divided into sections based on themes identified in the analysis process. An important mention is that unlike in most research papers in the field of information systems (IS), this study compares the results of the empirical study to existing literature already in the results-section. This is due the nature of the study, where context and comparison to literature provides a better understanding of the full picture, and how the findings of this study were formed, compared to if the results of the interviews were to be presented in a traditional way. The chosen structure allows the reader to form a more connected idea of the presented information, and therefore benefit from it better. The research method guidelines in the IS field have been criticized for not providing evidence of better outcomes or performance, and possibly prohibiting creativity (Siponen, Soliman & Holtkamp, 2021).

The discussion in chapter 6 explains how the research questions have been answered and presents the final outcome of this study. In addition, the contribution, limitations, and future research have been discussed. Chapter 7 briefly sums up the research and its outcomes.

2 TERMINOLOGY

To be able to study cyber security reporting on the management and board level, these concepts need to be taken under closer examination. In this chapter the terms *Cyber Security Reporting* and *Management & Board of Directors* will be defined to achieve an aligned understanding of what they mean in the context of this study.

2.1 Cyber Security Reporting

The definition of cyber security has changed over time and may still vary depending on the context. This section will be used to set a definition for the term "Cyber Security" in this study. We are going to briefly examine three different definitions and compare them to find the most suitable version for this study, in which the term cyber security is going to be used in the context of reporting. Reporting means giving a statement that describes an event or a situation as the result of observation (Dictionary, 2022).

IT Governance Ltd states on their website that *Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies*. (IT Governance Ltd, 2022). However, this definition excludes individual users, and feels rather vague. After all, multiple studies over the years have stated that cyber security has shifted from the predominant technical view to a more holistic definition (Craigen, Diakun-Thibault & Purse, 2014). It is viewed that in addition to technology there are multiple other aspects included in cyber security, such as users, environment, and organisation. (Schatz, Bashroush & Wall, 2017)

In their study, *Towards a More Representative definition of Cyber Security* (2017), Schatz, Bashroush and Wall proposed the following definition: *The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of* *safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users*. (Schatz, Bashroush & Wall, 2017). This definition has a more holistic approach and is quite like the definition that the International Telecommunication Union has stated on their website in the following way:

> "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity(which may include authenticity and non-repudiation), Confidentiality. " (ITU, 2022).

As stated before, the definition IT Governance Ltd has formed offers a very limited view on what cyber security includes. It fails to bring up the importance of people and their actions in cyber security, which is why the definition is not suitable for this study. Nevertheless, the definition might work well in a more technical study or matter. In the next examined definition Schatz, Bashroush & Wall have formed a very current overall concept for cyber security. However, the last definition, which is formed by the International Telecommunication Union, has very similar elements to the second definition but offers a more detailed view. Since cyber security is one of the core subjects of this study, a third definition, done by the International Telecommunication Union, was chosen because it offers the most pervasive concept for cyber security.

When talking about cyber security reporting in this study, it means the process where the person(s) responsible for the report completes at least the four following steps:

1. Gathers and analyses the relevant data regarding cyber security of the organisation
2. Transforms the analysed data in a presentable form
3. Delivers the report
4. Makes sure the presented information is actionable

When it comes to the step 4, the person responsible for the report must make sure that the people who receive the report are capable of making decisions based on it.

There are many variations on who reports cyber security to management and board of directors. CISO (Chief Information Security Officer), is an executive who is typically responsible for an organisation's information and data security (CSO, 2022). CISO may operate in the IT function and report to the CIO (Chief Information Officer), or they can report to the CRO (Chief Risk Officer).

In the previous models either the CIO or the CRO then report to the management and the board of directors. Under another model, the CISO reports to the management and maybe even the board of directors directly. (ISTARI, 2022). It must be noted that there may be different variations of the reporting models, depending on the organisation, their structure, and their needs. However, the ultimate accountability of cyber security of an organisation resides with the board of directors and the management (ISTARI, 2022), which is why it is important to make sure that cyber security reporting gives them enough understanding of the state of cyber security in their company and the world in general. Doing so ensures that board and management can act and make the right decisions when needed.

2.2 Management & Board of Directors

The base idea of this research is to study reporting cyber security to management and board of directors of organisations. This section will be used to examine the typical corporate structure, and to explain the roles and main differences of board of directors and management briefly. In Management and board level cyber security reporting the previously mentioned two entities are the receivers of the report.

Different organisations may have variations in their corporate structure, but the most common corporate governance consists of the three following entities: Management, Board of directors, and Shareholders. (Madhani, 2017). Shareholders are not very relevant to this study, so we shall just briefly introduce them as a person, organisation or company that holds at least one stock in a company in question (CFI, 2022).

It is important to note that management and board of directors are not the same group of people, although some members from the management team are sometimes members of the board as well. The board of directors is typically elected by the shareholders to represent them and their interest (CFI, 2022). A person who is a member of the board while being a full-time employee of the Company is called a **Management Board Member** (law Insider, 2022). There may also be other members of the board, outside the management, who work for the company daily. These people and management board members form a group of **Inside Directors**. Members of the board that are chosen externally and considered independent of the company are called **Outside Directors**. (Investopedia, 2022).

There are multiple theories, such as agency theory, stewardship theory, resource dependency theory and resource-based view (RBV), for defining what the roles of the management, and the board of directors are. To describe the best corporate governance practice, it is needed to use a combination of theories, since alone the theories cannot offer a solution for all times and situations, which may vary depending on the organisation. (Madhani, 2017). However, there seem to be key responsibilities that are realised in most organisations.

While management makes operational decisions and policies, board of directors approves major policies and makes major decisions (BoardEffect, 2022). Board of directors for example hires and fires senior executives, including the CEO. The board of directors is also responsible of maintaining company resources and making sure that the company is equipped with the tools it needs to be managed well. (CFI, 2022). It is the responsibility of management to keep the board of directors educated and bring them well-documented recommendations and information, so the board can oversee performance and make the important decisions (BoardEffect, 2022). Both the management and the board of directors are ultimately responsible for the cyber security of an organisation. (ISTARI, 2022),

3 LITERATURE REVIEW

This chapter is reserved for examining already existing literature about cyber security reporting to management and board of directors. First there is an overview of collecting the literature and perceptions of the existing literature. Later in this chapter there is a section for history of board and management level cyber security reporting, after which we will examine the most recent and still valid literature on the topic in the section "Board and management level cyber security reporting now".

The literature was searched from the following research databases: Google Scholar, Emerald insight, IEEE Xplore, ScienceDirect. Literature was also gathered from foundation- and organisational websites, that are widely acknowledged in the cyber security field. When searching for literature, the following key sentences were used: "management board cyber security reporting", "CISO reporting cyber security", "history cyber security reporting board management", "reporting cyber security management board future".

When searching for the literature, it shortly came to notice that there is not much public information about the subject. Especially academic research about the subject was very limited. Previous studies have mainly focused on the reporting hierarchy; to whom should the CISO report to. It was found that even when research was done on cyber security reporting structure, identifying the role of CISO, and recommending how to allocate duties and responsibilities, the study still lacked any recommendations on how the CISO should report (Shayo & Lin, 2019). However, to achieve an effective cyber security programme, board and executive management support and leadership is required (Geach, 2021), which is why this topic is very important and interesting.

One important source used in this literature review is the 2018 Cyber Balance Sheet Report done by Cyentia Institute, which includes research from different areas of cyber security. The research done on board- management level reporting and decision making, is used mostly in the section **3.2 Board and management level cyber security reporting now** (Cyentia Institute, 2018). The former Cyber Balance Sheet Report done in 2017 has also been used in the section 3.1 **History of board and management level cyber security reporting** (Cyentia Institute, 2017).

3.1 History of board and management level cyber security reporting

In the study done by Osterman Research, Inc., it was stated that reporting cyber security to the board was not what it should have been, and the board was not doing its job when it came to effectively managing cyber risk (Osterman research Inc, 2016). Board of directors had an overwhelming impression that no matter how much money they spent on security, they would still get breached (Cyentia Institute, 2017). While board- and management level reporting still needs to improve, it is important to examine the history of it to understand how it already has advanced.

In 2016 In 2013 Kwon, Ulmer & Wang studied the association between top management involvement and compensation and information security breaches. According to the study, when the CISO had a seat in the C-suite, organisational IT capability of the company was superior (Kwon, Ulmer & Wang, 2013). However, in a report done in 2016, Legrand (2016) found that while most businesses (85%) had someone chiefly responsible for their cyber security, only 58% of these were on the executive committee and 69% of these had other unrelated duties. In addition, 30% of the respondents reported that their board or executive team never receive reports of cyber threats to the company, and 46% reported that their board discusses cyber security rarely or never. (Legrand, 2016).

Cyentia Institute stated in their Cyber Balance Sheet 2017 report that management and board members had divergent views on the value of cybersecurity, how to measure and evaluate risk, and how to assess the effectiveness of information security projects. For the study they interviewed 50 CISOs, 25 Corporate board members and 10 subject matter experts. In the same study they also discovered that 46% of CISOs felt high confidence in their security controls, whereas amongst the board members only 5% expressed the same feeling. (Cyentia Institute, 2017). In the report done by Legrand (2016), it was found that 58% of respondents stated their board had a sufficient understanding of cyber risks (Legrand, 2016). Another report done in the same year stated that only one-third of IT and security executives believe their board understands the information about cyber security threats that is provided to them (Osterman research Inc, 2016). This may mean that some security executives reporting cyber security were not even aware of the lack of knowledge amongst their board and management. In fact, another study done in 2016 found that 90% of corporate executives said they are not capable of reading a cyber security report, nor are they prepared to handle a major attack (Rahdari, 2016).

According to the study done by Cyentia Institute (2017), CISOs tended to use technical jargon when reporting, instead of using business language, which would be more understandable for board members. (Cyentia Institute, 2017). In fact, vulnerabilities were the most reported topic and 81% of IT and security executives employed manually compiled spreadsheets to report data to the board (Osterman research Inc, 2016). Therefore, it can be interpreted that board members did not fully understand the content of the reports; hence they could not feel confidence in the state of their companies' security controls. (Cyentia Institute, 2017).

According to the study done by Cyentia institute (2017), board perspective was that they did not want to hear about the security, but the outcomes of security: does this help the business? What do we do that we did not do before? What do we eliminate? (Cyentia Institute, 2017). Still, the ability of security executives to report meaningful information to their boards was lacking, according to the study done in 2016. Instead, security executives tended to tell the board what they want to hear, regardless of the information not being actionable. This is interesting because the studies show that 74% of IT and security executives believed that their boards wanted reports with understandable language which did not require them to be cyber security experts. (Osterman research Inc, 2016). However, according to formerly presented information, security executives failed to deliver such reports, regardless of a high percentage of them knowing that reports without technical language were needed in board- and management level reporting.

In the Cyanite institute study (2017) there was a following CISO perspective: *"Lots of people say you have to dumb it down; that is a mistake. These board members are smart people. They do speak a different language, but they are not in another world, and we need to build a bridge."* However, as mentioned before, boards and management felt they did not understand the content of the reports, which shows that the more technical terms you want to use in your reports, the more you ought to orientate and train the audience to make sure they understand the language used.

In the report done in 2016, Legrand recommended that companies should discern and address low levels of cyber literacy amongst its executive teams (Legrand, 2016). Since then, more topics have been included into board- and management level cyber security reporting; for example, industrial cybersecurity developed into a board-level topic during 2017. (Schwab & Poujol, 2018).

3.2 Board and management level cyber security reporting now

As stated before, it is believed that poor cyber security reporting structure increases the risk of the occurrence of a cyber security breach (Shayo & Lin, 2019). Cyber security attacks pose a direct threat not only to business, but to personally identifiable data they hold. In addition, if a business were to fall under attack, the costs that come from restoring server status, reporting on any lost data, and upgrading defences to make sure the threat is mitigated in the future, could drain the yearly budget rapidly. (Zerlang, 2017)

To prevent the organisation from getting compromised, security culture across the organisation should be built upon proactive risk management and ability to recover from a cyber attack. To achieve this, the CISO should report and periodically update their boards about the cyber security situation in the organisation, especially cyber risks, and preparedness. Reporting should include assessing cyber capabilities realistically and comparing the organisation's security posture to its appetite and industry peers. (Geach, 2021).

For decades researchers have applied different kinds of algorithms that are based on machine learning and statistical methods to build better performing fault predictors, (Catal & Diri, 2009). Cybersecurity metrics can, for example, provide decision support and help measuring performance improvement and accountability for cybersecurity activities, therefore providing greater value to the organization (O'Reilly, Rigopoulos, et al., 2021). However, these metrics may not necessarily provide the absolute truth due to statistical errors. In general, statistical surveys do not aim to present the truth, but instead for example, statistical significance. In addition, in statistical methods and scientifical models there are typically hypotheses, which are wrong when taken literally. (Siponen & Klaavuniemi, 2021). In research focusing on statistical reporting in cyber security (2020), Thomas Groß states that statistically significant positive results are more likely to be published, than null results, regarding the fact that null results can have the same scientific rigor (Groß, 2020). There are also other statistical errors, which indicate that the metrics collected may be faulty; auditors often describe a failure to disprove the null hypothesis as an indication that the null hypothesis is true, and in some cases more than one data point is used per participant in a statistical test that assumes data points are independent. (Schechter, 2013).

In their 2018 Cyber Balance Sheet Report, Cyentia Institute conducted a study on what metrics are most often reported to the board (Figure 1), what metrics can be identified as top drivers of boardroom dialogue (Figure 2), and what metrics are most valuable to the board (Figure 3). (Cyentia Institute, 2018). According to the study respondents most frequently cited reporting security incidents and losses, while "What is the danger and are we safe?" is still a general question in board meetings. This can be related to the low confidence and high anxiety among directors, that Cyentia Institute observed in their previous study done in 2017. (Cyentia Institute, 2018). Another conclusion could be that the board members do not understand the metrics reported to them. However, according to the study done in 2019 based on interviews conducted with 200 CISOs in UK and USA, 96% either slightly or strongly agreed that senior executives have a better understanding of cyber security than they did five years ago (Help Net Security, 2019). The understanding of cyber security amongst boards and management has most likely increased after that.

Another interesting finding that Cyentia Institute made was that cyber risk appetite and exposure is one of the least-reported categories, despite the fact that in their previous study done in 2017, the interviewed board members ranked this category as the most important to them. (Cyentia Institute, 2018). The reason for this could possibly be either poor communication and CISOs not understanding what boards want and need, or that CISOs simply do not agree with boards when it comes to ranking the importance of reported categories. However, it must be noted, that the reason why boards rank some categories lower on importance, might also be the lack of understanding the category.

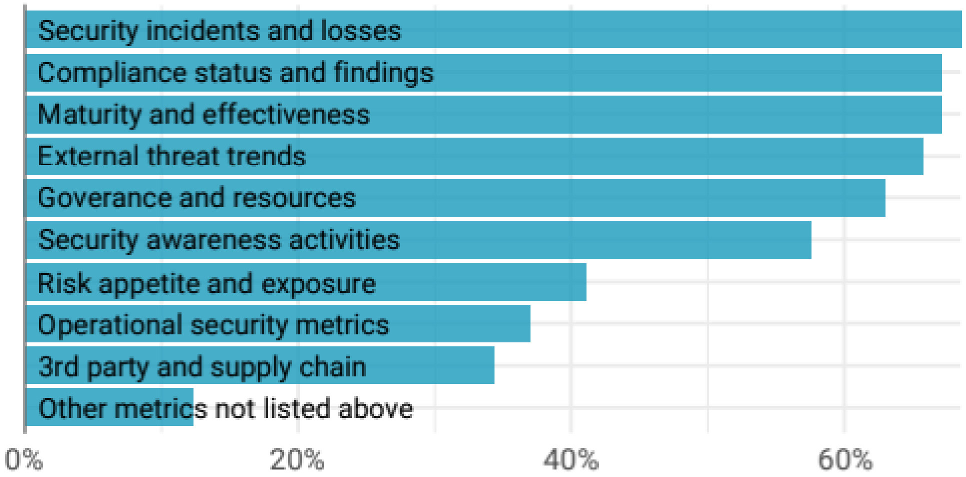


FIGURE 1 Metrics identified as most often reported to the board (Cyentia Institute, 2018).

One of the most common reporting numbers seen in board- and management level cybersecurity reports is the number of spam e-mails blocked. Another commonly reported metric is perimeter attacks blocked, which means the threats that hit the firewall. (Lindberg, 2020). However, these kinds of metrics do not reflect the cyber security state of the organisation on the level that the board and management need to view it. As one of the board members interviewed for Cyentia Institute's study (2018) summed up: "*Nobody cares how many packets your firewall blocked. If security reporting does not reflect business goals, you are doing it wrong*". (Cyentia Institute, 2018). Reporting on a large amount of spam messages blocked may in fact trick a board member into believing a false idea of staff training being less important because 99% of the spam messages are being blocked. Instead of reporting about spam messages, Lindberg (2020) states that one should report about employee cybersecurity awareness training results. (Lindberg, 2020). However, awareness training results may not necessarily be a good metric, unless they measure training shifting into operation. It is different to get a test right, compared to getting the same results in daily practical work. (Karjalainen & Siponen, 2011.) ~ (Puhakainen & Siponen, 2010).

The previously mentioned activity-focused metrics are very important when it comes to tracking day-to-day status and can be very useful to security teams and CISOs for demonstrating areas of strength or opportunities for improvement. However, they should not be the main item on the boardroom agenda. In general, board-level cyber reporting should be 'de-teched', since metrics that are useful to the cybersecurity organisation are not suitable for board-level reporting. Using Jargon and descending into irrelevance should be avoided. When reporting on management- and board level, it is best to consider not what the issue is, but what it means to the business tactically and strategically. Nevertheless, security metrics are difficult to translate into business terms, so the board reporting process itself can take weeks and may require many iterations. (Cyentia Institute, 2018).

In the study it was found that profit-seeking companies report maturity metrics most often, while public sector- and non-profit organisations focus on reporting about compliance. Even so, it is estimated that not reporting on maturity and effectiveness to the board may in fact weigh the organisation down. (Cyentia Institute, 2018).

Another factor worth mentioning found in the study done by Cyentia Institute, is that "3rd party and supply chain" is the last known category on the list of the categories reported to the board. It is mentioned that the researchers did not know what to expect since they did not include this category in their previous study but considering the number of public incidents tied to vendors, and the growth of services that monitor third-party risk, it was surprising to see it rank so low. However, it is hard to decide what this category should replace to move up, and the category may also be pushed down simply because not all organisations operate large supply chains. (Cyentia Institute, 2018).

In summary, metrics used in board- and management level reporting should be tied to business-level outcomes supported by the security program. All parties should participate in agreeing on the metrics, establishing thresholds and goals, and understanding what changes that come over time signify. In an ideal situation every movement and metric presented should have a meaning that can be used to support management decisions. (Cyentia Institute 2018).

Cyber reporting should enable discussion and dialogue, since adopting new technological innovations and capabilities may not only offer strong returns, but also increase cyber risk. Conscientious and comprehensive oversight at the board level is essential and requires more strategic dialogue with the management as well. (Clinton, Higgins, van der Oord, 2020).

In the study done by Cyentia Institute in 2018, comparing to the most reported categories, the most discussed categories rearranged quite a lot (Figure 2). It is still unclear if the amount of dialogue is linked to not getting enough information about certain categories from the report itself, or if the reports give enough information about the lesser discussed categories, leaving no need to discuss them. In summary, maximum airtime is given to incidents, threats, and risks, while operational minutiae and compliance create minimal discussion. (Cyentia Institute 2018). It may be that reporting about risks and external threat trends is difficult and even unreliable, since both academic and public knowledge of cyber conflict strongly relies on data from commercial threat reporting, meaning there are reasons to be concerned that the data provides a distorted view of cyber threat activity (Maschmeyer, Deibert & Lindsay, 2021).

When it comes to driving dialogue and value in the boardroom, organisations should consider maintaining records of boardroom discussions about cyber security and cyber risks. This helps staying informed on the industry-, region-, or sector-specific requirements that apply to the organisation. (Clinton, Higgins, van der Oord, 2020).

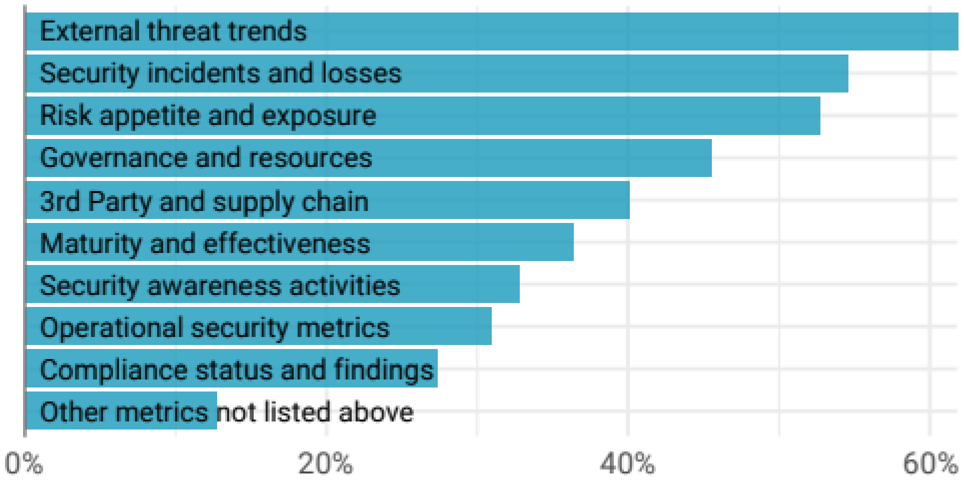


FIGURE 2 Metrics identified as top drivers of boardroom dialogue (Cyentia Institute, 2018).

In metrics identified as most valuable to the board (Figure 3), incidents and threats seem to top the list, as they do in most reported metrics (Figure 1). However, maturity metrics take a higher place on the list while risk exposure slides down. This is interesting since risk appetite and exposure creates more dialogue, according to Figure 2, yet holds comparatively less value. The reason could be that cyber risk is presented to the board in a way that is not satisfying to an audience who looks at risk more quantitatively and/or in a business context. (Cyentia Institute 2018).

It appears that boards place high value on both external and internal situational awareness, and on the fact whether their organisation has the capability to deal with it. Yet the metrics provided are often too technical and therefore not understandable to boards and management. This means boards and management also cannot link their meaning to business, therefore being unable to form opinions nor make decisions based on the provided information. (Cyentia Institute 2018).

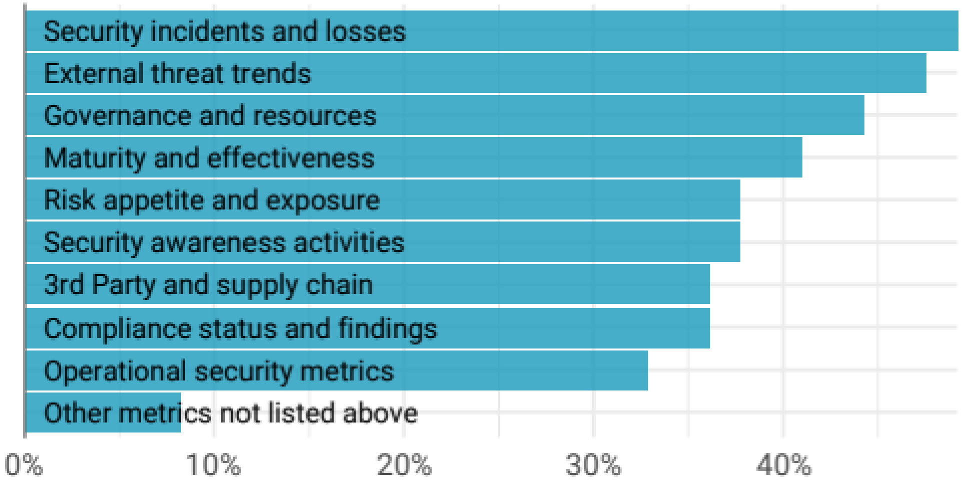


FIGURE 3 Metrics identified as most valuable to the board (Cyentia Institute, 2018).

To summarise and form better understanding of the previous three figures, Cyentia Institute has formed a figure comparing what metrics are most often reported to the board (Figure 1), what metrics can be identified as top drivers of boardroom dialogue (Figure 2), and what metrics are most valuable to the board (Figure 3). Compliance stands out as having low value and poor amount of dialogue compared to the reporting amount. The researchers reckon this may be because showing what has been achieved and done is easier than answering more complex questions of "have we done enough" and "what should be done next" regarding of them holding more importance and value. In addition, external threat trends, risk appetite and exposure, and 3rd party, and supply chain seem to be under-reported based on the amount of dialogue and the reported value. (Cyentia Institute 2018). Security executives should refrain from reporting on vain measures that only arouse emotions without driving real change (Zongo, 2021).

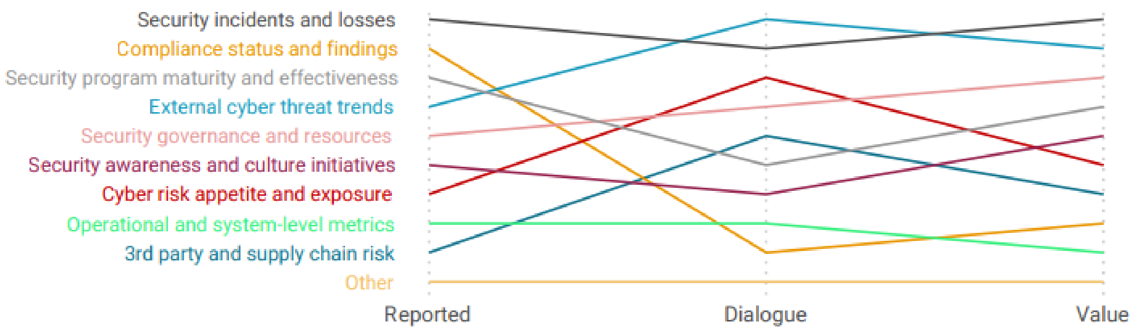


FIGURE 4 Comparison of how board-level cybersecurity metrics are reported, discussed, and valued. (Cyentia Institute, 2018).

What should the reporter focus on when choosing the metrics to report? Each organisation, and their board of directors and management are different and place value on different metrics. Risk-seeking firms seem to place higher value on awareness and operational metrics, while risk-averse organisations have great amount of dialogue on governance metrics. Private companies discuss plenty about governance and 3rd party metrics while putting more value on awareness. Dialogue and value in small businesses focuses on governance and operations. (Cyentia Institute 2018).

The security executive should pay attention on how the audience reacts during cybersecurity reporting; what prompts discussion, what questions are asked, and why are they asked. According to the study done by Cyentia Institute (2018), overall satisfaction with board-level cybersecurity reporting rates fairly high, over 40% reporting being very satisfied with the reporting. However, this may be because of the lack of knowledge; the board may not know what they want or need. The previous hypothesis can also be concluded from the fact that when measuring their *confidence* in security, the percentage drops to just a little over 20%. Nevertheless, the organisations that claimed high satisfaction with board-level cybersecurity reporting were more likely to include maturity and incident metrics, whereas less satisfied organisations reported about compliance and awareness more than anything else. (Cyentia Institute 2018).

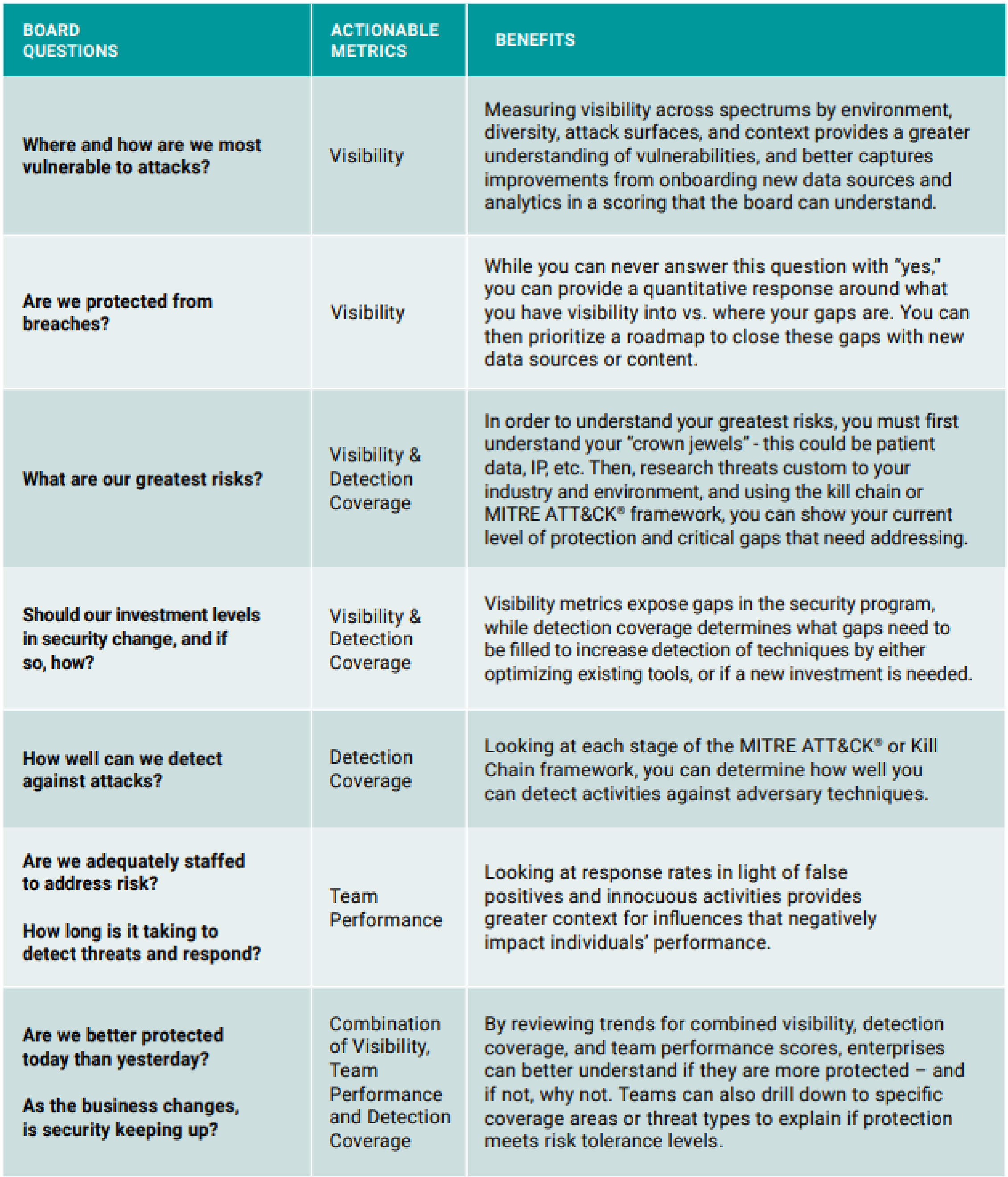
Traditional metrics fall short because they are centred on tools, they are not actionable, and they do not address people, processes, and technology. Such ineffective metrics are, for example, consumption-based metrics, ratio of alarms (open to closed), and number of vulnerabilities and patches. Consumption based metrics do not tell you if you are meeting or falling short of business or security objectives, even when they are easy to pull in from security tools. Metrics on ratio of alarms will likely give you an oversimplification of the true state of the security environment. Numbers of vulnerabilities and patches, however, are important to know, but do not convey a sense of your overall security posture without additional context. (Reliaquest, 2022).

In brief, the board wants to know whether the security of their organisation is managed or not, therefore detailed metrics are generally information overload. They want to better understand cyber risk, requiring a set of metrics that give a broad outline of posture and progress. According to the study, risk metrics were in fact the biggest relative difference between organisations with higher versus lower confidence levels. Instead of technical metrics and jargon, the security executive should provide simple metrics and information about benchmarks. (Cyentia Institute 2018). Unlike technical metrics, benchmarks are not a tangle of numbers, but an easy-to-read score. By using this single score, you ensure your time talking is spent on the aspects of security that matter, instead of explaining what your metrics mean. (SecurityScorecard, 2020).

There are, however, metrics that are recommended and seem to answer the questions the boards tend to ask. *Visibility* metrics are important to know if you have the right level of visibility into your environment. These metrics answer the common board room question like "Where and how are we most vulnerable to attacks?" and "Are we protected from breaches?". Many organisations seem to struggle to answer questions regarding visibility even if it is an important matter. (Reliaquest, 2022). Another important metric is *team performance*; How well does your team understand your environment, and where is your team spending its time? These metrics also tell how fast your team is resolving issues and are there any shortfalls in their analysis capabilities. The third important metric that is going to be mentioned is detection coverage. It helps you gauge how well you are protected against industry standard stages of an attack cycle. Based on many industry frameworks, such as NIST, MITRE, ATT&CK and CSF, it can be determined if you have the needed controls to get critical visibility into the threats concerning your business. From there use cases across your major detection controls (SIEM, EDR, UEBA) can be mapped to the previously mentioned frameworks to understand the types of attack techniques into which you have visibility.

Reliaquest has created a figure presenting the board questions, and metrics that deliver the answer in 2022. This figure is introduced in their paper *The CISO's guide to security metrics that matter in 2022* and presented in the following way:

TABLE 1 Board questions, and metrics that deliver the answer (Reliaquest, 2022).



BOARD QUESTIONS	ACTIONABLE METRICS	BENEFITS
Where and how are we most vulnerable to attacks?	Visibility	Measuring visibility across spectrums by environment, diversity, attack surfaces, and context provides a greater understanding of vulnerabilities, and better captures improvements from onboarding new data sources and analytics in a scoring that the board can understand.
Are we protected from breaches?	Visibility	While you can never answer this question with "yes," you can provide a quantitative response around what you have visibility into vs. where your gaps are. You can then prioritize a roadmap to close these gaps with new data sources or content.
What are our greatest risks?	Visibility & Detection Coverage	In order to understand your greatest risks, you must first understand your "crown jewels" - this could be patient data, IP, etc. Then, research threats custom to your industry and environment, and using the kill chain or MITRE ATT&CK® framework, you can show your current level of protection and critical gaps that need addressing.
Should our investment levels in security change, and if so, how?	Visibility & Detection Coverage	Visibility metrics expose gaps in the security program, while detection coverage determines what gaps need to be filled to increase detection of techniques by either optimizing existing tools, or if a new investment is needed.
How well can we detect against attacks?	Detection Coverage	Looking at each stage of the MITRE ATT&CK® or Kill Chain framework, you can determine how well you can detect activities against adversary techniques.
Are we adequately staffed to address risk? How long is it taking to detect threats and respond?	Team Performance	Looking at response rates in light of false positives and innocuous activities provides greater context for influences that negatively impact individuals' performance.
Are we better protected today than yesterday? As the business changes, is security keeping up?	Combination of Visibility, Team Performance and Detection Coverage	By reviewing trends for combined visibility, detection coverage, and team performance scores, enterprises can better understand if they are more protected – and if not, why not. Teams can also drill down to specific coverage areas or threat types to explain if protection meets risk tolerance levels.

In this figure we can see good examples of where the three previously recommended metrics can be used. These metrics are not too technical and do not provide information overload, but deliver explanations on the issues that the boards are interested in. Here we can see how, for example, on the question “Are we protected from breaches?” the answer can never be absolute “yes”, but instead visibility metrics allow security executives to show the existing gaps and to present a roadmap to close them. Presenting clear information and benchmarks in board and management level reporting helps them to better understand where resources are needed and what are the plans for the future. (Reliaquest, 2022).

In their study *Cyber Security Risk is a Board-Level Issue* Biljana Cerin has presented a list of activities that should be performed when preparing to structure a meaningful report for the board meeting:

1. review the existing information security risk register, risk mitigation activities and the status of associated cyber security controls
2. review the costs associated with previously materialized cyber security risks and gather relevant information to prepare the appropriate financial summary
3. review quantification of current unacceptable cyber security risks (in financial impact terms as possible)
4. review the established key risk indicators and determine trends to have better support for necessary early actions and mitigation actions
5. prepare the risk treatment plan proposal including necessary budgets, time frames, responsibilities and any other information that will help in receiving the necessary understanding and support of the Board members.

In addition to these activities, the security executives should also aim to efficiently present the major cyber security improvement projects and challenges, along with the current state of the cyber security program, its influence and efficiency, using objective metrics wherever possible.(Cerin, 2020). The security executives should also make it clear what actions they want the board to make: for example, to challenge specific positions or approve key decisions (Zongo, 2021).

It must also be noted that the boards and managements level of understanding of cyber security is not solely the CISOs burden; while it is not the responsibility of the board to become IT experts, they must still know what questions to ask the IT and security departments. (Cerin, 2020). According to Koivunen (2021), there are three questions he expects the board members to ask him whenever they get a chance:

1. What are the key threats against your top assets?
2. How do you protect your assets from cybersecurity threats?
3. Whose responsibility is it to implement protections?

   (Koivunen, 2021)

However, it must be noted that ideal questions for the board to ask may vary depending on the industry, how much understanding of cyber security the board members have, and what is the current situation of their organisation.

Regardless, these questions work as a fine example of how the board members should be active as well.

After all, boards and the management are the ones who must provide the leadership and the commitment necessary. (Cerin, 2020). The role of the board is to approve or disapprove the cyber resilience strategy instead of setting it (Zongo, 2021). National Association of Corporate Directors (NACD) has defined the following principles the responsible Boards should be driven by:

1. Boards should not approach cybersecurity as just an IT issue, but an enterprise-wide risk management issue

2. Boards need to understand the legal implications of cyber risks, as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas

4. Boards should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.

5. Board management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

   (Clinton, Higgins, van der Oord, 2020).

However, when it comes to executing these principles in practice, there are often issues that lay within the current capabilities of both the board members and the CISOs. One issue is that in some cases CISOs communicate with boards through the CEO. This means there is a need to identify a common language that both the board and the CISO understand. Another issue is the time reserved for cyber security in the board room; sometimes CISOs get as little as 10 minutes to present their report (Zongo, 2021). Presenting all the key factors and making sure the board understands them in such a short time is challenging.

Now corporate directors and senior management have begun requesting reports on the effectiveness of their cyber security risk management programs from independent third-party assessors, while well-integrated cyber security risk management frameworks should be able to deliver the adequate information. In conclusion, there is an issue in getting the most out of security risk management frameworks. (Cerin, 2020).

There are many popular frameworks, for example NIST SP 800-37 Rev. 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, which states that the risk management framework

> " Provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF includes activities to prepare organizations to execute the framework at appropriate risk management levels."

Regardless, these frameworks may not be flexible enough; many CISOs feel that documenting new types of risks is difficult, because they do not fit into a standardised, wider enterprise risk management framework. Implementation of the integration of a framework also significantly depends on the clear and full support from the upper management levels and cannot be perceived as just another "checklist". (Cerin, 2020). In addition, current frameworks and standards possess the classic weaknesses of standards and risk management. They are, for example, generic in scope, hence not providing methods tailored to environment and operations of each organisation. (Siponen & Willison, 2009). Baskerville also stated already in 1991, that future information systems are not predictable enough to allow standards to develop, like the accounting community (Baskerville, 1991).

In conclusion, the existing literature shows that reporting cyber security to boards and management has evolved through its history and shifted towards a more risk-based approach. Even when the boards and management now have a better understanding of cyber security than they did before, it has become a more prevalent view that technical metrics and jargon are not suitable, nor effective on reports for that level. Instead, the metrics should be and are becoming more focused on business-level outcomes, and they provide explanations on the issues that the audience on board and management level is interested in. Examples of those kind of metrics are presented earlier in Table 1. However, the metrics used, and other topics reported to the boards and management vary depending on the industry and size of the organisation. For example, as mentioned earlier, it has been found that profit-seeking companies focus on maturity while non-profit organisations report about compliance.

4 RESEARCH METHOD

This research was carried out by using a qualitative research method. Qualitative research methods were originally developed in the social sciences to allow researchers to study social and cultural phenomena (Myers, 1977). Qualitative research is usually selected when research is needed in relative new research areas, and the research seeks an answer for questions related to "what", "how", "when", or "where". (Basias, Pollalis, 2018). Qualitative research methods are optimal especially when exploring a new research area because they are more flexible than quantitative methods, therefore being more suitable for research where issues are not yet understood or properly identified (Hancock, Ockleford & Windridge, 2007). Since the research problem is relatively new and the goal of the study is to understand the subject on a deeper level, qualitative method offers the best possibilities in achieving the desired results.

It is important to note that separating qualitative and quantitative methods is philosophically problematic without providing sufficient definitions, since qualitative interview papers do not refrain from expressing information quantitatively (Siponen & Klaavuniemi, 2020). Regardless, when choosing a research method for this study, it was realised that using a *fully* quantitative method would not give the in-depth view that was needed to achieve the goal of this research (Basias, Pollalis, 2018; UoN, 2022). In addition, finding enough participants with expertise in management and board level cyber security reporting, for large quantitative research, would be highly challenging. Since a large data collection or a broad literature review would be required to use a mixed method, it was not suitable for this study either (Byrne & Humble, 2007).

The purpose of this research was to study cyber security reporting methods and practices, and to separate practices that are efficient or insufficient. The end goal was to find an answer to the main research question: *How can cyber security be reported effectively on board and management level?* Therefore, in this study data was collected by using a qualitative interview method. This method is not only beneficial in describing meanings of central themes in the life world of the subjects, but also allows one to get more in-depth information around the set questions (McNamara, 1999).

The interview method chosen for this study was semi-structured interview because it allows to get answers to questions about basic practices of cyber security reporting, while finding previously unknown trends and issues (Rahman, 2019). The semi-structured interview method can offer the advantages of both structured and unstructured interview methods. This method provides an opportunity to spontaneously explore topics relevant to that particulate candidate, while allowing the objective comparison of candidates. (Pollock, 2022).

As in every research method, there are some limitations and disadvantages. When using a qualitative research method, the research might be influenced by the attitude, culture, and ethos of a researcher (Eisner, 1991). Since semi-structured interviews require a large quantity of analysing transcripts, it is difficult to collect a large enough sample to present enough variety (Newcomer, Hatry, Wholey, 2015). The interviewer must also know how to formulate questions because of the interactive nature of communication in a way that the interviewees understand them in a similar way (Opdenakker, 2006). It must also be noted that because most of the interviewees work for a Finnish company and live in Finland, there may be a possibility of the culture affecting the processes and methods used in their cyber security reporting.

4.1 Data collection

The data collection process of this research was implemented between October 2021 and January 2022. It was determined that the interviewees should be people with a current or former CISO title, or that they would have strong expertise on cyber security reporting on the board and management level in other ways.

In October a survey was created using Google Forms, which was then shared in various communicating channels of cyber security specialist. The survey explained the nature of this research and had a field where willing participants could enter contact details of their choice. Interviewees were also searched via Linkedin, using "CISO" as the keyword. An invitation was then sent to the possible candidates. Both Finnish and international candidates were contacted. The invitations were sent either through Linkedin or e-mail.

The invitation was sent to 42 persons from which eighteen were interviewed. This means that 43 percent of the people who were contacted also participated in the interview. Fifteen participants were working as CISO:s in a Finnish company, and three were CISO:s in a foreign company. Nine of the eighteen companies operate internationally.

The structure of the interview was built based on the background of cyber security reporting, how the reporting has since evolved, and if there are any known changes in the future. The structure of the interview was also based on the existing literature, and on the areas, it did not yet cover. Thus, the interviews focused on the known issues, such as the level of understanding cyber security among board and management, as well as areas that have not been studied before, like visuality in board and management level cyber reporting. The questions were approved by both supervisors of this thesis. The goal of the questions was to understand the background and evolvement of cyber security reporting, and to find similarities and differences in similar fields.

The interview questions could be split in three different categories: background related questions, questions about the current situation, and questions related to the future and ideal situations. The background questions focused on finding what type of organisation is in question, how long and how have they been reporting about cyber security to the management and the board of directors, and how the reporting methods have changed and evolved into the current state.

Questions about the current situation focused on how cyber security reporting is done now. These questions circled around the currently used practices, reporting frequency, and how interested the board of directors and the management are in cyber security reporting. The goal of the questions in this section was also to find how the CISOs assure the quality of their report is satisfactory.

Future and ideal situations related questions were formed to understand how cyber security reporting might change in the future, and what is currently considered to be the ideal cyber security reporting situation. The questions consisted of such as "what could you improve in your cyber security reporting?", "what would you describe as an ideal cyber security reporting state without considering resource and budget issues?" and "what measures are you taking to get to your ideal state of cyber security reporting?"

4.2 Data set

The data set consists of people who were holding a CISO title, or a comparable title during the interview. In most cases the CISO of a company is the main responsible person when it comes to reporting cyber security to the management and the board of directors. Therefore, all interviewees can be considered experts in the area studied in this research.

As stated before, 18 persons were interviewed, consequently forming the sample of this research. 15 of these persons worked in a Finnish company. From these companies 6 operated internationally, while 9 operated only in Finland at the time. In two of the interviews the language was English, while the rest of the interviews were in Finnish. The CISO:s and the companies will remain anonymous, and only the industry of each company will be mentioned. Finland is a low population country, which is why some industries may only have a few different operators in there, hence some of the industries are displayed with a vaguer term to ensure the anonymity of the interviewees and the companies they work for.

CISO:s from outside Finland were contacted to get perspective from outside the Finnish reporting culture. In addition, CISO:s from different industries were contacted to get enough variation between interviewees. There is also one industry, Finance, which is represented by more companies than the other industries. This allows finding similarities in board and management level cyber security reporting between one industry. Of course, this must be done bearing in mind that the sample is rather small, which may reduce the reliability of the connected findings.

The industries of the companies where the CISO:s interviewed were working at the time are listed below in a table. The number of the companies representing the industries are also displayed. One of the interviewees did not represent any specific company, but answered the questions based on what would be ideal or has been proven to be the best method in their opinion. This is because of the nature of the company they work in, and their experience with multiple different companies in cyber security reporting. Therefore, the industry of this interview case has been marked as "unknown" in the table below.

TABLE 2 Industries and number of the interviewed companies

Industry	number of companies
Energy industry	**1**
Engineering and Service	**1**
Finance	**4**
Food and Drink industry	**1**
Gaming industry	**1**
Higher Education industry	**1**
Information Technology	**1**
Personnel Service	**1**
Public Administration	**2**
Retail	**1**
Software industry	**1**
Telecommunication	**1**
Transportation industry	**1**
Unknown	**1**

4.3 Data analysis

The data gathered from the interviews was analysed by utilizing a thematic analysis method, which is a qualitative analysis method. The focus of thematic analysis is to identify themes and patterns of living and/or behaviour (Aronson, 1995). Thematic analysis can be used to identify patterns not only within the data, but across it as well. The patterns can be identified in relation to participants' experience, views and perspectives, behaviour, and practices (Clarke, Braun, 2017). After the data has been collected, transcribed, and the patterns have been identified, the patterns can be listed. (Aronson, 1995). The listed themes provide a framework for organising and reporting the analytic observations (Clarke, Braun, 2017).

The phases of the data analysis of this study included the following steps:

1. Transcribing the interviews
2. Reading the material
3. Identifying repeating themes and patterns in the material
4. Placing data with the corresponding pattern
5. Cataloguing data into sub-themes
6. Finding observations
7. Reporting the results

In the first step, interviews were transcribed from a recording to text format. The transcribing process was carried out carefully, and the material was processed thoroughly, to make sure that the transcriptions were equivalent to the recordings. The second and the third step included reviewing the transcriptions and identifying repeating themes and patterns. The repeating patterns were identified and assembled in a text file, where they were further reviewed, and connected to larger main themes. The related data was placed to the themes, after which it was organised into a logical composition.

After the data was placed in the main themes, it was catalogued into subthemes where it was necessary for the sake of maintaining a clear and consistent structure. In the sixth step the data was deeper reviewed and analysed to find differences and similarities between the interviewees. The sixth step of data analysis also included comparing the differences and similarities to existing literature to strengthen the arguments behind the findings. In the final step the results were reported in the study.

In the data analysis the most used software during processing the transcriptions were Microsoft OneNote and Microsoft word. When data was processed further, Microsoft Excel was used in combination with the previously mentioned two.

In this study, eight themes were found when analysing the interviews. Four sub-themes were found under one of the main themes. All the themes and the sub-themes are presented in this study as following:

1. Evolution of cyber security reporting on board and management level
2. Frequency and target audience of cyber security reporting
3. Models and Frameworks
4. Contents and topics of the Report
    - 4.1 Roadmap
    - 4.2 Responsibility and taking ownership
    - 4.3 Risks, threats, incidents, and other challenges
    - 4.4 Metrics and other numbers
5. Interest and reaction
6. Level of understanding Cyber Security amongst boards and management
7. Significance of visuality
8. Using external help with the report

5 RESULTS

This chapter presents the results of the empirical study, also comparing it to already existing literature. First, we are going to look into when and how cyber security reporting on board and management level has evolved according to the 18 CISOs interviewed in this study. After this we are going to examine how often and to whom they report about cyber security. Then we are moving to discussion about models and frameworks, after which section 5.4 opens more what contents and topics are often reported amongst the interviewees.

Section 5.5 examines how interested the boards and management of the interviewees are, and section 5.6 talks about their level of understanding cyber security. Later on, we are going to study the significance of visuality, mirroring the answers gathered from the interviewees against literature. Lastly, section 5.8 briefly presents how external help is used in building the report.

5.1 Evolution of cyber security reporting on board and management level

In this section we are going to investigate results regarding how and whenboard as well as management level cyber security reporting has changed. The results show that the change has often spiked after significant cyber incidents. According to the interviews, the turning point for board and management reporting generally was in 2017, as almost all interviewees stated they noticed major change starting to happen around that time.

There were two specific incidents mentioned in the interviews that interviewees believe have influenced what board and management level cyber reporting has become. In addition, according to interviewee 17, another wave of change occurred when the General Data Protection Regulation (GDPR) was set.

The first incident is mentioned by Interviewee 17, who noticed change in increased interest in board and management level cyber reporting after a company called Moller-Maersk suffered a major cyber security incident. The cyber-attack was caused by the NotPetya malware, which affected many organisations globally. Moller-Maersk's operations in transport and logistics ended up getting disrupted, and the malware wiped out almost all online backups of the company's active directory. The incident happened in June of 2017. (Bannister, 2021).

The second incident was mentioned by several Finnish interviewees, who noticed a spike in interest after a Finnish company Vastaamo suffered from a security breach that came out in October 2020. The aspect compromised during the breach was the company's database, which the attacker got access to. The database included sensitive information about the customers of Vastaamo, such as their social security numbers and medical reports. The attacker demanded ransom from the customers after they stated the company had refrained from taking responsibility. The attacker claimed they had information of 40 000 people, and it is estimated that information of almost 32 000 people was leaked in Tor Network. (Hakoniemi, 2021).

Interviewee 16 says board and management level cyber security reporting has evolved a lot in five years; before there used to be more activity reporting, which means reporting activities done, such as the number of threats and attacks blocked. Now cyber security is seen as a risk discipline, which is why reports are now more focused on the outcomes rather than the activities. Interviewee 14 says their reporting has improved drastically in the last five years; they mention that reporting maturity has improved the most, and they have also added external threat map to their reports.

Interviewee 9 states their board and management level cyber security reporting has improved significantly in the past five years: they report more strictly and frequently, and the contents of the report have changed. Interviewee 7 says their board and management level cyber reporting has activated drastically in the past year. Before they have had issues with getting the topic to be a board and management level agenda, since the board and management were not so interested in cyber security. Now they say the interest has grown and keeps on growing continuously.

Interviewee 15 feels their reporting has improved a lot in the last five years, and especially in the last two years. They say their capability to report and highlight important facts has improved. Interviewee 15 states that even if their cyber security is in a good state now, it might take even six years for them to get to where they want to be.

Interviewee 6 feels their reporting has evolved a lot in the past two years. Interviewee 5 states they changed their board and management level cyber security reporting drastically in 2018, and it is still constantly evolving. Interviewee 1 states their reporting has evolved a lot in a sense that it used to be rather technical, including many metrics and charts, which the board and management did not have capacity to digest. Now they describe their report as a more strategic one. Interviewee 4 states their board and management level cyber security used to be part of general security reporting, but in the past three or four years it has become its own agenda. Interviewee 14 states they want to increase their capability in operational reporting, since now it is somewhat qualitative, but other than that they feel their reporting is on a good level.

In conclusion, all the interviewees felt that their board and management level cyber security reporting has improved and evolved during the recent years. However, none of the interviewees say that they would not change anything in their reporting. Even if it can be concluded that board and management level cyber security reporting is in a much better state now as it was five years ago, there is still room to improve much more.

When talking about enhancing already existing reporting practices, most interviewees said the obstacle to make the changes is resources and time. In the future, organisations may prioritize cyber security more: Interviewee 14 mentions they have already scheduled more time for cyber security in the future on top management level. According to many sources, cyber security is becoming the first priority in companies (FIIF, 2022), since it has become increasingly clear that boards and management must act in a direct way to avoid personal risk in addition to increasing cyber risks (DirectorPoint, 2022). Interviewee 16 believes cyber security is a top agenda item for most organisations already.

> “Serious cyberattack could basically wipe them out of business.” -Interviewee 16

Interviewee 16 states they believe that reporting evolves with the organisation as its cyber security capability matures.

> “When there is low level of maturity, the focus is typically very much on compliance obligations and on protecting the most critical assets with some key controls.” -Interviewee 16

They also mention that reporting shifts over time towards more sophisticated risk reporting, key risk indicators, cyber security capability and maturity.

Interviewee 2 believes that in the future cyber security reporting on board and management level will be more risk based. Research has shown that when boards consider environmental, social and governance (ESG) factors, companies that manage the entire portfolio of risks, do better in the marketplace (Gleason, Clinton, Joyce, Dobrygowski, 2021). Interviewee 2 also believes that the reports will focus more on the future rather than the past. Interviewee 1 however says future of cyber security is hard to measure, which is why reports of it tend to focus on the past. Regardless, since technology is constantly evolving and there is a recognised need for ways to measure what could happen in the future, it is not impossible that more reliable ways to do so can be developed.

5.2 Frequency and target audience of cyber security reporting

Two of the 18 interviewees did not answer the questions regarding reporting frequencies in their current situation, but instead gave recommendations. With their wide experience in many companies, interviewee 17 recommends ensuring reporting on operational level once a month, including outsourced services to ensure necessary transparency to security levels — It's not enough to have good contract, you need to also manage your suppliers and ensure close co-operation in operational level, including necessary transparency to security and privacy levels. Interviewee 16 says that there should typically be a monthly meeting of governance committee, and a quarterly or a bi-annual meeting with the senior executives and the board.

One finding that was made during analysing the interviews was that all four interviewees who worked in finance (interviewees 18, 14, 2, 7.), reported to their management quarterly. From all interviewees, 25.1% reported more frequently, 25.1% reported less frequently, and 12.5% reported as frequently to their management as all interviewees from finance industry. Interviewee 18 states they have a monthly meeting with the security and IT executives, and to the board and other management they report quarterly. Interviewee 14 says that in addition to the quarterly report to the management, they report once a year to the board. Interviewee 2 says they report about information security to the management at least once a year, and about risk focused cyber security quarterly. Interviewee 7 says the same quarterly report goes to their board as well.

Between companies whose business heavily relies on information technology, such as software industry, gaming industry, telecommunication and IT, there was no correlation found in how often they report to their boards and management. Interviewee 13 says they report once a month to the management, including the CEO, and have quite recently (two years ago) started to report to the board, doing so once a year. Interviewee 9 says they report to the management quarterly, and the same report goes to the board. Interviewee 5 says they report quarterly to the board, and monthly to the management. Interviewee 4 states they report to the board when asked. They do not have a formal schedule for reporting to the board, because before it was not seen necessary. However, recently their board has been more interested in cyber security, hence requesting a report for themselves occasionally. To the management interviewee 4 reports quarterly.

Amongst other interviewees there were no significant correlations regarding how often they report to their board and management. Interviewee 12 reports to the top management once a year formally and in addition more informally twice a year. Interviewees 15 says they report to the board once a year and to the management more frequently, approximately nine times a year. Interviewee 11 says they report to the top management twice a year. Interviewee

10 says they report to the management twice a year, and to the board when needed or if additionally asked. Interviewee 8 reports to the board and management formally twice a year, and informally more often when needed. Interviewee 6 reports to the management when needed, and to the board once a year. Interviewee 1 states they report to the management once a month, but that they also have a "situation room" for them, where there are different metrics that can be followed constantly. Interviewee 3 states reporting to the board and management is not yet a continuous practice in their organisation. They are hoping to make it one soon during the following year. Their board and management have already expressed interest in the topic.

The frequency of Reporting Cyber security to the management amongst 16 interviewees of this study has been visualised in Figure 5. As we can see, reporting quarterly is the most popular frequency among the interview partners of this research. Only single interviewees reported three or nine times a year, hence the small percentage. Section *Undefined* includes those who report when asked or needed, or who in other ways do not have a set schedule for reporting.

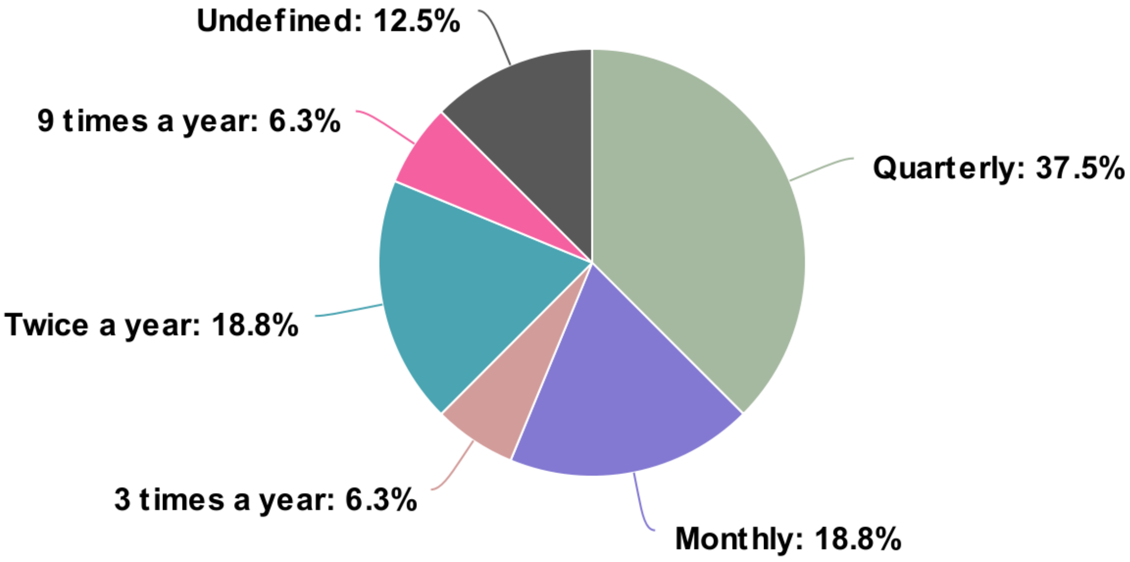


FIGURE 5 Frequency of reporting Cyber Security to the Management

Figure 6 is an adaptation of the figure "Frequency of Reporting Cyber Security Program Status to the Board " from an Osterman Research Survey Report. Their study was based on 136 completed data surveys, that were completed during December 2015 and January 2016. Figure 7 visualises the frequency of reporting cyber security to the board among the 16 interviewees of this research. It must be noted that the data set of this research is smaller compared to the Osterman research survey report. Therefore, we cannot make conclusions of how much the frequency of reporting cyber security to boards or management has changed since 2016. The figures are used to visualize how the reporting frequency of this data set compares to a larger study done a few years back.

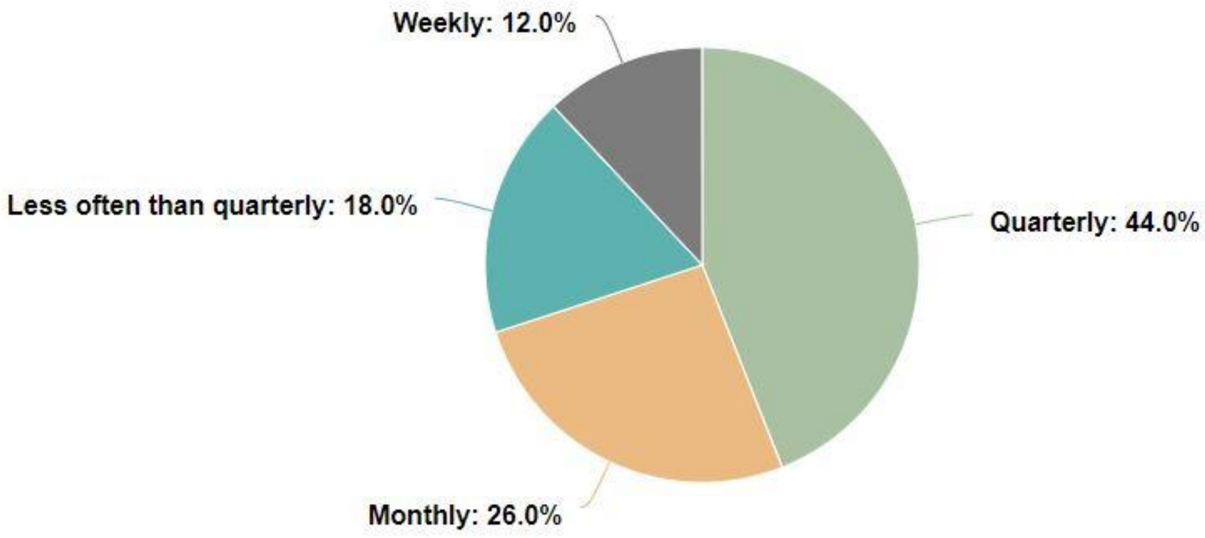


FIGURE 6 Adaptation of "Frequency of Reporting Cyber Security Program Status to the Board", (Osterman research Inc, 2016).

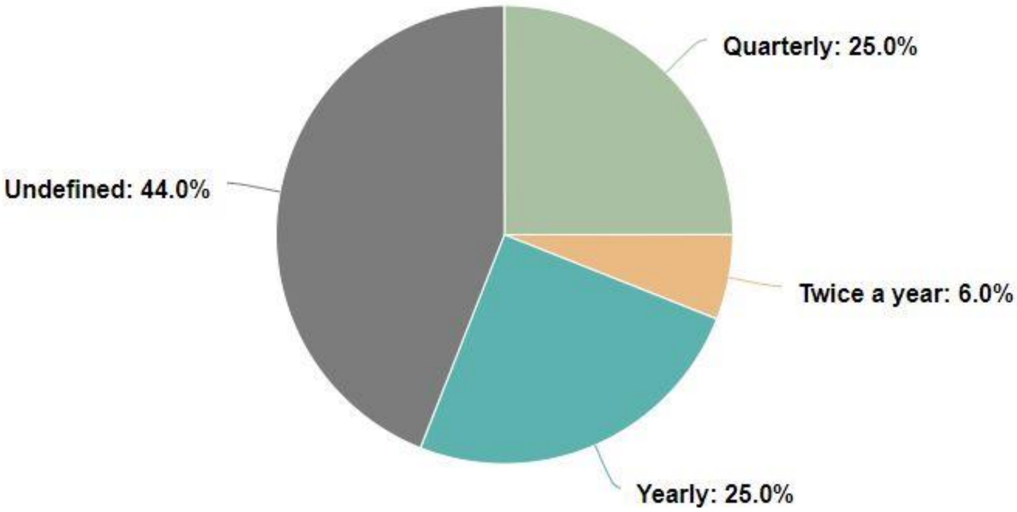


FIGURE 7 Frequency of reporting Cyber Security to the board

5.3 Models and Frameworks

When asking about models and framework, the opinions and practices used ranged widely. Some interviewees stated they benefitted from already existing models and frameworks, while other interviewees feel they are not flexible enough for their needs in reporting cyber security on board and management level. In this section we are going to examine different ways of using models and frameworks in reporting.

There were a few objects that rose up during the interviews recurrently when talking about models and frameworks. Gartner, an international company focusing on technological research and consulting, was mentioned frequently. Gartner offers, inter alia, materials and services regarding cyber security reporting. They offer free access to some of their materials, but to view certain research and to receive expert advice, toolkits, and diagnostics one needs to be a client. (Gartner, 2022).

The opinions regarding using Gartner varied amongst the interviewees. Interviewee 7 says they have benefitted from sparring with Gartner. They say it has helped them to gain understanding of how the reporting is done in other companies, and what they should include in their report. They have built their report model based on Gartner analyses. Interviewee 17 says Gartner analyses are one of the sources used when selecting providers for security operations. According to Interviewee 17, Gartner analyses give visibility to set of companies that have been selected as suppliers by others, but do not necessarily always tell which of them would suit the needs of your organisation best. In addition, the top list of the providers might also be too expensive for smaller companies. Interviewee 1 says they have used Gartner, but that those analyses and models are not suitable for board and management level reporting as they are.

Interviewee 5 says they have sparred with Gartner before but decided not to use their models as they are. Now they use a model/template they have created themselves. Interviewee 5 says their model focuses a lot on risk management. They have used many elements that are commonly used in the field, but describe the model has "their own look". Their goal is to additionally create a dashboard for the board and management level people, where they could get the latest picture of the cyber security state in their company. However, interviewee 5 states the downside would be lack of visuality:

> "It would be only a click of a button from Jira or somewhere, so it would never come out in a good condition." -Interviewee 5

In conclusion we can state that the analyses and other services Gartner offers, might not necessarily give the best option for your organisation. One of the interviewees claimed to have benefitted from Gartner, while the rest of the interviewees had either not used Gartner to begin with or had given it up at some point. While the materials and services Gartner offers may be highly useful at other points in managing IT and cyber security in organisations, general view during the interviews was that using Gartner is not efficient for board and management level cyber reporting. However, it must be noted that in this study all the companies that had experience with Gartner, were large companies. Therefore, there is a possibility that Gartner could be very useful to smaller organisations, but to confirm this, further studies would be needed. In addition, a few interviewees mention that smaller organisations could not most likely afford Gartner's services. All the interviewees who had experience with Gartner worked in different industries, so there was no causal connection between any industry and opinion on using Gartner.

NIST and ISO/IEC 27001 were also repeatedly mentioned when asking about using models and frameworks. NIST, as in National Institute of Standards and Technology, claims that their cybersecurity framework consists of standards, guidelines, and best practices to manage cybersecurity risk (NIST, 2022). ISO/IEC 27001 is a standard created by the International Organisation for standardisation. It is part of ISO/IEC 27000 family and is claimed to provide a model for setting up and operating an information security management system. (ISO, 2022).

Interviewee 16 says they prefer NIST framework as a fundamental framework, even though the framework itself is not quite comprehensive: the framework is light on, for example, risk management and cyber security culture. They state that frameworks are good in a sense that they provide consistency, but they are restrictive because there is not a framework yet that can answer all the key questions that boards and management have.

> "There is more what you need to report to boards than just what is in the NIST framework." -Interviewee 16

Interviewee 4 states they use a maturity model that is based on NIST standards. They feel it is easier to understand for people who have no cyber security expertise, comparing to, for example, ISO 27001 model. Their whole organisation is ISO 27000-certified, but they use elements from other models, when they find them beneficial. Interviewee 4 feels that ISO 27001 gives a very perfunctory view on certain topics, and they need a deeper angle on them. Interviewee 12 says they use ISO 27001 model in a formal report but talk about other topics outside the formal report. Interviewee 3 says they have recently adopted ISO 27001 to their reporting and are building a frame for their reporting practices based on it. They have also used a situational map model, which includes different metrics about how many incidents they have detected, and how well they have been able to react to them.

In addition to the three previously mentioned models and frameworks, Interviewee 17 adds they believe in adapting Kotter's Model of Change when doing cultural change inside an organisation. They add that it also helps to set expectations for cyber security implementations on board and management level, in addition to the rest of the company. According to interviewee 17, it takes time and requires not only investment in guidance and tools within the company, but also resourcing inside the business units. Kotter’s 8 step Model of Change is presented in the figure 8. Interviewee 17 highlights that it is not enough for the boards to state that cyber security is important to them at Step 1: Increase Urgency, but that they also realise it when the actions need to be taken, and prioritisation and resourcing are needed in the Step 5: Empower Action. Interviewee 17 says that continuous follow-up and expectation management is needed when the company is proceeding on their cyber security journey.

> “We must gradually tell them (the management) how we are proceeding on our journey with clear expectations on a role-based approach, and that we have different kinds of expectations for different roles within the company, especially the teams responsible for IT solutions, services, and products. We should inform the management realistically about whether we have enough resources in place.” -Interviewee 17

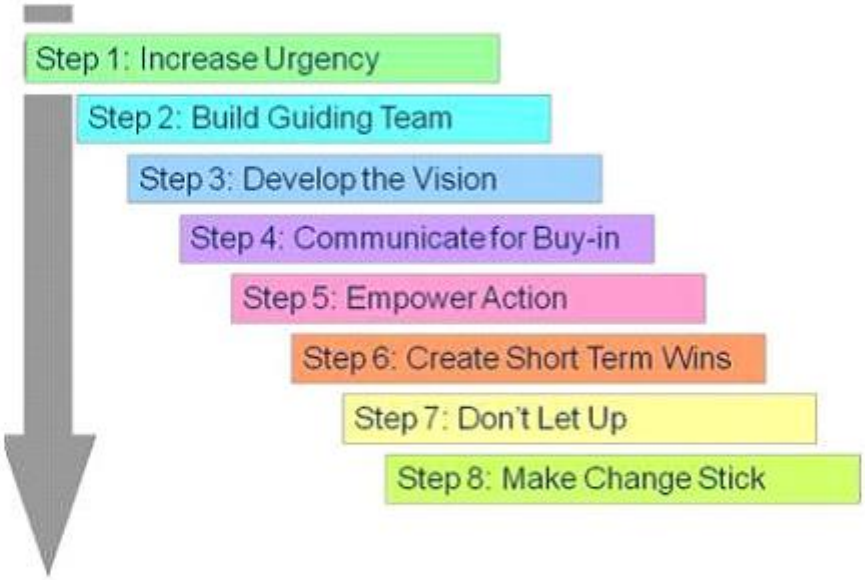

Step 1: Increase Urgency
Step 2: Build Guiding Team
Step 3: Develop the Vision
Step 4: Communicate for Buy-in
Step 5: Empower Action
Step 6: Create Short Term Wins
Step 7: Don’t Let Up
Step 8: Make Change Stick

FIGURE 8 Kotter's 9 step Model of Change, Adapted from Kotter 1996 (Management study guide, 2022)

Most of the interviewees found currently existing models and frameworks at least somewhat restrictive. Interviewee 7 believes standardized frameworks are rarely flexible enough for modern reporting on board and management level, and interviewee 9 states frameworks do not show the full picture, and that they find frameworks restricting. As stated earlier, Interviewee 16 believes there is none of the existing frameworks can answer all the key questions that boards and management have. While many interviewees stated to have adopted at least some parts of the already existing models and frameworks, some of the interviewees said they do not use them at all. Instead, they have either created their own, or report different topics depending on the situation.

Interviewee 10 states they have used a more informal model when reporting, but after they updated their cyber security management system, and the regulation changed, they formalised their reporting model. Interviewee 9 says they use a template, that can easily be edited. It includes a model they have used for two years. Interviewee 6 says they have started to use a reporting model, but the model changes continuously because they are still trying to find what works for them. Interviewee 14 says they do not use any specific reporting models but have adopted some parts of previous reports that seemed to have worked for them. They say they haven taken the approach to try to report about what is relevant to the board and management at certain times.

Interviewees 15 and 11 say that instead of using already existing or organisational frameworks and models, they report about thematic topics. Interviewee 15 adds that these thematic topics have certain repeating elements, but also changing ones. They state there is not one specific existing framework that would work for every board and management level cyber security reporting situation.

5.4 Contents and topics of the Report

This section presents the topics and contents that interviewees stated is relevant to report or avoid reporting. Many topics are overlapping, which is why, for example, risk and incidents are mentioned in the **Metrics and other numbers** - section, even though they have their own section as well.

In this study it was found that while similar topics were reported in different organisations, sometimes the opinion on certain topic varied drastically. For example, maturity metrics were considered very useful according to some interviewees, while some stated they are not based on evidence, thus are not a good metric to use.

5.4.1 Roadmap

Some interviewees said they report a roadmap of their cyber security to the board and management. Interviewees 18 and 4 say they include a roadmap in their report. Interviewee 18 tells the roadmap consists of their situation, including last strategy and the current one, their achievements, threats and are they prepared for them, what has changed, and where they may be delayed. Interviewees 14 and 8 also highlight the importance of reporting achievements, and Interviewee 8 adds it is important not to report only about the negative issues.

Interviewee 4 highlights the importance of reporting benchmarks. Interviewee 5 says that they report about what they have learned in their cyber security journey. Interviewee 14 says they also show a situational map, where all business units are lined up. Interviewee 7 reports what they have done in the past, measures, and trends. Interviewee 10 tells they report to the management a roadmap, and about risks and money. They state they use reporting method, which combines risks, threat landscape, current state, money, estimations, currents, losses, roadmap, action points, implemented, decisions and long yardage.

Interviewee 15 on the other hand says that a roadmap did not work for them, and they left it out of the report. They say it was hard for the audience to understand and relate to it. Instead, interviewee 15 says they have evolved into reporting more thematic subject and adopting Objectives and key results (OKR) -thinking. They state their focus areas are clear now and it is easier to compare the previous reports to the current ones as well.

Reporting a roadmap is also recommended by Reliaquest in their paper "The CISO's Guide to Metrics That Matter in 2022". You can either build a roadmap to explain multiple phenomena, or to present how you are, for example, planning on closing the existing gaps you have in your security. When building a roadmap, one should include peers across the organisation early in the process. This ensures alignment and foster trust. (Reliaquest, 2022).

5.4.2 Responsibility and taking ownership

When talking about responsibility in this section, it means a **social responsibility**. The definition for social responsibility is that businesses produce goods and services in a way that is not harmful to society or the environment. Ethicality is also mentioned along with social responsibility. When a company operates ethically, it means doing so in a way that tries not to cause social or environmental harm. Taking ownership, however, means a situation where someone takes a responsibility for an idea or problem. (Cambridge Dictionary, 2022). In the context of this study, it can be seen as the situation where someone must take the responsibility of the internal cyber security challenges in the organisation. During the interviews social responsibility and taking ownership of challenges were often brought up in the same context, which is why they are presented under one section in this study.

Being socially responsible and ethical is important, and are a big topic now, according to interviewee 17. In recent years corporate social responsibility has become one of the major concerns for many organisations (Hyun, Yang, Jung & Hong, 2016). Interviewee 4 also states adding a story of being socially responsible is becoming more popular in reporting cyber security to the board.

> "However, it is not enough to say that "we are responsible", but one also must explain how they are being responsible." -Interviewee 17

Interviewee 7 says social responsibility is a topic they are trying to highlight in their reporting besides information security. They believe it is a trend now, especially amongst younger people. Interviewee 6 highlights ethicality and reporting about it. Interviewee 15 says they like to highlight being socially responsible, and talk about the benefits of cyber security, but sometimes it feels like they should be able to bring up their challenges more.

> “Definitely not in a way that we would point fingers at anyone, but if we put business units’ side to side, none of them would want to be the last, and they would work on their challenges before next year”. -Interviewee 15

Interviewee 4 says that if they only showed their risk metrics without naming where they locate, the management might only look at them and say: “looks bad, what are you going to do about it?”. However, if they show what risks belong to which business unit, the person accountable for the unit feels a larger need to improve their situation, especially if the person sitting next to them has less risks.

> “No one wants to take ownership for something that has not been designated to anyone.” -Interviewee 4

5.4.3 Risks, threats, incidents, and other challenges

In this section we are going to examine what interviewees stated to report about risks, threats, and incidents. In this context cyber security risk means an uncertain effect within information and technology, which relates to the loss of confidentiality, integrity, or availability of data and information systems, and reflects potential adverse impacts to organisational operations. Threat means any circumstance or event, which has the potential to adversely impact the operations, assets, or individuals of the organisation through an information system. Incident is defined as being a cyber security event that has been determined to have the kind of impact on the organisation that needs response and recovery. (NIST, 2022). In this section we will examine both incidents the organisation in question has faced, and incidents happening worldwide.

As mentioned before, Interviewee 16 states they believe that reporting evolves with the organisation as its cyber security capability matures. They believe that when the maturity level of cyber security in the organisation is low, they focus typically on reporting compliance obligations and protecting the most critical assets with key controls. However, when maturity increases, reporting shifts towards more sophisticated risk reporting, key risk indicators, cyber security capability and maturity.

Interviewee 17 states that management and boards are busy, therefore they have no time to read up on what happens to companies who suffer from security breaches. Nevertheless, they may not know about the situation unless you explain it to them.

> “It is important to make sure that the board and management know what is happening around the world, what is relevant for their business area, and that they understand that similar incidents can happen to their companies too. However, you should always be up to date about existing threat landscape and able to explain *why* it may happen to you too, and what you have done to prevent it.” -Interviewee 17

Interviewee 17 also says that nowadays cybersecurity is an important topic on the news, which is why boards and management are more exposed to hear about security incidents in other companies more than before, and might ask questions, such as "what does this mean to us?" and "what have we done to prevent this happening in our organisation?". It is the cyber security executive's responsibility to be able to answer these questions and explain if the threat is relevant to them too, and if relevant, what they have done to prevent it.

Interviewee 4 says they report operations, goals, incidents, and threats. They do not report about individual vulnerabilities, but about phenomenon and issues on a wider scale. They report about incidents and trends worldwide and evaluate how close these incidents are to their business. Interviewee 12 however brings up that evaluating relevance of external trends and incidents that happen in other organisations, is challenging. It is hard to evaluate the impact on their organisation, and when it becomes a board or management level topic.

Interviewee 3 says they focus on risks in the industry, giving the risks a context. They explain what the high-level risks are and where they may need actions from the management. Interviewee 3 believes that without giving proper context, the data will only confuse the audience. Interviewee 18 says they include one "panic slide" but not more. In this panic slide they report about the challenges they have, and what incidents have happened in the same industry recently.

Interviewee 12 states they report about changes in operational environment, situation in documentation and risk management. They also estimate the information security objectives and issues and talk about current phenomenon. Interviewee 5 says their report focuses a lot on risks and managing them, information security, cyber hygiene, and areas that need to improve. Interviewee 5 says it is not a secret that they have three crucial threat scenarios, against which they mirror the report. Interviewee 1 says they that they report about disturbances in their cyber security, security training of their staff and predictions for the next season. Interviewee 8 says they report about the situation of their company's cyber security compared to other companies of the same industry. Interviewee 8 says they also report about their operating models, responsibilities, technology resources and focus areas. Interviewee 11 says they report only very general level statistics and metrics, for example about anomalies in information security. They do not report risks or risk evaluation but are hoping to do so in the future.

Interviewee 7 states they report about their risk profile and focus areas that need to improve. Interviewee 18 says talking about budget and resources openly is important; you should clearly address what risks you can address and mitigate for the budget, how a change in budget could affect the resources, and where the money will be used. Interviewee 8 says they address the budget widely, comparing the balance, and has the budget been enough, or should the company invest more money in cyber security next year. They say it is important to know what is included in the budget and how big the budget is compared to the "neighbour" company.

According to few interviewees, while you must give a realistic view of your challenges, you do not have to do that using fear. Interviewee 18 reminds that you should not spread panic, but still be transparent about the issues you have, and the issues companies around you have. Interviewee 7 underlines that they have been trying to "sell" cyber security to the board and management through positive outcomes, rather than fear and worst-case scenarios. Interviewee 6 follows the same line, stating that they do not want to threaten the board and management with possible sanctions. However, they tell what the reality is, and how they can protect themselves from the existing threats. Interviewee 14 states specialists often say that "humans are the weakest link in cyber security", but they(interviewee 14) prefer talking about the fact that humans can be a great factor in protecting cyber security. Interviewee 4 states it is important to display the negative issues in a way that it does not send a message that everything is failing. They say the message needs to be formed into something like:

> "We are looking at phenomenon we are not quite prepared to. We need to add stakes to this, and I need your support to do so." -Interviewee 4

Interviewee 17 states that if you only bring up problems without having solutions to them, you cannot expect any reaction or action from the board and the management. That is why it is important to consider the language used in the report to ensure it is understandable for the business as well. You must be able to explain the impact to the business, instead of just laying out the problem, or scaring them unnecessarily. Interviewee 14 also underlines the importance of presenting relevant topics and therefore relevant issues, that the board and management can have an impact on. In addition, there should be logic behind every reported aspect, explaining why it is relevant.

Interviewee 9 states they have been reporting about cyber security to the board and management very intensely recently, especially about their lack of resources in cyber security since that is a current issue in their organisation. They feel their perception is on lower level than it used to be, which brings more challenges and incidents to report about. However, they feel they are changing and going in the good direction, hence one can assume that reporting has been effective. Interviewee 9 says they report trend charts, that include trends even from 20 years ago. Another important subject in their reports are reputational risk and situational map. Interviewee 8 states calculating reputational risk is difficult, but important.

Interviewee 3 says their board and management are very interested in the financial impact of risks. Interviewee 17 states it is important to present business impact when talking about risks and threats. For example, denial of service attack (DOS) is a cybersecurity threat, which might lead to downtime of service, if the resilience of the service was not possible to keep remained. Cyber security experts might end up raising cybersecurity threats and root causes instead of the real risks to business. In practice real risks to business are the downtime of certain services critical to business, which causes loss of sales and/or stops production line. In this kind of situation critical vulnerability in the system is a cyber security threat, and if vulnerability is used, leading to a cyber attack, it becomes the root cause for the respective security incident.

> "The issue often is that we talk about the threats and their root, instead of the risk it causes to the business, which is more understandable to the audience in question." -Interviewee 17

They believe this is one of the biggest stumbling blocks when it comes to communicating with boards and management. They believe a solution how much it costs if certain service is down because of a cyber attack. This is further explained and talked about in section **5.4.4 Metrics and other numbers.**

In conclusion all of the interviewees stated to report about risks, threats or/and incidents to their board and management at least to some extent. Multiple methods of doing so came up, but many interviewees highlighted that instead of making the situation look scary and tragic, the risks, threats and incidents should be presented realistically, with the suggestions to improve them.

5.4.4 Metrics and other numbers

According to Reliaquest (2022), when relevant security metrics are packaged with the right communication strategy, they can be a powerful tool for CISOs to better highlight their current security program and roadmap improvements (Reliaquest, 2022). Most of the interviewees have stated to report even some sort of metrics to their management and board. However, interviewee 6 says they report numbers very little. Instead, they present risks verbally. Interviewee 2 says they use some metrics and numbers but prefer to present the board and management level report verbally, like telling a story. Interviewee 1 says that their experience is that if you report many charts which may be difficult to understand, the audience will not read them.

Interviewee 14 states using numbers has worked for them well, and their board and management level cyber reporting has improved significantly, especially since they started reporting numbers concerning each business unit. Nevertheless, they underline the fact that the numbers should be accurate, and the only way to make sure they are, is to work on them frequently. Interviewee 14 also states that if the numbers come straight from a system or scanner, they may be a good start but are most likely not accurate and therefore cannot be used. Interviewee 13 states most of the numbers they report to their management, come from previously mentioned systems. They in fact have had comments from the management that the metrics are not 100% trustworthy, and therefore it must be taken under consideration, whether some of them should be completely left out of the report. On board level interviewee 13 does not report metrics, but instead they describe quality of their cyber security.

Interviewee 17 says board and management like to see maturity metrics when reporting cyber security, but those metrics do not necessarily tell anything about your cyber capability. Interviewee 17 says that maturity metrics and certificates may tell what kind of capability you *should* possess but, the implementation of the operations is what matters in the end. In addition, legislation has a much slower pace than new evolving technologies, which means being compliant does not guarantee that you are cyber capable and resilient. Interviewee 17 thinks boards and managements may want to see maturity and compliance metrics because it is something they are used to seeing in other reporting areas. Interviewee 7 however states maturity metrics offer an easy way to demonstrate current situation, and how much money and resources are needed to get to the next level. Many other interviewees stated to use maturity metrics too.

Interviewee 18 says when it comes to metrics, they only report high level metrics to top management; for example, how many people have done the awareness training, how many incidents they have had, or how many risks are being accepted. To the board they report only vulnerabilities, which they state are also hard to explain on the board level. Interviewee 15 says boards and management are used to tracking numbers, which is why using metrics is not going to upset them. However, the issue lies in the fact that they do not know what good or normal looks like, because they might only have six months worth of previously reported metrics. Interviewee 14 also highlights the importance of knowing what the previous metrics have looked like, because presenting only one report would not tell anything about the whole story, and conclusions could not be made.

Interviewee 16 believes in reporting metrics and using numbers even if they are not entirely accurate at first. However, in this situation it should be made clear to the audience that the accuracy of the metrics is faulty. Interviewee 16 believes the numbers will get more accurate over time, and in the beginning, they at least give visibility over the issue. Interviewee 18 on the other hand does not believe in reporting numbers, because they tried doing so with the FAIR model, but it was hard to justify those numbers if you got challenged. FAIR is a model that codifies and monetizes risks by identifying and defining the parts that make up risk, and their relationship to one another (O’Reilly, 2019). Interviewee 18 adds that if the numbers prove to be incorrect, it would be hard for the audience to trust them anymore. Therefore, they state the numbers should be traceable and really accurate, if one were to present them. Interviewee 17 also says the audience on board level often raises a request for quantitative metrics. However, their maturity might be on such an early stage, that the only metric they can follow is the progress of implementation projects, which in future will give more accurate visibility to cybersecurity level.

Interviewee 6 states they do not believe in reporting numbers because the following question is “what are you going to do about it?”, and if it does not require decision making on the board and management level, it only burdens them. However, it must be noted that the organisation of interviewee 6 is not as dependent on information technology as for example, financial institutions or IT companies are, which is why metrics may not be a board or management level issue for them.

Interviewee 15 says information technology metrics are not relevant when reporting cyber security on board and management level. However, as stated before, maturity metrics on the other hand are a popular topic to report to board and management.

> “There are many different metrics you could use to report about your cyber security, but the question is what is the limit for your audience.” – Interviewee 3

Interviewee 8 says they follow certain metrics monthly and use the same metrics when reporting on board and management level, to show that they are not playing with different numbers in everyday work versus what they want to show to the board and management people. Interviewee 5 states they report metrics of security breaches, their amount and severity, and the reasons why they happen. They also evaluate if the risk is relevant to them. Interviewee 5 also says they report for example results from their phishing simulation which they use in their organisation.

Interviewee 5 states it is important that the audience knows what good or bad metrics look like for the CISO to be able to present them. They state their board and management know what the metrics presented mean, and what good metrics look like especially in their company. However, interviewee 5 says the cyber security metrics are currently still undeveloped.

As mentioned in the risk section, Interviewee 17 says that often CISOs talk about the root cause of a risk, instead of telling what it means to the business. Interviewee 17 believes a solution could be as simple as evaluating how much it costs if certain service is down for one hour because of a cyber attack. They state the business manager of each business unit should be able to evaluate the cost of their service being down for an hour, regardless the cause. Cost figures help people on board and management level to understand the actual risk to business, rather than just describing the root cause. Interviewee 17 adds that naturally, everything cannot be estimated with cost figures, such as possible brand damage, but cost figures are recommended to be used whenever possible. Interviewee 8, on the other hand, says that evaluating the cost of the service being down can vary for many companies, depending on many factors. For example, for some companies the cost may be linked to different seasons of year or the time of the day. In these situations, using numbers to present the financial impact can be tricky. Interviewee 3 also adds that it is difficult to estimate the cost of risk, especially if one should estimate the financial losses that come from lowered reputation.

Interviewee 17 says one cannot evaluate business impact unless they discuss with the business unit. The best is to communicate with the business unit and to agree together what you are going to report about their situation to top management and the board. Therefore, it can be avoided that a business unit is not prepared to answer something that has been informed to the board and management. Interviewee 16 believes it is relatively easy to calculate the impact cyber attacks could have on business but quantifying how likely something would happen is difficult.

Interviewee 15 states using numbers when talking about risks and business impact has worked for them. Interviewee 11 says they do not use numbers to describe possible financial losses but thinks it might be a good way to wake the audience. Interviewee 14 on the other hand states they do not use numbers that describe financial losses, but present other statistics, such as organised cyber crime. Interviewee 4 states that whenever presenting numbers that express money, you must be ultimately sure that you can stand behind those numbers.

> "Even if they would not understand the rest, these people (board and management) stick to the numbers, and they are very good with numbers." -Interviewee 4

When analysing the interviews, it was noticed that using numbers to describe financial losses was more common in companies that offered separate purchases or services (for example, retail or food and drink industry), than in companies that had a continuous contract or agreement with their customers (for example, finance or higher education industry). Overall, the opinions on using metrics and numbers varied drastically.

In the literature review we examined metrics that are recommended, most reported, and most valued by the board. According to the studies done before, the metrics provided are often too technical and therefore not understandable to boards and management. Not understanding what is being reported to them, prevents the board and management from making important decisions. As mentioned before, the board wants to know whether the security of their organisation is managed or not, therefore detailed metrics are generally information overload. (Cyentia Institute 2018). Most of the interviewees of this study agreed on this, but still some use relatively technical metrics, that they use among their cyber security teams. Of course, depending on the organisation and the level of understanding their board and management has, in some situation these type of metrics might work even on the c-suite level reporting. But at this point it is safe to make the conclusion, that these metrics are far from optimal in most cases.

5.5 Interest and reaction

An important factor when reporting is the interest and attitude of the board and management. Without the audience being interested in the topic, is hard to present something and actually get the agenda through to them. Many articles and papers published during the past few years, such as “6 ways to spur cybersecurity board engagement” and “Why Some Board Directors Still Don't Take Cybersecurity Seriously”, tell that even when the interest rate may be constantly rising, there is still work to do. (Irei, 2021). ~ (Price, 2018). In fact, according to the survey done by PwC (2019), less than 63% of boards acknowledged giving cybersecurity enough attention on their board agendas (PwC, 2019).

In this section we are going to examine how interested their boards and management are according to the interviewees. In addition, we are going to look into the reactions the previously mentioned audience tend to have; do they comment on the report, or even give suggestions on how to improve it? Do they make the needed decisions? Interviewee 8 states for them the report is not just a report, but it usually has an agenda of something that needs to be decided on the board and management level, thus it being extremely important that the board is interested and reacts when needed.

Interviewee 15 says the customers of their company are also interested in cyber security, and cyber security is even becoming a selling point. Interviewee 2 also believes than in five years cyber security will be a marketing advantage. Therefore, this increases the interest in cyber security amongst the board and management. Interviewee 15 feels like their interest in cyber security has grown year by year. Interviewee 15 also mentions the interest usually spikes up when there is a cyber incident on the news that is relatively close to their company. Interviewee 15 says they have also built interest in cyber security amongst board and management, by focusing on cyber security culture in the whole company and organising cyber security themed events.

Interviewees 6 and 14 state their boards and management are generally interested in the report, and therefore the intervieweed do not feel a need to raise their interest more. However, unlike many other interviewees, Interviewee 6 cannot confirm that the interest rate has gotten higher in the past years, which indicates their level of interest in cyber security has been relatively high for a longer time.

Interviewee 12 says their top management is very interested and wants to know even about the unpleasant topics. The interviewee says their management is constantly asking for more reports and analyses about the state of their cyber security. Interviewee 10 states their management and board are very interested, and their “buy in” rate is excellent. Interviewee 9 states they have highlighted the responsibility of the management and board when it comes to cyber security, which has increased their interest and improved reporting. Interviewee 9 mentions the situation before used to be that when they were presenting the report, it felt like one or two people from the audience actually paid attention and the rest of them were more focused on their laptops. However, as said earlier, the interest has improved drastically in the past few years.

Interviewee 5 states the interest of the board and management increased approximately a year ago when another company from the same industry suffered a major security breach. They wanted to know better how their company is protected from similar risks. Interviewee 5 also states meeting the regulations regarding cyber security is very important to their board and management. Interviewee 5 states they think that when the board knows that they are legally responsible for something, their interest rate increases drastically. In addition, they say that people have recently come to realise that the impact on the reputation is major, if something were to happen.

Interviewee 2 says their board and management are "diplomatically" interested in the subject, but not as interested as they should be. However, interviewee 2 says they have tried to rise the interest levels and it has continuously improved. Nevertheless, according to the interviewee, their board and management comment on the report and give ideas on how to improve it in the future. Interviewee 2 states one big aspect that has increased the interest of the board and management, are recent cyber security interests around the world, where the outcome has been destructive due to lack of interest in the organisations board and management level.

Interviewee 14 states their audience gives feedback on the report and asks more detailed questions about the subjects they want to know more about. They also comment on priority in a sense that they mention if something should be put on a higher or a lower priority on the agenda. Interviewee 14 also mentions they can openly bring up issues that need to be addressed to the management, which helps moving the situation forward. Interviewee 13 also says their audience gives very straightforward feedback and is active: especially their CEO participates in dialogue and requires explanations, rather than letting the CISO do a monologue, which would just be approved at the end. Interviewee 12 states their top management evaluates their success in cyber security and reporting it, twice a year. Their top management also asks for advice when it comes to decisions they have to make regarding cyber security.

Interviewee 11 says they may get questions during presenting the report, but not after, nor do they get comments on what the report should include. However, they feel the audience understands the report quite well, and has not so far expressed lack of understanding. Regardless, interviewee 11 states the time resources they have for cyber security on board and management level are small, and cyber security sometimes feels like a lesser prioritised agenda. They also feel that their report could improve on presenting a truthful picture of the state of their cyber security.

Interviewee 10 states their audience actively asks about the report when it is presented and asks for more concrete and detailed explanation for certain topics. They have also requested a strict and punctual presentation. They want to know right away what they need to know and what areas need to be decided about. Also, interviewee 9 says their board and management have asked for a more compact report as well. Interviewee 9 states their board and management however comment and asks for more specific explanations. Interviewee 8 says their board and management comment on the report, asking more specific or more vague information about certain topics for the next time. Interviewee 6 states their audience comments on the report and even ask about it sometime after receiving it.

In summary most of the interviewees felt that their boards and management are interested enough when it comes to cyber security. Many of the interviewee's state that there is enough dialogue, and according to some interviewees their boards and management even comment on the reports afterwards and give ideas on how to improve the report in the future. There were still many interviewees who felt that even when their boards seemed to be interested, they did not drive much dialogue, nor did they react in other ways. Only a few interviewees felt that their boards and management are not interested enough, and that dialogue and reaction was significantly lacking. Nevertheless, in addition to the fact that estimating the right level of interest is subjective, it is harder to evaluate the interest levels of audience which does not drive dialogue or react in other ways. Therefore, stating whether the interest levels of the boards and management are generally on a good level, would require further studies.

5.6 Level of understanding Cyber Security amongst boards and management

As mentioned before, according to studies 96% of CISOs either slightly or strongly agreed that senior executives have a better understanding of cyber security than they did five years ago (Help Net Security, 2019). Studies presented in the literature review however show, that there are still issues with the boards and management understanding the cyber security report presented to them. In literature review we examined the possible reasons causing this, one of them being the very short time window reserved for cyber security in the board room (Zongo, 2021).

According to interviewee 17 It is hard for CISOs to evaluate how much the board and management understand about the report and the vocabulary used in it. Interviewee 3 states it is hard to calculate how much each person understands, when there are people with different levels of understanding: some may know very little about the subject, while some may possess even deeper level understanding. Interviewee 14 says the audience may not even ask the reporter to explain what certain words or phrases mean, even if they do not understand them. Interviewee 4 also mentions it is hard for some of the audience to say "hey, I did not understand this. Can you explain it better?".

Interviewee 17 says the time limit might also cause the audience to think, that they will look the words up after, but often they may forget to do so. They say the time limit can sometimes be as short as 10 minutes, which is why it is important to focus on topics that are interesting specifically on board and management level. If you present these topics in an understandable way, the audience will listen and understand their responsibility in the matter, says interviewee 17.

> "I feel that the boards and management understand the severity of the matter clearly, but the challenge comes in communication." -Interviewee 17

Interviewee 16 says that even if some people in the board and management understand more technical language, the reporter ought to cater to the entire audience and write the reports in business language instead of using technical terms. Interviewee 13 also brings up it is a common challenge to use language, that is understandable to each person in audience.

> "One indication that I have learned is that you do not have the right message to your target audience, when someone takes their phone and starts browsing it. It indicates that your narration is either on a level too deep, or on the contrary it does not bring any additional value." -Interviewee 4

However, interviewee 16 mentions they have recently seen the level of understanding cyber security increase significantly at senior executive and board level. This means one can use more technical language now than they could before, of course still depending on the level of understanding in their board and management. Interviewee 16 also advices to avoid acronyms whenever you can. They had seen a situation where the person presenting the report struggled to explain what a certain acronym meant when asked. However, they add:

> "When you have explained an acronym once or twice, people get it typically." -Interviewee 16

Interviewee 18 says they use examples from the physical world, because some of the terminology used in cyber world can be translated to describe a similar situation, for example describing vulnerabilities as "unlocked doors". They state that in their experience board level people can relate to physical world better, and even ask them to explain something they did not understand using a physical building as an example.

Interviewee 15 states they try to present the reports in a way that the people in the audience do not need to be experts on the subject. However, they also believe it is their responsibility to educate board members and the management on the basic terminology. Interviewee 15 states that if a board member were to meet a customer for example and would not understand basic level conversation about cyber security, or would use wrong terms, it would not give a good impression. Interviewee 14 says they report similar themes to both the management and the board, but make the boards report more abstract, hence including less technical language. According to interviewee 12, they have not had a situation in their organisation, where it would have required any deep level understanding of cyber security to understand their reports. However, they mention that it might be because they are not the type of organisation whose business is very depended on technology, hence they do not have a need to use such technical language. Interviewee 10 states they have adjusted the report to the level that their board and management understand it, and if there is a need to explain something more technical, they use analogies and examples to explain it.

Interviewee 16 who has experience about board and management level cyber security reporting in many companies, states that in their experience the executives and the board take their role seriously and ask lots of good questions to make sure they understand the report, and that they get the full picture. Interviewee 5 says that when they started working as a CISO in their current company and presented the first report on board and management level, the board stated the report was not what they wanted. After that they sparred and the board explained to the CISO what they wanted, and what kind of topics are interesting to them in different situations. Interviewee 5 says they still occasionally spar with a few board members, to make sure the quality of the report stays good.

Interviewee 7 says they have analysed that their board and management do not understand cyber security as much as they should, despite of their interest in the topic. Interviewee 1 also believes they need to improve their report even more, because they feel their audience still does not digest the information as well as they should. Interviewee 17 also mentions there is a need to educate the board and management more on the reported subject. Their board and management have expressed their willingness to get help in the matter, which makes achieving the wanted state easier. Three of the interviewees said they have had specific training on understanding cyber security and its terminology for board and management level people. two of the interviewees felt no need for such training, and thirteen of them thought it would be a good idea but might not necessarily have resources for it now.

When it comes to reporting language, most of the Finnish interviewees stated they report to the board and management in Finnish, even if their business operated internationally. All interviewees whose companies operated mostly outside Finland reported in English. However, a few Finnish interviewees stated they report in English. For example, interviewee 4 states translating cyber security vocabulary from English to Finnish is hard and clumsy.

> “It is better to write the words in English, when they have been designed in English.” -Interviewee 4

Interviewee 15 says that even if all the board and management spoke Finnish as their first language, they would still most likely report in English because some of the report slides could then be used in different context as well. They mention that it also motivates you more to work on the slides if you know they will be used more than in one meeting.

Interviewee 17 suggests that CISOs find one person from the top management or the board to spar with before presenting the report to the rest. With this person they can go through the report and make sure it is formed in a way that non-technical people understand it too. Interviewee 14 says they go through the report with one member of the executive team before presenting it to the rest. Interviewee 18 says they do one on one meetings with the board to help board members to gain understanding on the matters that interest them, and to allow them freely ask questions. Interviewee 15 mentions they have considered this idea and should and will most likely focus on this more in the future. Interviewees 6 and 1 say they have had one on one meetings with a few C-suite members, but it has been regarding cyber security in general, and not necessarily about the report. Interviewee 2 says they do occasional one on one meetings with management members. There are also other methods to ensure that the report is understandable enough: for example, interviewee 12 uses a consult to ensure the quality of the report.

Interviewee 5 underlines the importance of building a good presentation, which requires significant amount of time. The person presenting the report should always think about what kind of message they want to send, and what will the reaction to the report be. Amongst most of the interviewees CISO is the one responsible for the cyber security report that goes to the board and management, but interviewee 9 says they have a task force who all help to form the report and sign it in the end. Interviewee 7 says their team takes part in forming the report, the CISO then forms the final version, and sends it forward. Interview 6 states their report goes through the IT management first, who perform quality assurance for it. Interviewee 5 says they spar with CIO and if needed, with the secretary of the board/management meeting before presenting the report. Interviewee 2 says they have different defence lines, and CISO being in the first defence line creates the report, while people on the second defence line review it and send it forward. Interviewee 4 says they have many meetings with their team about the report, to make sure it looks right and sends the right message.

Generally, almost all interviewees stated their boards and management have a good level of understanding the report. However, as stated before, evaluating how much the audience understands of the report is difficult. In addition, as mentioned in the section **5.5 Interest and reaction**, it is also hard to claim that the board and management understand the report, if in some cases they still do not drive much dialogue or react. The conclusion is that while the understanding of cyber security amongst board and management has increased rapidly, there are still cases where the level of understanding is poor or uncertain.

Another matter that should be brought up is how much of the report can be simplified to the level that the audience understand it, without losing its value. For example, Interviewee 15 stated they stopped using a roadmap in their reports, because it was hard for the audience to understand and relate to it. The question is, can the same important information be presented effectively in other ways, and what is the point where instead of simplifying the information, one should start focusing on educating the audience?

5.7 Significance of visuality

One of the goals of this research was to study the significance of visuality since there is no existing literature of the impact of visualisation in the context of reporting cyber security on board and management level. In this section we are going to look into results from the interviewees and examine literature considering visuality and visualisation. Visualisation means a process where data is mapped onto visual dimensions to create a pictorial representation (Bianco, Gasparini, Schettini, 2014). According to research, all the surveys have confirmed that supporting analytic tasks by using visual interfaces is important (Ošlejšek, Rusnák, Burská, Švábenský, Vykopal & Cegan, 2021). It has also been stated that visualising data is an essential element of business intelligence (Eckerson, Hammond, 2011).

90% of information transmitted to the brain is visual, and coloured visuals increase people's desire to read content by 80% (Eisenberg, 2014) ~ (Xerox, 2017). These factors alone are a heavy reason to add visuality in your report. In addition, according to research using colours makes an impression that is 39% more memorable, and it increases readers' attention spans and recall by 82% (Xerox, 2017). Nowadays technology provides an easy way to create and demonstrate images and animations, and visualisation equipment costs have dropped, which should lower the threshold of using visuality (McGrath, Brown, 2005). While some people still think visual tools are overrated, and do not provide an advantage over traditional methods, it is often what is needed to improve reporting (Vaught, 2022).

> "Everyone of us is different and learns in different ways. Certain people understand visualisation better." -Interviewee 17

According to a survey done by Eckerson and Hammond (2011), visualisation improves business insight majorly. This is presented in the figure 9, which is based on 210 respondents of their survey. Of the respondents 76% were either business intelligence- or information technology professionals. The impact of visuality on productivity is presented in the figure 10.

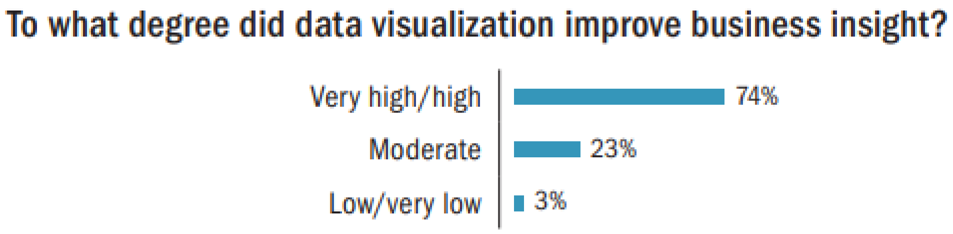


FIGURE 9 To what degree did data visualization improve business insight? (Eckerson, Hammond, 2011)

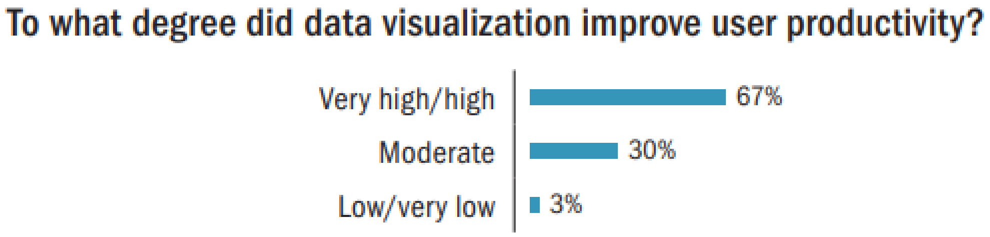


FIGURE 10 To what degree did data visualization improve user productivity? (Eckerson, Hammond, 2011)

During the interviews of this study, it was found that generally the interviewees who claimed to use visuality in their reports, stated that their boards and management had better level of understanding cyber security, were more interested in the report, and interacted more. For example, interviewee 12 stated that their board and management are extremely interested in the report, and that they even ask for more reports and analyses about the state of their cyber security, in addition to the formal reports. Their top management evaluates their success in cyber security and reporting it, twice a year. Their top management also asks for advice when it comes to decisions they have to make regarding cyber security. When talking about visuality, interviewee 12 also states they try to visualize their report as much as possible, including using colour coding.

Interviewee 11, however, says they do not use any visual effects, except for some tables, but think it would be a good idea to do so. They also stated that cyber security feels like a lesser prioritised agenda amongst their board and management, and that they might get some questions about the report during presenting it, but not after. In addition, they do not get comments on what the report should include.

There were a few exceptions: While interviewee 1 stated to use some visual effects in their report, such as colour coding and a PowerPoint template that has the visual look of their company, they still felt that their audience is not digesting the information properly. Interviewee 7 also says that using visual elements is necessary when the report is going to board and management level, and also use a template that fits the organisation's image. Regardless, they feel that their audience does not understand the report as much as they should. It must still be noted that analysing how much your audience understands, is very difficult, and the results are dependent on both the nature of the analyser, and the subjects.

Besides visuality, there are also many other factors that may affect the interest, interaction and understanding of the board. In addition, while visuality is clearly increasingly important in reporting, poorly designed visual displays may in fact force the audience to work even harder to get the information they need (Eckerson, Hammond, 2011). Visuality can, however, be a great factor in increasing the quality of your report.

How can one form a well-designed visual report? It is suggested that all possible data should not be presented, but the most relevant parts. Even then it should not all be crammed into one graph, chart, or infographic. (Tervort, 2022.) Otherwise, it may cause visual overload. Overall, the best visual displays introduce new information gradually, and thus have higher adoption rates among users. (Eckerson, Hammond, 2011). Interviewee 17 states it is also important not to change the visual view of the report all the time. When the audience gets used to a certain look, it makes it easier for them to follow it. Therefore, it is important to make changes with consideration and in a controlled way. It is also good to inform the audience beforehand about changes, stated interviewee 17.

Interviewee 16 states a visual report does not have to be "too fancy", but visual reports are typically more effective than word documents. They say they have seen a change: people include more diagrams and graphs inside the long form reports now as well. They also mention the importance of colour coding, which also many other interviewees claimed to use a lot in their reporting. Colour coding means associating a set of colours with a set of items, and can be used in multiple ways, for example, to present quality or quantity, (Bianco, Gasparini, Schettini, 2014). Colour coding is often used by assigning different colours to indicate various risks, dangers, and safety hazards (Safeopedia, 2022). Colours can distinguish quickly between "good" and "bad": for example, green arrows are often used to show increase, while red arrows present loss. (Megalytic, 2017).

> "Especially board level people are sort of attuned to focus on the red, so if you want get attention, you make something red." - Interviewee 16

Eckerson and Hammond have created a list of recommendations on how to incorporate visualisation into business intelligent applications. Many of these recommendations can be applied when creating a visual report for cyber security reporting on board and management level. First, one must focus on what information the audience needs, and how they are going to use it. The visuals should be populated by high-quality data, or even the prettiest pictures will not have any value. One should create a prototype and get feedback on it before presenting it. To create the perfect design, the prototype needs to be iterated continuously. While visual templates are important, one should avoid excessive decoration that takes the attention away from the important messages. One must also remember that visual preferences change over time as users become more familiar with the data and the visual environment. Thus, visual displays should be sparse at the start and then become denser over time. Finally, one should create a standard look for their report: using standard graph types, fonts, labels, and colours. Templates are a great way to improve usability, which is why creating a template that can easily be edited depending on the current need, is important. (Eckerson, Hammond, 2011).

An important factor when creating an effective visual report is choosing the format. Some organisations use, for example, PDFs, while others use PowerPoint slides. When choosing focusing on formatting, one should make sure the format is easily scannable for eyes: make sure to pay attention on choosing a font that is easy to read and use bullet points. It is important to use headings and sub-heading to provide clear statement of the purpose and organise the information. Doing so offers a visual contrast and helps the audience to navigate around the information. Consistency is key, and the template used should include solid style and fonts throughout the report. At last, the report should follow a hierarchy; reporting should the treated like a narrative that tells a story. Make sure the topics in the report are presented in a logical order. (Megalytic, 2017).

Metrics and other numeric data should be presented visually by using graphs, charts, and tables. There are multiple choices on how to visualise data, but the key is using a consistent theme between all the graphs and tables presented. One should remember that graphs and charts are not the only way to add visuality in reports: using colours, images, and screenshots can stimulate emotion and make the report easier to follow. (Megalytic, 2017).

We already examined how some interviewees used visuality in their reports, but to get a better picture of how visuality was used among all interviewees, we will look into additional statements from the interviews. Interviewee 15 reports using strong, effective visual elements. In addition, they repeat key words and phrases, which makes it easier for the audience to remember the content. Interviewee 15 says it is important that the slides and stories are made in a way that it is easy to look at or to listen to them without getting bored.

Interviewee 8 states they use visual elements in their reports, and that the PowerPoint slide they present must be maximum eight pages long. Doing so they ensure that it is easy to follow and go back on certain page or topic if needed. They also say they like to use visual elements that wake the audience and create dialogue. Interviewee 9 says they only have some visual charts and admits they should improve the visual side of their report. As mentioned before, their board and management have asked for a more compact report. If more information were presented visually, it would make it easier for the audience to digest it. Thus, they could possibly even use the same amount of information if it was presented more visually.

Interviewee 6 also states they would want to add more visuality in their report in the future. Now lack of time is limiting their capability of making visual reports. Currently they are using the company fonts and colour scheme and adding visual charts whenever possible. They say the report should not look like it is “made by engineers, for engineers”. Interviewee 2 states they do not focus on visuality, but that they probably should. They thought it would be a good idea to for example use an external service to create a base that can easily be edited.

Interviewee 5 says they are currently working on and iterating a report template. They already use colour coding. Interviewee 14 uses a solid report base, that has been created with the help of external professionals. Interviewee 4 states they have recently improved their reports' visuality significantly. They have used an external expert to create visually impressive slides.

> "When it looks like one has gone to great lengths to create the slides, the viewer gets the feeling that one has really worked on the report." -Interviewee 4

Interviewee 3 uses lots of visual elements in their report, starting from a visual template. They have drawn a visual map which shows different units, their information systems, and the risks that are linked to them. Interviewee 3 says that especially risks are hard to explain in the report, which is why they focus on using visual effects and other clarifying elements when taking the information to the audience.

In conclusion, while most interviewees use at least some basic elements to make their reports more visual, there were some interviewees that stated to use visuality very little or not at all. However, all the research points to the fact that visuality is essential in efficient reporting, especially when reporting cyber security on board and management level since they are rarely experts on the subject. In summary, visuality increases interest and interaction and makes learning easier. As previously stated, the interest and understanding levels of boards and management are still often an issue. Creating more visual reports can be a key factor when trying to improve the overall quality of the report, thus there is a high chance that visuality alone can already affect how interested your audience is, and how much they understand of the report.

5.8 Using external help with the report

A few interviewees brought up using either external services to help with the report, or even hiring a data analyst. Eight out of 10 interviewees who have used external analysts, consults, or other professionals to help with their report, state they have benefitted from it.

Interviewee 18 speaks for having a data analyst, and interviewee 14 says they have used external services with data analysts. Interviewee 1 says they have recently hired an analyst whose job is to produce and analyse the situation map and oversee the metrics. Interviewee 1 states that before the data presented in the report was slightly scattered, and the presentation was not as coherent as it could have been. They also say the report was not as understandable, because cyber security professionals tend to use language, that they do not even know that other people do not understand as well. After hiring an analyst, who does not have expertise in cyber security itself, they feel their report has become more professional and understandable.

Interviewee 8 says they are planning on getting external help with the report, which will most likely increase their maturity. They have also had external professionals doing presentations for the board to give more impartial view of the state of cyber security in their company. Interviewee 1 also states occasionally having external professionals talking about cyber security in their meeting with board and management. Interviewee 8 believes that the message goes through better when it does not come from one person only. Interviewee 7 also states to have noticed a similar phenomenon, and therefore uses external help with creating the report and gathering information for it. Interviewee 5 states that during the interview they were currently using a consult to find out better ways to address the needs of the board, and to support their decision making.

6 DISCUSSION

This chapter discusses the interpretation of the literature and the results of this study compared to the research questions, after which the contribution and limitations are presented. Finally, future research is discussed.

The main research question of this study, "**How can cyber security be reported effectively on board and management level?**", was based on the rising importance of reporting cyber security to boards and management, and the recognised problem of doing so effectively. This study aimed to answer this question by identifying repeating themes from the interviews of the empirical part of this research and comparing them to already existing literature.

The empirical study was done by interviewing 18 CISOs from different industries. The interview mainly focused on questions of how they are doing their reporting now, and how they are going to improve it in the future. The literature review focused on the history of board and management level cyber security reporting, as well as how it is done now. Focusing on these two main themes allowed to gain understanding of how reporting in this field has changed, and to what direction it is going.

As the examined literature and the interviews showed, there is not any existing model or framework that could answer all the needs of every company when it comes to cyber security reporting on board and management level. After analysing the literature and the interviews, it was realised that trying to create one would not be rational. Even when two organisations share the same industry and are similar in size, they may have very different needs in cyber security reporting on board- and management level. Therefore, the model created and presented as a result of this study does not state any best practices in reporting, nor does it encourage to report always in the same way. Instead, the model helps to create and improve an individual efficient reporting method, that can be shaped to meet the needs of organisations.

While using the model may appear more time-consuming than using already existing reporting frameworks, performing the steps should get faster and easier as the cycle is repeated: the more familiar you get with each step and their objectives, the less time you have to spend on studying/preparing them.

In the end, using your own iterated method instead of strict frameworks and models can benefit you by decreasing the number of irrelevant subjects in your report, and replacing them with what your audience needs to fulfil their role. This model is explained in section **6.1 Creating an efficient reporting method** and presented in figure 12

There were two sub-questions in this study, the first being **"What is the impact of visuality in board and management level cyber security reporting?".** The first sub-question was answered by studying literature from different fields and analysing the interviews. All the literature found supported the statement that visuality, if done well, improves interest, learning and information digestion. Among the interviewees, excluding a few exceptions, those who reported using lots of visuality in their reports, also reported higher rates of interest, understanding and interaction among their audience. In conclusion, it can be stated that visuality has great significance in reporting cyber security to boards and management. However, if executed poorly, it may have an opposite effect; for example, if you use too many different colours when presenting charts, or add too much data, it becomes harder for the brain to digest (Gupta, 2022).

The second sub-question of this study was **"How has cyber security reporting on board and management level evolved?"**. In the chapter **3. Literature review** two different sections focused on presenting the history of board and management level cyber security reporting, and what it is now. The section **3.2**, which focused on the current state, presented the most recent literature, and literature that has not been proven outdated. During the interviews conducted in the empirical part of this research, the interviewees were asked about their current reporting practices, as well as when and what type of change they have noticed in cyber security reporting on board and management level — inside their organisation and in general.

The conclusion is that boards and management have generally become more interested in cyber security and understand the topic better than they did five years ago. Cyber security reporting on board and management level has become more risk-based instead of focusing on single vulnerabilities and will most likely focus on risks even more in future. Therefore, instead of technical metrics, metrics describing visibility and business impact have become more popular. Many interviewees also stated to have recently used external help with reporting cyber security to boards and management, for example by using a data analyst or a professional to improve visuality of the report. Some interviewees are also planning on getting external help. In the future, including more external professionals in the reporting process will most likely become more common, since it has proven to be beneficial.

The reporting frequency has grown in the past years but is still not as frequent as it should be. However, many interviewees who did not formerly have schedule for reporting, stated to have created one recently. Therefore, one can estimate that the reporting frequency will grow in the future. Deloitte has stated in their survey done in 2019, *The Future of Cyber*, that half of the boards surveyed are not discussing cyber security as often as they likely should be. They claim today's boards should have adequate access to cybersecurity expertise, and cyber security should have at least some levels of consideration at every board meeting. (Deloitte, 2019). In conclusion, cyber security on board and management level has evolved greatly, but still has room to improve.

6.1 Creating an efficient reporting method

Creating an efficient reporting method is not a simple one-time task. As stated before, there is not a single model or framework for reporting cyber security on board and management level, that meets all the needs organisations have. There are articles and blog writings on best practices for building a cyber security report, but they still do not address all the issues CISOs tend to have with reporting. In addition, these best practices are not necessarily based on evidence, nor do they work for every organisation.

Deloitte has created a figure presenting seven strategies to improve cybersecurity communication to leadership, presented in figure 11. These strategies are a great start, and especially effective when building interest and understanding amongst board and management, but they do not address every issue regarding creating an efficient reporting method: for example, using metrics and money-describing number has proven to be controversial in some industries and organisations.

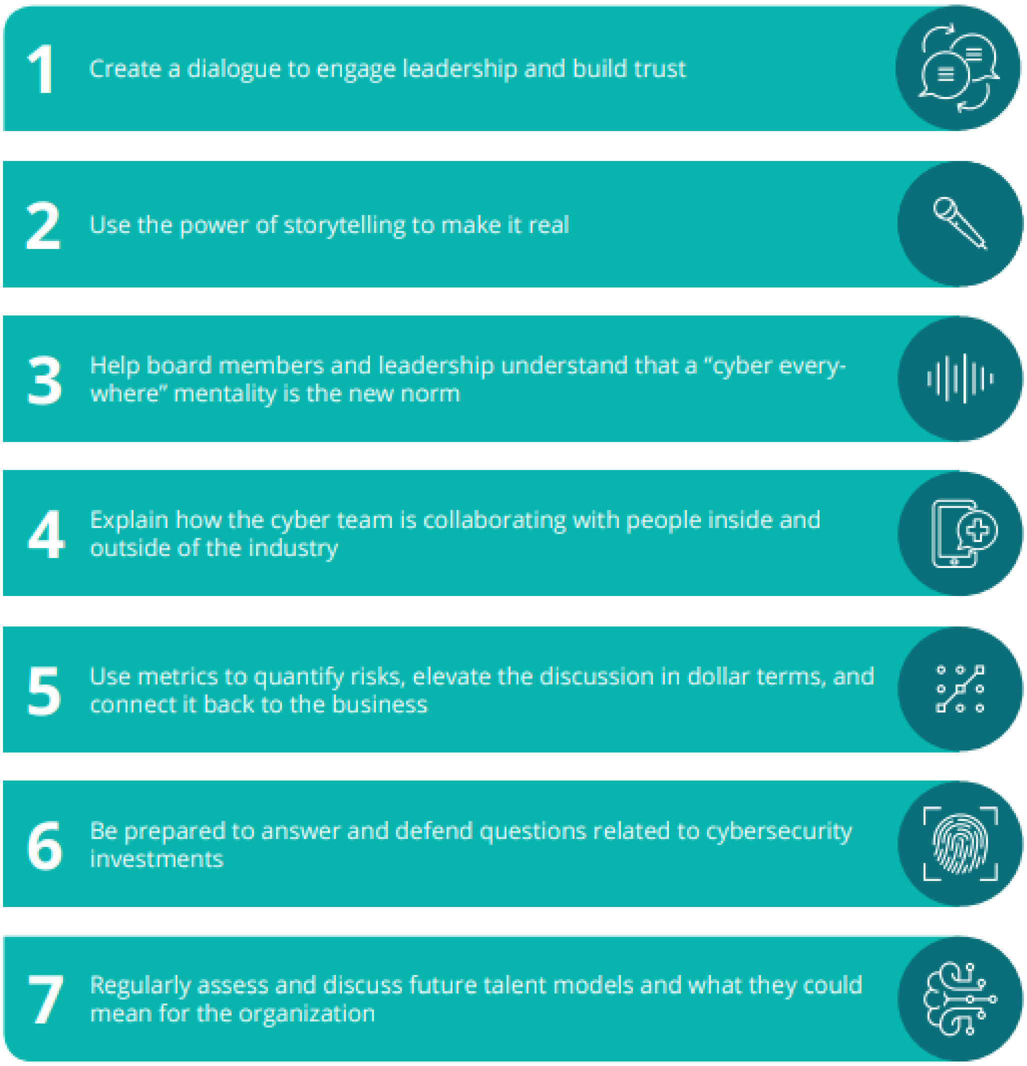

1 Create a dialogue to engage leadership and build trust
2 Use the power of storytelling to make it real
3 Help board members and leadership understand that a “cyber every-where” mentality is the new norm
4 Explain how the cyber team is collaborating with people inside and outside of the industry
5 Use metrics to quantify risks, elevate the discussion in dollar terms, and connect it back to the business
6 Be prepared to answer and defend questions related to cybersecurity investments
7 Regularly assess and discuss future talent models and what they could mean for the organization

FIGURE 11 Seven strategies to improve cybersecurity communications to leadership (Deloitte, 2019).

As an end result of this study, a process model for creating an efficient reporting method for reporting cyber security on board and management levels, was formed based on the empirical study and the existing literature. This model does not suggest any best-practice topics to report, but instead it guides and encourages the people creating the report to find what is relevant to report in their organisation, and how it should be reported to their audience. As already established, creating an efficient reporting method is not a one-time task, but the methods must be iterated and changed over time, as the world, organisation, and their reporting needs change. Therefore, the model created is iterative, and not a waterfall model. The model is presented in the figure 12.

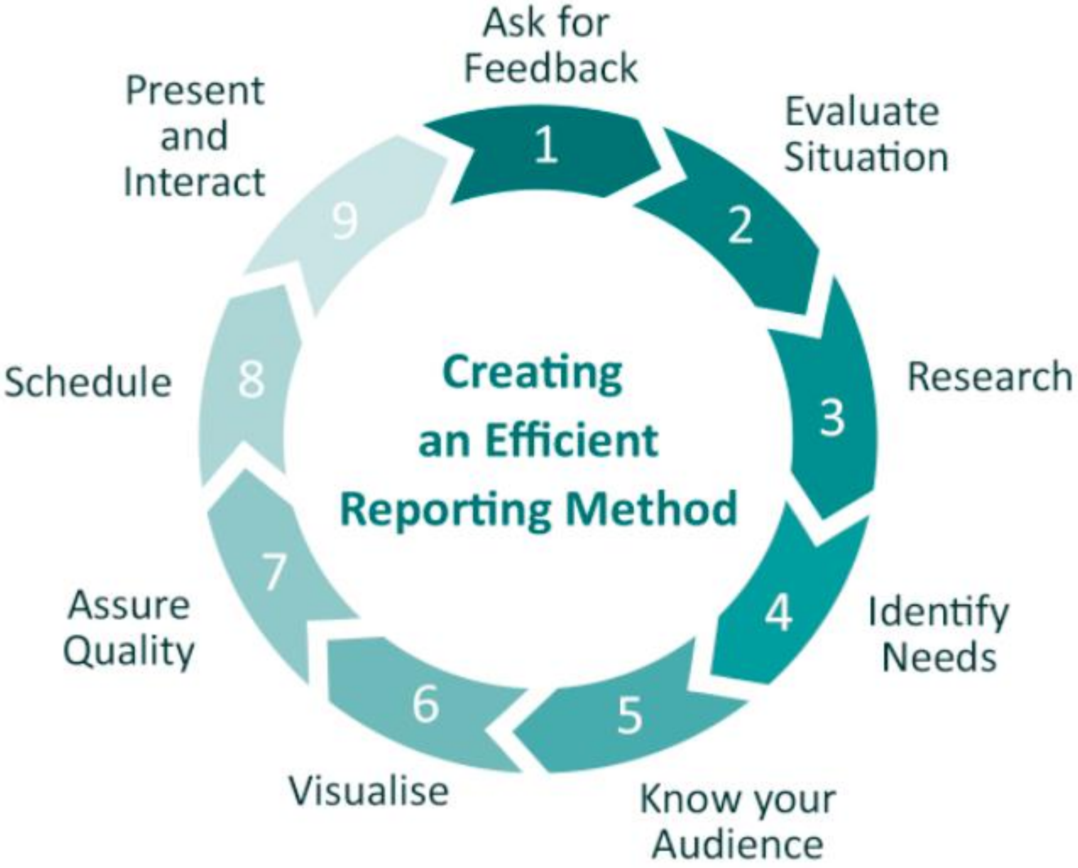


FIGURE 12 Creating an efficient reporting method

6.1.1 Ask for feedback

The first stage of creating and efficient reporting method is to ask for feedback from your board and management; what topics have been relevant, less relevant, or not at all relevant to them? Is there something they do not understand? Do they have any suggestions? It is important to understand what you are already doing right, and which areas require improvement. In the literature review we already examined the phenomena of the most reported metrics not matching the metrics that are most valued by the board (Cyentia Institute 2018). With increasing communication and asking for feedback more often, one could better provide the information the audience wants.

Amongst interviewees, those who reported getting feedback on the report from their board and management, also reported more often that their reporting is on a good level. Receiving feedback frequently makes sure that the reporting method keeps evolving with the organisation and does not become outdated. Make sure to ask the audience beforehand what topics they would like to see in the report, and after the presentation ask if the report was what they wanted.

6.1.2 Evaluate Situation

When talking about evaluating situation in this context, it means evaluating the condition of cyber security in your organisation, and what is the state of reporting it on board and management level. What is the message you want to send? What are your challenges and what have you achieved? Do you need the audience to make decisions on certain matters?

To define the message you want to send, and what decisions need to be made, you must also evaluate what needs to be done to improve your cyber security. If you cannot present your plans, you cannot expect the board and management to make the needed decisions.

There are many different ways to evaluate the state of your organisation's cyber security. One of them is by conducting a self assessment. There are multiple methods to analyse your own performance; for example, gap analysis is a method for assessing the performance to determine whether the requirements or objectives are being met, and if not, and what steps should be taken to meet them (Hanna & Sales, 2021). Another tool for conducting a self assessment is an Information Security Controlled Self Assessment (CSA), which has been created by the IT@UC Office of Information Security. A CSA sets expectations of adherence to industry best practices and policies, and it is meant to be used to rate yourself on the standard CMM maturity scale. The intent of CSA is to also seek continual improvements each year in areas of immaturity. (University of Cincinnati, 2022).

When it comes to evaluating cyber security within their organisation and estimating what still needs to be done, one can also consider using other maturity metrics, and for example, threat modelling. The goal of threat modelling is to identify, communicate, and understand threats and mitigations when protecting something of value (Drake, 2022). Other ways to evaluate the situation of your cyber security, is to order an assessment from outside of your organisation, or to use security benchmarks, and compare your performance to other companies in the same industry.

Interviewee 14 highlights the importance of repeatability of the methods chosen for evaluating the state of your company's cyber security: the situation may change along with the threat environment, and continuous tracking helps with finding the focus areas. Interviewee 14 adds that maturity assessments can be tracked, for example, once a year, or as often as four times a year, which they do.

6.1.3 Research

We have already talked about already existing frameworks and models. According to research and the interviews conducted in this study, these frameworks and models are not flexible enough and do not answer all the needs in cyber security reporting on board and management level. However, even if these models and frameworks might not work in this context as they are, they also have beneficial parts that could be implemented in your reporting. Some interviewees stated to have adapted some parts of popular models and frameworks, such as NIST and ISO 27001, into their report. In addition to the previously mentioned, there are other existing tools that can be beneficial in the report. If you do your research and examine your options, you might not have to start from nothing, or invent something that has already been invented.

Doing your research also means studying and being aware of what is happening outside your organisation. Trends, threats, and incidents around the world may change the course of your reporting. Many interviewees have stated to report the previously mentioned topics to their board and management. At the bare minimum, the boards and management should know the changes regarding them. For example, when there are new laws and rules considering cyber security that the organisation has to start following, they need to be prepared for them (Dobrygowski, 2022).

6.1.4 Identify needs

After you have evaluated the state of cybersecurity in your organisation, done your research on what is happening outside your organisation, and decided what message you want to send to the board, you must identify what is the information the audience wants and needs in order to fulfil their role in decision making. Board members should be provided with information that helps them make the best decisions regarding governance, and senior leaders should be provided with the intelligence to make optimal management decisions (Deloitte, 2019).

Interviewee 8 highlights it is important to report only about subjects that matter for the operational effect, hence reporting what teams do is not necessary; boards and management are not interested in, for example, how many attack their firewall has blocked. When it comes to other metrics and numbers, evaluate whether they could be necessary in your organisation. When you have recognised your challenges and achievements in cyber security, estimate their value on board and management level reporting: what risks and incidents should you focus on, and what should you present of your progress.

According to already existing literature and the interviewees of this study, using metrics and numbers is controversial. They can easily become information overload, but in the best case, they can be a powerful tool in highlighting your current security program and improvements. Currently, the reported metrics often vary depending on the nature of the organisation: risk-seeking firms report awareness and operational metrics, while risk-averse organisations focus on governance metrics. (Cyentia Institute 2018). Amongst the interviewees of this study, it was noticed that using numbers to describe financial losses was more common in companies that offered separate purchases or services (for example, retail or food and drink industry), than in companies that had a continuous contract or agreement with their customers (for example, finance or higher education industry). Whether you should report maturity metrics or/and present numbers that describe financial impact on business, depends significantly on the audience, and how they digest information.

6.1.5 Know your audience

When you know your audience, it is easier to plan *how* you are going present your information to send the message you want and engage the audience in decision making. According to a study done by Deloitte (2019), boards and management want to have dialogue instead of briefing on cybersecurity (Deloitte, 2019).

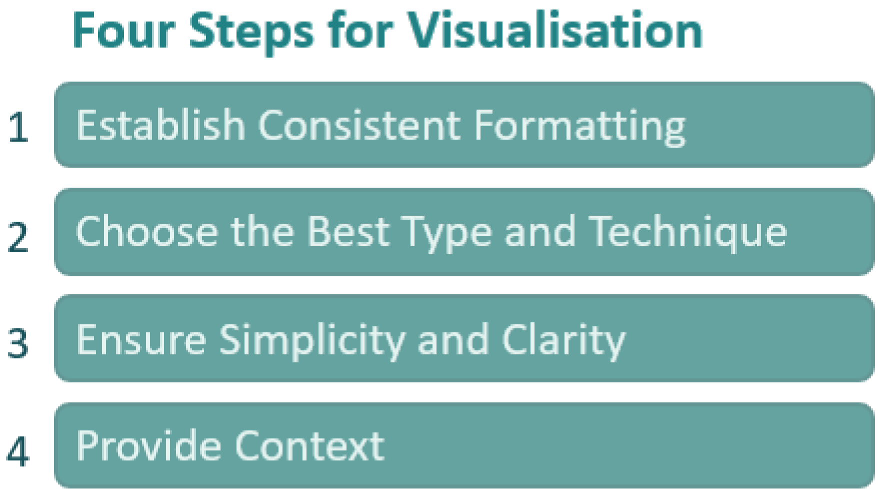
You must understand in what form your audience wants to receive information. Based on the literature and interviews done in this study, a roadmap has been an efficient way to describe risks, incidents, and achievements, amongst other topics. According to Reliaquest (2022), presenting clear roadmaps and benchmarks in board and management level reporting helps the audience to better understand where resources are needed and what are the plans for the future. However, this might depend on the level of cyber security understanding of your audience: Interviewee 15 reported to have given up using a roadmap because their audience did not understand, nor did they relate to it. How you present information to your audience can and should evolve with the level of cyber security understanding amongst your board and management.

It is important to know how interested your audience is and how much your board and management understand of cyber security and the report. If the audience does not pay attention or does not understand what is being presented to them, delivering the report has very little to no value. However, estimating the interest and understanding levels of your audience is difficult. In the section **5.6 Level of understanding Cyber Security amongst boards and management** we looked into ways of how to better understand your audience, and how to improve their understanding regarding the report. For example, you could arrange one on one meetings with the board members and management, or spar with just one of the people from the group. Increasing communication between the person reporting, and the people receiving the report builds trust and increases understanding (Deloitte, 2019). As interviewee 17 stated, they feel that the boards and management understand the severity of cyber security, but currently finding a common language in communication is the challenge.

6.1.6 Visualise

As was concluded in the section **5.7 Significance of visuality**, visualisation can be a key factor when trying to improve the overall quality of the report. Creating a more visual report can already affect how interested your audience is, and how much they understand of the report. In addition, former studies suggest that visualization provides ways of examining and improving managerial judgement (Yee, Walker & Menzfield, 2012). However, data visualization, especially for non-expert audiences, should be attractive and clear (Quispel, Maes & Schilperoord, 2018). Poorly designed visual displays can make it even harder for the audience to scan and understand the presented information. Visualisation should not only present information, but to tell a story that allows us to easily see patterns, trends, correlations, and distribution (Gupta, 2021).

Combining the existing literature and the results of the empirical study of this report, a list of key steps for using visualisation in reporting cyber security to boards and management was created. The steps were chosen based on how often they appeared in different literature, and if they were brought up during the interviews of this study. They were also reflected to the context of this study and aligned in a suggested chronological order. The list is presented in figure 13. Following these steps helps in forming a clear, understandable report that should be easy to follow for a non-expert audience.


Four Steps for Visualisation

1 Establish Consistent Formatting

2 Choose the Best Type and Technique

3 Ensure Simplicity and Clarity

4 Provide Context

FIGURE 13 Four steps for using visualisation in reporting cyber security to boards and management

Establishing consistent formatting is mentioned in both literature and interviews of this study. One should establish consistent formatting across all reports (Somers, 2020). The page layout, colours, font styles and sizes should align (Megalytic, 2017). If your company has a brand book, it can be very helpful when choosing colours and fonts. (Somers, 2020). Additionally, using PowerPoint is a good way to present the report when telling a narrative, as it provides flexibility. A template that can easily be edited, with consistent colours and fonts, is a great way to increase visuality of your report.

When it comes to choosing a visualisation type and technique, it is important to decide what type of visualisation and technique is suitable for the objective it is meant to serve (Nausheen, 2021). For example, charts, diagrams, and graphs are the most common data visualisation types, and include techniques, such as pie charts, bubble graphs and tape diagrams. Visual summaries, on the other hand are extremely useful for showing anomalies, outliers, and top rankings. (Gupta, 2021). Maps, on the other hand, should be used for visualising physical locations (Somers, 2020).

Ensuring simplicity and clarity is important to keep the report as understandable as possible. Using pictures and other colours can make the reports easier to follow. However, as stated before, one must be careful not to decorate their report excessively, as it might take the attention away from the important messages and make the information harder to digest. Colour coding is often seen as a method, that clarifies the presented information. Nevertheless, when presenting graphs, one should avoid making them too multicoloured, as it makes the graph less comprehensible by forcing the brain to process more categories. Instead, one can use sequential colours, and, for example, red for highlighting. (Gupta, 2022). An example of sequential colours is presented in figure 14.

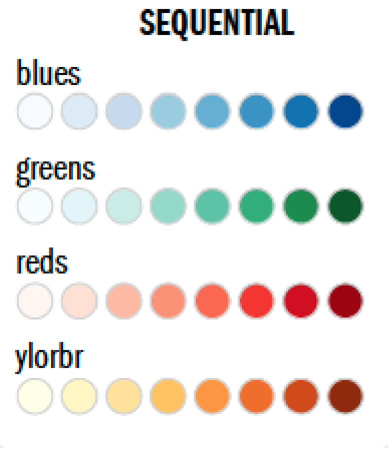


FIGURE 14 Example of sequential colours (Gupta, 2022.)

It is also important not to present all the possible data you have, but only the most relevant parts. Even then you should not cram it all into one graph, chart, or infographic. (Tervort, 2022.) In addition, using inconsistent scales are considered as poor, unclear visualization, which can have a negative effect on how your audience understands the report (Stobierski, 2021).

Providing context was often brought up in literature, and it is believed that tables and charts are meaningless without context (Gupta, 2021). One should provide context around visuals to ensure that the audience understands the meaning of the data presented and ensure that it provides only the necessary information (Nausheen, 2021).

6.1.7 Assure Quality

While the existing literature does not mention quality assurance often when talking about reporting cyber security to boards and management, many interviewees of this study brought up different ways they use to make sure the quality of their reports stays good. Some suggest sparring with the members of the audience, while others recommend using a consult or an analyst. Interviewee 7 states their report goes through IT management, who perform quality assurance for it before presenting it to the rest of the audience. However, it is not necessarily mandatory to use an external person to assure the quality of the report, even if it would be advisable. Especially considering smaller companies, all organisations do not have resources for it. Nevertheless, the person responsible for the report should make sure the report possesses most of the characteristics of a good report, which we are going to talk about next.

While quality assurance of a report is not presented much in literature focusing on cyber security, characteristics of an ideal report have been studied in other fields. Regardless of the field, a report is defined as a clearly structured document, that identifies and examines issues, events, or findings of an investigation. There are some main characteristics of an ideal report, that Kumar (2020) has presented in their paper as following:

- An ideal report should be Clear, concise, accurate and well organised with clear section headings.
- Easy for the audience to understand.
- Presentation is a key element in successful report writing. Formatting, revising, and proof reading are important process for good report writing.
- All reports should have an executive summary that presents the essential elements of the report from the introduction through to the recommendations and outcomes.
- Reports should be visually appealing and easy to read. Diagrams, figures, charts, tables, and graphs can all add interest to a report.

(Kumar, 2020).

6.1.8 Schedule

It has been brought up that cyber security is relatively rarely on board and management agenda, considering the importance of the topic. Communication frequency is a key factor in reducing risk, due to it providing visibility of relevant facts, giving the board and management the ability to process the information, and allowing them to get in-depth with the CISO. (Zeni, 2022).

As mentioned before, it is claimed that cyber security should have at least some levels of consideration at every board meeting, and boards should have adequate access to cybersecurity expertise. Discussion about cyber risk management should be given regular and adequate time on the board meeting agenda. (Deloitte, 2019).

The frequency often considered a leading practice in reporting cyber security to the board is once a month. However, in the survey done by Deloitte (2019), only 4% of respondents stated that cyber security is on the agenda of the board that often. (Deloitte, 2019). Amongst the interviewees, none reported to their boards monthly, and the shortest reporting frequency was quarterly. However, most of the interviewees reported to their management more frequently. Nonetheless, only 18.8% reported to their management monthly, and the biggest percentage, 37.5%, reported to their management quarterly. Some interviewees also stated that cyber security feel like a lesser prioritised agenda amongst their board and management, and that the time limit for presenting the report is very short.

It is important to raise interest amongst the boards and management, and make sure that there is enough time reserved for cyber security in the agenda of their meetings. In addition, one should make sure that the reporting frequency is short enough, so that the board and management still remember what is important in their cyber security. The reporting frequency can change over time, depending on the situation and state of each organisation's cyber security: when more decision making is needed, or there are critical topics to discuss, cyber security should be added on the agendas of board and management more often.

6.1.9 Present and interact

As mentioned before, presentation is key in successful report writing (Kumar, 2020). There are many articles on how to present a report effectively, but in short, they can be summed into preparation, preparation of visual aids, practice, and delivery. Preparation includes for example estimating the time available and considering the audience and their background. (University of Birmingham, 2022). We already know, members of boards and management are rarely experts on cyber security, even if their level of understanding it has increased majorly over the past years. This means you should avoid technical language, unless you are sure they understand the meaning, or you are going to explain the terms used in the same context. Even then it is advisable to avoid bringing too many new words to the presentation. As we already discussed visualisation, we are not going to explain in further in this context.

Practice is important before delivering the report. You should also prepare for the questions that you may not be able to answer and know how you will respond to them. (University of Birmingham, 2022). When delivering the report, you should pay attention on how the audience reacts; what questions they ask and why, and what prompts discussion (Cyentia Institute 2018). This will not only help in keeping the attention of the audience, but also will help you to understand how much *they* understand of the report, and what topics seem relevant to them.

As stated in the Terminology chapter, cyber security reporting in this study means a process where the person(s) responsible for the report completes at least the following steps:

1. Gathers and analyses the relevant data regarding cyber security of the organisation
2. Transforms the analysed data in a presentable form
3. Delivers the report
4. Makes sure the presented information is actionable

While making sure that the presented information is actionable should start already in the early phases of creating the report, it is important to interact with the audience when you present the report and need them to act. You should not only inspire dialogue, but to offer the board and management help when they need it in decision making. After the presentation, interact by asking your audience for feedback.

6.2 Contribution

In this section, the contributions of this study to the fields of information systems and cyber security, are presented. The research topic is relatively new, and for example, the significance of visuality in board and management level cyber security reporting has not been directly studied before.

The research problem defined in this study was the issue of reporting cyber security to management and boards efficiently, since according to former studies, it is not at the desired state . The conclusion is that while reporting has improved especially in the past years, unnecessary data is still being reported, and ineffective reporting methods are being used. The main contribution of this study is a process model, that presents an iterative way of creating an effective reporting method. This model was created based on the empirical study of this study, and the already existing research.

There are existing frameworks and tables of contents for reporting cyber security to boards and management. In addition, former literature presents sample reports, that include some key areas of reporting in this context, such as the threat landscape and cyber risks. The most recent literature also presents models for metrics and calculating risks. (Dezeure et al., 2022). However, these solutions presented in former literature do not meet the needs of all organisations. The existing guidelines for communicating cybersecurity to boards and management also do not directly aid in creating a reporting method, and maintaining it up to date (Deloitte, 2019).

Former literature, for example “How to create cybersecurity reports for boards” by Carissa Duenas (2021) and “Cyber Balance Sheet report 2018” by Cyentia Institute (2018), review how reporting has been done, and what are the likely issues in it. They also present claimed best practices, such as using certain metrics, in reporting. Compared to the existing literature, the model invented in this study offers a new way to create a unique reporting method that answers the needs of each organisation, by also using already existing useful material and keeping the method up to date, instead of offering best practices, which may not in fact suit the needs of all types of organisations. For example, monetizing (calculating value at risk in monetary terms) is often mentioned, especially in the latest literature (Dezeure et al., 2022). However, according to the empirical part of this study, monetizing risk does not hold as high a significance among companies who have a continuous contract with their customers, compared to organisations who offer separate purchases or services.

In conclusion, the model created in this research differs from former literature, and it contributes to the field of science significantly by presenting aspects of areas that have not been discussed before or have only been briefly mentioned in this context, such as visualisation and assuring quality of the report. In addition, the model exploits formerly discovered knowledge, such as using metrics and benefitting from existing frameworks, by suggesting analysis on the current situation and needs of one’s organisation and target audience.

In this study, significance of visuality was studied. While visuality and its impact has been studied in other practices, it has not been studied before in cyber security reporting on board and management level. At the most, it has been briefly mentioned in literature regarding the subject. In this study, the interviewees were asked about how and how much they use visuality in their reports. These answers were compared to what they reported about the interest, understanding levels, and interaction of their audience. The results were also compared to the literature about visuality in other fields. The conclusion was that visuality, when done right, has a great positive impact on reporting cyber security to boards and management. However, based on the interviews, the importance of visuality had not been realised in all organisations, which is why studying the significance of visuality in this context was significantly important, and therefore brings great contribution to the field. In this study, good and bad methods for visualisation were studied. Based on the literature and the empirical part of this study, a four-step list for using visualisation in the context of reporting cyber security to boards and management, was created. The results of this study regarding visualisation bring valuable new information from the interviewees. The findings regarding visualisation in this study contribute to the field of science, as they do not only state the importance of visualisation, but also suggest ideas and steps that have been customised for using it in reporting cyber security on board and management level.

This research also studied the evolution of cyber security reporting on board and management level, therefore presenting the updated view on how it has changed until now and is done in year 2022. In addition, this research mentions how the reporting can be estimated to change in the future. For example, it was estimated in this study, that reporting cyber security on board and management level will become more frequent a practice, and shift towards more risk-focused content. In conclusion, this study contributes the fields of the study by bringing new information, strengthening findings that have been made in former studies and offering an updated view on areas that the existing literature has studied before.

6.3 Limitations

In this section, the limitations of this research are going to be examined. Since this study has been carried out using a qualitative research method, it holds the classic limitations of qualitative research. As qualitative analysis aims to provide a detailed description, no attempt is made to assign frequencies to the linguistic features, and rare phenomena can receive the same amount of attention as more frequent phenomena. Qualitative research also allows for fine distinctions to be drawn. (Atieno, 2009). The causality between different research phenomena is also difficult to investigate, and the quality of the research is highly dependent on the individual skills of the researcher. (Barbour, 2000) ~ (Anderson, 2010). The research is also more likely to be influenced by the personal biases and idiosyncrasies of the researcher (Anderson, 2010). The main disadvantage of qualitative research is that the findings cannot be extended to wider populations with the same level degree of certainty compared to quantitative analyses. (Atieno, 2009).

In addition to the limitations qualitative research usually has, this study also has other limitations. These limitations were related to earlier research and the data set. As mentioned before, the existing literature was limited, since the whole concept of reporting cyber security to boards and management is a relatively new research area. Therefore, earlier research is seen as a limitation of this study.

The data set consisted of 18 CISOs from 13 different industries, and one that was marked as "unknown" due to the nature of their industry. Because from most industries, only one interviewee presented them, this study may not provide a reliable view of the practices in the whole industry. It must also be taken under consideration that the age of the company, their size, and their company culture affect the way they report about cyber security to their boards and management. Since these factors were not directly examined in this study, it is difficult to evaluate their significance in the reporting methods.

Another limitation related to the data set is language. Sixteen of eighteen interviews were held in Finnish, which may affect how the results are displayed, as they had to be translated in English for this study. Whenever translated, the meanings can change slightly, even when the data analysis process is carried out as carefully as possible. This is due to semantic change, which means the process where the meaning of word changes in every language for many reasons. (Hasan, 2015).

6.4 Future research

This section presents the suggestions for future research. The proposed future research is based on the observations of this research and identified areas that require further research in order to form conclusions.

It was found that based on the data set of this research, which consisted of 18 CISOs, it was not possible to form further conclusions based on the size of the company. While connections were found between industries and the nature of the companies, there were no significant findings based on the company size. In order to study how cyber security reporting on board- and management level is done in large vs small companies, a larger data set would be needed. However, the subject is important and is a possible topic for future research.

Another interesting factor that could affect reporting cyber security to boards and management, is company culture. Former studies have already identified different types of company cultures, and specific reporting practices and methods could possibly be linked to them in the future studies. By identifying different cultures among companies who report about cyber security to their boards and management, and studying which reporting methods work for them, more specific tools could be introduced to specific culture groups.

Language is yet another important factor, that most likely has impact on board and management level cyber security reporting; for some boards and management, the reporting language is not their first language, which may affect how much they understand about the subject. Contrarily, when the reporting language is not English, due to semantic change the translations might change the meaning of the words, hence changing the message of the report. The future research could focus on what impact the reporting language has on the interest, understanding levels and interaction among boards and management.

7 CONCLUSION

In the beginning of this thesis, section **1.1 Research question and goals** introduced the research questions of this study. The main research question was "How can cyber security be reported effectively on board and management level?", while the two sub-questions were "What is the impact of visuality in board and management level cyber security reporting?" and "How has cyber security reporting on board and management level evolved? ".

This study presented a literature review, that focused on the history of reporting cyber security to boards and management, and how it is done now. The former literature has a united view of the state of the subject: Reporting cyber security to boards and management is extremely important, but the practice has not yet evolved to meet the expected quality. Generally, the subject is not addressed and prioritised as often as it should be, and the reporting methods are not efficient enough to achieve the goals of reporting. There are multiple reasons for this that we have been examined in this study; for example, cyber/information security executives use language and data that is too technical for the audience to understand, and there might be a lack of communication, which already could help improve the reporting.

The empirical part of the study was conducted by using semi-structured interviews, in which 18 CISOs from 13 different industries were interviewed. The data was analysed as presented in the section **4.2 Data analysis**, after which it was presented in the chapter 5**.** The results were also compared to existing literature.

When studying the results and trying to find a solution for ineffective cyber security reporting on board- and management level, a conclusion was made that none of the existing frameworks or "best practices" serve all organisations as they are. The needs of each organisation's board- and management level cyber reporting vary even inside one industry. However, there were certain practices, such as visualisation, that both the interview results and the existing literature supported. These practices have been harnessed into a form of a process model for creating an efficient reporting method for reporting cyber security on board and management level. This model is presented in FIGURE 12.

This study also studied the impact of visuality in board and management level cyber security reporting. The interviewees of this study were asked about how they use visuality in their reports, and the answers were compared to literature of different fields. The ways and amount of visualisation varied majorly between the interviewees. It was found, that visuality generally has major significance in board and management level cyber security reporting.

This research also aimed to answer the question regarding how cyber security reporting on board and management level has evolved. The conclusion was that it has improved overall and shifted towards more risk-based topics. However, there are still aspects that need to improve, for example, the frequency of reporting.

REFERENCES

Anderson C. Presenting and evaluating qualitative research. *American Journal of Pharmaseutical Education, 74(8)*. doi: 10.5688/aj7408141.

Aronson, J. (1995). A Pragmatic View of Thematic Analysis. The Qualitative Report, 2(1), 1-3

Atieno, P. (2009). An Analysis of the Strengths and Limitation of Qualitative and Quantitative Research Paradigms. In *Problems of education in the 21stcentury Volume 13,* pp. 13-18.

Bannister, A. (2021). When the screens went black: How NotPetya taught Maersk to rely on resilience – not luck – to mitigate future cyber-attacks. In *The Daily Swig: Cybersecurity news and views.* Retrieved from: https://portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks

Barbour, R.S. (2000). The role of qualitative research in broadening the "evidence base" for clinical practice. In *Journal of Evaluation in Clinical Practice, 6(2)*, pp.155–163.

Basias, N. & Pollalis, Y. (2018). Quantitative and Qualitative Research in Business & Technology: Justifying a Suitable Research Methodology.. In *Review of Integrative Business and Economics Research, Vol 7*, pp. 91-105. SIBR.

Baskerville, R. (1991). *Risk analysis: an interpretive feasibility tool in justifying information systems security.* School of Management, State University of New York, Binghamton

Bianco, S., Gasparini, F. & Schettini, R. (2014). Color Coding for Data Visualization. *Information Science Reference.* Information Resources Management Association, USA.

BoardEffect (2022). Board of Directors vs. Board of Management: What is the Difference? Effective March 3, 2022. https://www.boardeffect.com/blog/board-of-directors-vs-management/

Byrne, J. & Humble A.M. (2007). An Introduction to Mixed Method Research. Mount Saint Vincent University.

Cambridge Dictionary (2022). Social responsibility. Effective on May 31, 2022. https://dictionary.cambridge.org/dictionary/english/social-responsibility

Catal, C. & Diri, B. (2009). Investigating the effect of dataset size, metrics sets, and feature selection techniques on software fault prediction problem. *Information Sciences 179*, pp. 1040-1058. Elsevier.

Cerin, B. (2020). Cyber Security Risk is a Board-Level Issue. 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO). 384-388.

CFI (Corporate Finance Institute) (2022). What is a Shareholder? Effective February 18, 2022. https://corporatefinanceinstitute.com/resources/knowledge/finance/shareholder/

CFI (Corporate Finance Institute) (2022). Board of Directors. Effective February 18, 2022.

Clarke, V. & Braun, V. (2017). Thematic analysis. The journal of positive psychology, 12(3), 297-298.

Clinton, L., Higgins, J. & van der Oord, F. (2020) NACD *Director's Handbook on Cyber-Risk Oversight*. National Association of Corporate Directors.

Craigen, D., Diakun-Thibault, N & Purse, R. (2014) Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21. http://doi.org/10.22215/timreview/835

Cyentia Institute (2017). Cyber Balance Sheet, the 2017 Report. https://library.cyentia.com/report/report_001538.html

Cyentia Institute (2018). Cyber Balance Sheet, the 2018 Report. https://library.cyentia.com/report/report_002384.html

CSO (2022). How the CISO role is evolving. Effective March 3, 2022. https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html

Cybersecurity Ventures: Cybercrime Magazine (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Effective January 13, 2022. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Deloitte. (2019). Communicating the value of cybersecurity to boards and leadership. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/5002_Value-of-cyber-investments/DI_Value-of-cyber-investments.pdf

Deloitte. (2019). The future of cyber survey 2019: Cyber everywhere. Succeed anywhere. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf

Dezeure, F., Webster, G., Trost, J., Leverett, E., Gonçalves, J., Mana, P., Mccord, G. & Magri, J. (2022). Reporting Cyber Risk to Boards. CISO Edition. In *Dictionary*. Effective February 18, 2022. https://www.researchgate.net/publication/359338731_Reporting_Cyber_Risk_to_Boards_CISO_Edition

Directorpoint (2022). Cyber Security Becomes a Boardroom Priority. Effective on April 6, 2022. https://landing.directorpoint.com/risk-management/cyber-security-becomes-boardroom-priority/

Dobrygowski, D. (2022). How to prepare company boards for new cybersecurity rules. In *World Economic Forum.* Retrieved from https://www.weforum.org/agenda/2022/03/cybersecurity-rules-prepare/

Drake, V. (2022). OWASP: Threat Modeling. Effective of May 20, 2022. https://owasp.org/www-community/Threat_Modeling

Eckerson, W. & Hammond, M. (2011). Visual reporting and analysis. TDWI Best Practices Report. TDWI.

Eisenberg, H. (2014). Humans Process Visual Data Better. Thermopylae. Retrieved from https://www.t-sciences.com/news/humans-process-visual-data-better

Eisner, W. 1991. The enlightened eye, qualitative inquiry and the enhancement of educational practice. New York, Macmillan.

FIIF. (2022). Finnish Industrial Internet Forum. Cyber Security Becoming The First Priority In Companies. https://fiif.fi/news/cyber-security-becoming-the-first-priority-in-companies/

Gartner (2022). Effective on April 28, 2022. https://www.gartner.com/

Geach, D. (2021). Grid cyber security: secure by design, continuous threat monitoring, effective incident response and board oversight. In *Network Security,* June 2021, pp. 9-12.

Gleason, P., Clinton. L., Joyce, S. & Dobrygowski, D. (2021). Principles for Board Governance of Cyber Risk. Insight report, March 2021.

Groß, Thomas. (2020). Fidelity of Statistical Reporting in 10 Years of Cyber Security User Studies. Newcastle University.

Gupta, A. (2021). 15 Data Visualization Techniques (for Analysis & Presentation). Retrieved from https://www.polymersearch.com/blog/data-visualization

Gupta, A. (2022). 10 Good and Bad Examples of Data Visualization. Effective on May 31, 2022. https://www.polymersearch.com/blog/10-good-and-bad-examples-of-data-visualization

Hakoniemi, J-P. (2021). Case Vastaamo. Poliisiammattikorkeakoulu, Tampere.

Hancock B., Windridge K. & Ockleford E. (2007). An Introduction to Qualitative Research. The NIHR RDS EM / YH, 2007

Hanna, K.T. & Sales, F. (2021). Definition: Gap Analysis. https://www.techtarget.com/searchcio/definition/gap-analysis

Hasan, M. (2015). Semantic Change of Words Entered into Another Language Through the Process of Language Borrowing: a Case Study of Arabic Words in Bengali. In PEOPLE: *Problems of education in the 21stcentury Volume 13*, pp. 1375-1390.

Help Net Security. (2019). CISO role grows in stature, but challenges remain. https://www.helpnetsecurity.com/2019/09/24/ciso-role/

Price, N. (2019). Why Some Board Directors Still Don't Take Cybersecurity Seriously, Diligent. https://www.diligent.com/insights/cybersecurity/why-some-board-directors-dont-take-cybersecurity-seriously/

Hyun, E., Yang, D., Jung, H. & Hong, K. (2016). Women on Boards and Corporate Social Responsibility. Sustainability 2016, 8, 300. MDPI.

International Telecommunication Union (2022). Definition of cybersecurity. Effective February 11, 2022 https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx

Investopedia (2022). The Basics of Corporate Structure. Effective March 3, 2022. https://www.investopedia.com/articles/basics/03/022803.asp

ISO (International Organization for Standardization) (2022). ISO/IEC 27001

Information Security Management. Effective on April, 27. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

Irei, A. (2021). 6 ways to spur cybersecurity board engagement. SearchSecurity. https://www.techtarget.com/searchsecurity/feature/6-ways-to-spur-cybersecurity-board-engagement

ISTARI (2022). Where Should the CISO Report? Effective March 3, 2022. https://istari-global.com/insights/where-should-the-ciso-report/

IT Governance Ltd. (2022). What is Cyber Security? Definition and Best Practices. Effective February 9, 2022. https://www.itgovernance.co.uk/what-is-cybersecurity

Karjalainen, M. & Siponen, M. (2011). Toward a New Meta-Theory for Designing
Information Systems (IS) Security Training Approaches. The Journal of the Association for Information Systems, Volume 12, Issue 8, pp. 518 – 555.

Koivunen, E. (2021). Questions that help CISOs and boards have each other’s back. Help Net Security. Retrieved from: https://www.helpnetsecurity.com/2021/07/22/questions-board-members-security/

Kumar, A. (2020). Business Research Methodology. University of Lucknow. Retrieved from https://www.lkouniv.ac.in/site/writereaddata/siteContent/202004021910157977arvind_kumar_com_BRM_hypothesis_testing.pdf

Kwon, Ulmer & Wang. (2013) The Association between Top Management Involvement and Compensation and Information Security Breaches. *Journal of Information Systems, Vol 27*, pp. 219-236. American Accounting Association.

Law Insider (2022). Management Board Member definition. Effective february 18, 2022. https://www.lawinsider.com/dictionary/management-board-member

Legrand, T. (2016). *Weakest Links: Cyber Governance and the Threat to Mid-sized Enterprises.* Australian National University.

Lindberg, R. (2020). 6 Cybersecurity Metrics that financial institutions should not report to the BOD. *Rivial Data Security.* https://www.rivialsecurity.com/blog/cybersecurity-metrics-for-the-board

Madhani, P.M. (2017). Diverse Roles of Corporate Board: Review of Various Corporate Governance Theories. In *The IUP Journal of Corporate Governance, Vol. 16, No. 2, pp. 7-28.* SSRN.

Management study guide. (2022). Kotter's 8 step Model of Change. Effective on April 26, 2022. Retrieved from https://www.managementstudyguide.com/kotters-8-step-model-of-change.htm

Maschmeyer, L., Deibert, R.J. & Lindsay J.R. (2021).) A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society, *Journal of Information Technology & Politics, 18:1*, pp. 1-20.

McGrath, M. B & Brown, J. R . (2005). Visual learning for science and engineering, in *IEEE Computer Graphics and Applications, vol. 25, no. 5,* pp. 56-63, Sept.-Oct. 2005

McNamara, C. (1999) General Guidelines for Conducting Interviews. Sage, Minnesota.

Megalytic. (2017). 3 Ways to Make Your Analytics Reporting More Visual. Retrieved from https://www.megalytic.com/blog/3-ways-to-make-your-analytics-reporting-more-visual

Mir, S., Irshad, A. & Bilal, M. (2018). Investigating the denial of service attack: A major threat to internet and the security of information.

Myers, M.D. (1997). Qualitative Research in Information Systems. In *MIS Quarterly* (21:2), June 1997, pp. 241-242. *MISQ Discovery*

Nausheen, F. (2021). Data Visualization Examples: Good, Bad and Misleading. https://www.syntaxtechs.com/blog/data-visualization-examples

Newcomer, K.E., Hatry, H.P. & Wholey, J.S. (2015). Handbook of Practical Program Evaluation, 3rd Edition: Conducting Semi-Sturctured Interviews. Jossey Bass.

NIST (2022). Cybersecurity Framework. Effective on April 17, 2022. Retrieved from https://www.nist.gov/cyberframework

NIST (2022). Cybersecurity Incident. Effective on April 25, 2022. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity_incident

NIST (2022). Cybersecurity risk. Effective on April 25, 2022. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity_risk

NIST (2022). Threat. Effective on April 25, 2022. Retrieved from https://csrc.nist.gov/glossary/term/threat

O'Reilly, P. (2019). Risklens: The FAIR Model Explained in 90 Seconds. https://www.risklens.com/resource-center/blog/the-fair-model-in-90-seconds

O'Reilly, P. & Rigopoulos, K., et al.(2021). 2020 Cybersecurity and Privacy Annual Report. U.S. Department of Commerce.

Ošlejšek, R., Rusnak, V., Burská, K., Švábenský, V., Vykopal, J. & Cegan, J. (2021). Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training. In *IEEE Transactions on Visualization and Computer Graphics. 27.* IEEE.

Osterman research, Inc. (2016). *Reporting to the board: Where CISOs and the Board are Missing the Mark*. Osterman Research Inc.

Pollock, Tom (2022). The Difference Between Structured, Unstructured & Semi-Structured Interviews. OliverParks. Effective on March 11, 2022. https://www.oliverparks.com/blog-news/the-difference-between-structured-unstructured-amp-semi-structured-interviews

Puhakainen, P. & Siponen, M. 2010. Improving Employee's Compliance through IS Security Training: An Action Research Study. MIS Quarterly, 34(4), pp. 757-778.

PwC. (2019). PwC's 2019 Annual Corporate Directors Survey. Retrieved from https://www.pwc.com/us/en/services/governance-insights-center/assets/pwc-2019-annual-corporate-directors-survey-full-report-v2.pdf.pdf

Quispel, A., Maes, A. & Schilperoord, J. (2018). Aesthetics and Clarity in Information Visualization: The Designer's Perspective. In *Arts 2018 Vol. 7.* MDPI.

Rahdari, A. (2016). The Accountability Gap: Cybersecurity & Building a Culture of Responsibility. *Cyentia Cybersecurity Research Library.*

Rahman, M. M. (2019). Semi-Structured Interview: A Critical Analysis. ResearchGate,1-3. Retrieved from https://www.researchgate.net/publication/334277239_Semi-Structured_Interview_A_Critical_Analysis

Reliaquest (2022). The CISO's Guide to Metrics That Matter in 2022. Retrieved from https://www.reliaquest.com/resource/white-paper/the-cisos-guide-to-metrics-that-matter/

Robinson, Jones, Janicke & Maglaras. (2018). Developing cyber peacekeeping: Observation, monitoring and reporting. In *Government Information Quarterly Vol. 36,* pp. 276–293. Elsevier.

Rothrock, R.A., Kaplan, J. & Van der Oord, F. (2018) The Board's Role in Managing Cybersecurity Risks. *MIT SLOAN MANAGEMENT REVIEW, Winter 2018.* https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/

Safeopedia (2022). Color Coding. Effective on May 1, 2022. Retrieved from https://www.safeopedia.com/definition/5635/color-coding

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. In Journal of Digital Forensics, Security and Law, Vol. 12, pp. 53-74.

Schechter, S. (2013). Common Pitfalls in Writing about Security and Privacy Human Subjects Experiments, and How to Avoid Them. Microsoft.

Schwab, W. & Poujol, M. (2018). *The State of Industrial Cybersecurity 2018.* CXP Group.

SecurityScorecard (2020). The Importance of Cybersecurity Benchmarks for Organizations. Effective on April 27, 2022. https://securityscorecard.com/blog/security-ratings-benchmark-cybersecurity-program

Shayo, C., Lin, F. (2019) An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. In *Journal of Computer Science and Information Technology, Vol 7, No 1,* pp. 1-20. ISSN

Shea, S., Gillis, A.S. & Clark, C. (2021). *What is cybersecurity?* Security operations and management. Effective February 2, 2022. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Siponen, M., Klaavuniemi, T. (2021). Demystifying Beliefs about the Natural Sciences in IS. Journal of Information Technology 36(1).

Siponen, M., Soliman, W. & Holtkamp, P. (2021). Research Perspectives: Reconsidering the Role of Research Method Guidelines for Interpretive, Mixed Methods, and Design Science Research. Journal of the Association for Information Systems (2021) 22(4), pp. 1176-1196

Somers, A. (2020). Best Practices for Data Visualization. https://medium.com/analytics-vidhya/best-practices-for-data-visualization-d305c8340974. Analytics Vidhya.

Sridhara, V. (2020). CISOs: Quantifying cybersecurity for the board of directors. Help Net Security. Retrieved from: https://www.helpnetsecurity.com/2020/04/21/quantifying-cybersecurity/

Stobierski, T. (2021). Business Insight: Bad Data Visualization: 5 examples of misleading data. Harvard Business School. https://online.hbs.edu/blog/post/bad-data-visualization

Tervort, C. (2022). Rearchreporting: The Psychology of Visual Reporting. Retrieved from https://reachreporting.com/blog/the-psychology-of-visual-reporting

University of Birmingham (2022). Tips for effective presentation. Effective on may 2, 2022. Retrieved from https://www.birmingham.ac.uk/schools/metallurgy-materials/about/cases/tips-advice/presentation.aspx

University of Cincinnati (2022). Controlled Self Assessment. Effective on April 20, 2022. https://www.uc.edu/infosec/services/riskmgmt/csa.html

University of Northampton (2022). Quantitative, Qualitative and Mixed Methods. Effective on March 11, 2022. https://cpb-eu-w2.wpmucdn.com/mypad.northampton.ac.uk/dist/d/6334/files/2018/01/Quantitative-qualitative-and-Mixed-Methods-Jan-2018-1hvxxl1.pdf

Vaught, L. (2022). Phaseware: The Importance of Visual Data Reports. Retrieved from https://www.phaseware.com/phaseware-files-blog/the-importance-of-visual-data-reports

Xerox. (2017). 20 Ways to Share Color Knowledge. Xerox Coorporation. Retrieved from https://www.office.xerox.com/latest/COLFS-02UA.PDF

Yee, J., Walker, A. & Menzfield, L. (2012). The use of Design Visualisation Methods to support Decision Making. International Design Conference – DESIGN 2012, Dubrovnik.

Zeni, P. (2022). How Often Is Cybersecurity on Your Board's Agenda? In *Security Roundtable.* Retrieved from https://www.securityroundtable.org/how-often-is-cybersecurity-on-your-boards-agenda/

Zerlang, J. (2017). GDPR: a milestone in convergence for cybersecurity and compliance. In *Network Security*, June 2017, pp. 8-11.

Zongo, P. (2021). Getting Board Cyber Risk Reporting Right. In *Cyber Leadership Program: Embedding agile CISO driven governance.*

Zongo, P. (2021). Measure what matters – Board Cyber Risk Metrics. In *Cyber Leadership Program: Embedding agile CISO driven governance.*

APPENDIX 1 INTERVIEW FRAME

BACKGROUND

1. What organisations have you worked in with the CISO -title, and what is the organisation you are currently working as a CISO in?
2. What is the industry of your organisation?
3. What is the definition of management in your organisation when talking about cyber security reporting on board and management level?
4. How long have you been reporting to your board and management?
5. How have you tried to raise interest in your target group in the matter?
6. Has the interest grown in the past years, and how much?

CURRENT SITUATION

7. How often do you report to your board and management?
8. Are you using any models, frameworks, or templates when reporting?
9. What are the themes and topics you report about to your board and management?
10. Who is responsible for the reporting process? Who forms and sends the report?
11. Do you use quality assurance in your reporting?
12. Do you use external help in forming your report?
13. What is the reporting language?
14. How much do you generalise the language used in report? How technical is the language used?
15. How well do you explain the meaning of new terms when introducing them?
16. How well does your target group seem to understand the report?
17. Do you use visuality? How?
18. How does your target group react to the report? Do they comment or give feedback, or do they ask for explain something in further detail? Do they give recommendations?
19. How interested is your target group?

FUTURE AND IDEAL SITUATIONS

20. Do you feel that your reporting is in a good state?
21. Do you feel that your report gives an accurate view of the situation of your organisation's cyber security?
22. What could you improve your boards and management level cyber security reporting?
23. What would you describe as an ideal cyber security reporting state without considering resource and budget issues?
24. What measures are you taking to get to your ideal state of cyber security reporting?