TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Marita Müüdla 212029IVCM

Reporting of cybersecurity incidents among Estonian government and government-affiliated organizations

Master's thesis

Supervisor: Sille Arikas, MSc

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Marita Müüdla 212029IVCM

Küberintsidentidest teavitamine Eesti riigiasutustes ja riigi osalusega organisatsioonides

Magistritöö

Juhendaja: Sille Arikas, MSc

Tallinn 2024

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Marita Müüdla

04.01.2024

Abstract

In the dynamic realm of cybersecurity, the escalating frequency and sophistication of cyber threats present significant challenges to organizations globally. Incident reporting serves as a pivotal tool for establishing cybersecurity resilience, facilitating effective detection, response, and mitigation of security incidents. Although cybersecurity incident reporting is a critical aspect of an organization's defence against cyber threats, many organizations are hesitant to report cyber incidents to authorities due to different reasons.

This study addresses the trends and reasons behind hesitation of reporting the incidents. The study employs a qualitative research method in order to assess the reasons behind the hesitation to report cyber incidents and to analyse which incentives could motivate organizations to actively report cyber incidents. The scope of this study includes Estonian public sector and government-affiliated organizations. The research outcomes serve as valuable insights and recommendations tailored to the unique challenges faced by Estonian public entities.

This thesis is written in English and is 58 pages long, including 6 chapters, 15 figures and 7 tables.

Annotatsioon

Küberintsidentidest teavitamine Eesti riigiasutustes ja riigi osalusega organisatsioonides

Küberturvalisuse kiirelt muutuvas valdkonnas esitab küberohtude sagedus ja keerukus ülemaailmselt organisatsioonidele keerukaid väljakutseid. Küberintsidentidest teavitamine on küberturvalisuse vastupanuvõime keskne element, mis hõlbustab küberintsidentide tõhusat tuvastamist, neile reageerimist ja nende maandamist. Kuigi küberintsidentidest teavitamine on organisatsiooni kaitse seisukohalt kriitiline, ei raporteeri paljud organisatsioonid neid mõjutanud ja neis toimunud küberintsidente asutustele, kellele ka seadusest tulenev teavituskohustus sisse seatud on..

Magistritöö uurib küberintsidentidest teavitamise trende ning erinevaid põhjuseid, miks seadusest tulenevat kohustust küberintsidentidest teavitada, ei jälgita. Magistritöös on kasutatud kvalitatiivset uurimismeetodit, et hindamaks põhjuseid, miks organisatsioonid on küberintidentidest teavitamise osas kõhkleval seisukohal ja analüüsida, millised stiimulid võiksid organisatsioone innustada küberintsidente aktiivselt teistele osapooltele raporteerima. Magistritöö keskendub Eesti avaliku sektor ja riigi osalusega sihtasutuste küberintsidentide raporteerimisel kuna mainitud organisatsioonidel on seadusest tulenevalt kohustus oma küberintsidentidest teavitamiseks. Läbi viidud uuringu tulemusi on võimalik kasutada soovituste andmiseks teavitusprobleemide lahendamiseks, kohandamaks neid Eesti avaliku sektori iseloomulikele eripäradele.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 58 leheküljel, 6 peatükki, 15 joonist, 7 tabelit.

List of abbreviations and terms

CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
DDoS	Distributed Denial of Service
DPI	Data Protection Inspectorate
DPO	Data Protection Officer
DSP	Digital Service Provider
E-ITS	Estonian Information Security Standard
EISA	Estonian Information System Authority
EU	European Union
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
NCSC	National Cybersecurity Centre
NIS	Network and Information Systems
OES	Operators of Essential Services
PII	Personally Identifiable Information
UK	United Kingdom

Table of contents

List of figures

List of tables

1 Introduction

1.1 Motivation

In the ever-evolving landscape of cybersecurity, organizations are facing an increasing number of threats and challenges. Cybersecurity incidents have surged in frequency and sophistication, posing significant threats to organizations' data, infrastructure, and reputation. According to their annual report, a total of 27115 cyber incidents were reported to the Estonian National Computer Emergency Response Team (CERT-EE), operating under the Information System Authority (EISA) in Estonia, in 2022 [1], 2,672 of those had an impact on either the confidentiality, integrity, or availability of information or systems. Incident reporting is a critical aspect of cybersecurity, as it enables the organizations to detect, respond, and mitigate the impact of security incidents effectively. The potential consequences of inadequate incident reporting are far-reaching, affecting not only the targeted organizations, but also the security of individuals, their business partners, and in the worst-case scenarios the entire nations. While incident reporting is critical for collective cybersecurity resilience, many organizations face challenges in promptly and transparently reporting such incidents. Understanding the factors influencing incident reporting practices, identifying barriers and concerns as well as exploring incentives for proactive reporting, are essential to fortifying cybersecurity practices globally.

1.2 Scope and goal

This thesis seeks to identify the barriers that hinder transparent reporting and the incentives that could encourage more proactive disclosure. By investigating these aspects, this research endeavours to offer actionable insights that can advance incident reporting mechanisms, thereby enhancing the cybersecurity resilience of public entities in the face of evolving cyber threats.

This study focused on the public-sector and government-affiliated entities in Estonia. Public sector and government-affiliated entities were chosen as a target group since they have an obligation of reporting their cybersecurity incidents to CERT-EE operating under EISA. Private sector entities, who are not the operators of essential services do not have any mandatory reporting of their cybersecurity incidents and reporting their cybersecurity incidents to CERT-EE is voluntary. By concentrating on a specific geographic and institutional scope, the research aims to capture nuances unique to Estonian public sector and government-affiliated entities, in example the obligation to report their cybersecurity incidents. This narrowed focus enables a detailed investigation into the specific challenges and opportunities faced by these organizations, allowing for targeted recommendations and insights tailored to this sector. As a control mechanism, a subject matter expert interview has been introduced to validate the findings of the study.

1.3 Research questions

To reach the goal of the study, the author proposes the following research questions:

1. What are the key factors influencing an organization's incident reporting practices?

2. What are the primary barriers and concerns that deter organizations from reporting cybersecurity incidents?

3. What incentives can be introduced or improved to encourage organizations to report cyber incidents more proactively, ultimately leading to enhanced cybersecurity practices and resilience?

1.4 Novelty

The novelty of this research lies in its exploration of cybersecurity incident reporting practices within Estonian government organizations and government-affiliated entities, a perspective that has not been previously investigated within the cybersecurity landscape of Estonia.

Previous academic research has used a more quantitative approach to identify correlations, patterns, or relationships between variables using statistical methods. The focus of this study is to analyse the responses from qualitative perspective to understand the meaning, context, and trends within the data to establish an understanding of cybersecurity incident reporting trends.

Prior research has primarily relied on secondary data collected for purposes other than to analyse the reporting trends, more specifically reporting trends of government entities as well as government-affiliated organizations. The authors of these studies have also highlighted some discrepancies in their results due to the formulation of the questions used during the initial data collection. In contrast, this study also includes the creation of a specifically tailored questionnaire by the author, ensuring a unique perspective tailored to meet the research goals. Additionally, the data collection process has also directly facilitated by the author, encompassing both closed and open-ended questions, providing a deeper insight into the subject.

1.5 Outline of The Thesis

The crucial background data on incident reporting and the state of the art are provided in Chapter 2. The research methodology used in this study is described in Chapter 3. Key takeaways from the analysis have been presented in Chapter 4 along with the findings of the study. The author discusses the investigation and evaluates the findings in Chapter 5. The study is concluded in Chapter 6 along with the summary of the key findings, contributions, and implications.

2 Background

The number of incidents reported to CERT-EE has been in constant rise over the past 5 years. As indicated in Figure 1, the number of reported incidents has nearly tripled over the past six years. It is also relevant to mention that the number of reports include events and incidents reported both by government and private sector entities, as well as incidents that have been identified by CERT-EE's monitoring solutions.

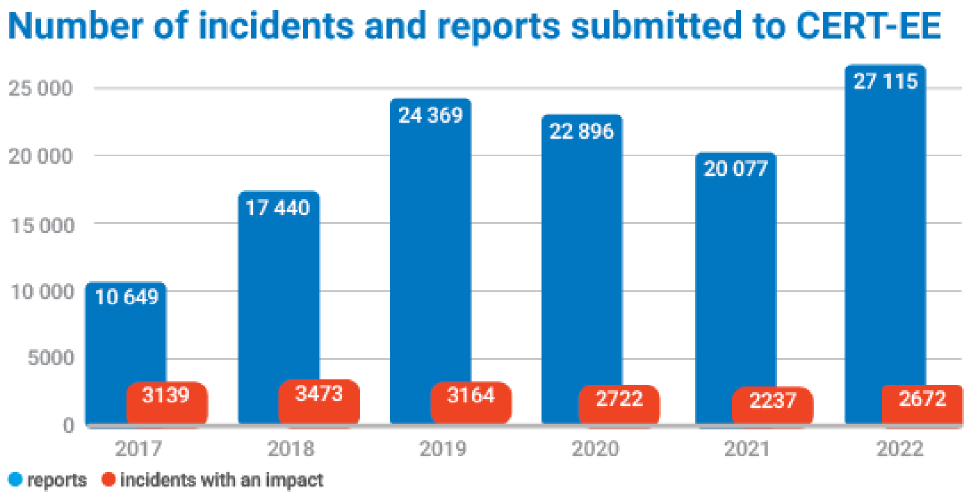

Figure 1. Number of incidents and reports submitted to CERT-EE [1].

Although the number of incidents with an impact has slightly decreased, the types of incidents reported in 2022, as seen in Figure 3, seem to be more diverse than in 2017 (Figure 2). The 2018 report [2] emphasizes that malware attacks were a significant concern, in the 2022 report, malware amounts to only around 3 percent of the incidents with an impact. The 2022 report emphasized a significant increase in phishing incidents that had an actual impact. Overall, this shift highlights the need for enhanced cybersecurity awareness and education, especially in identifying and mitigating different kind of cyber threats.

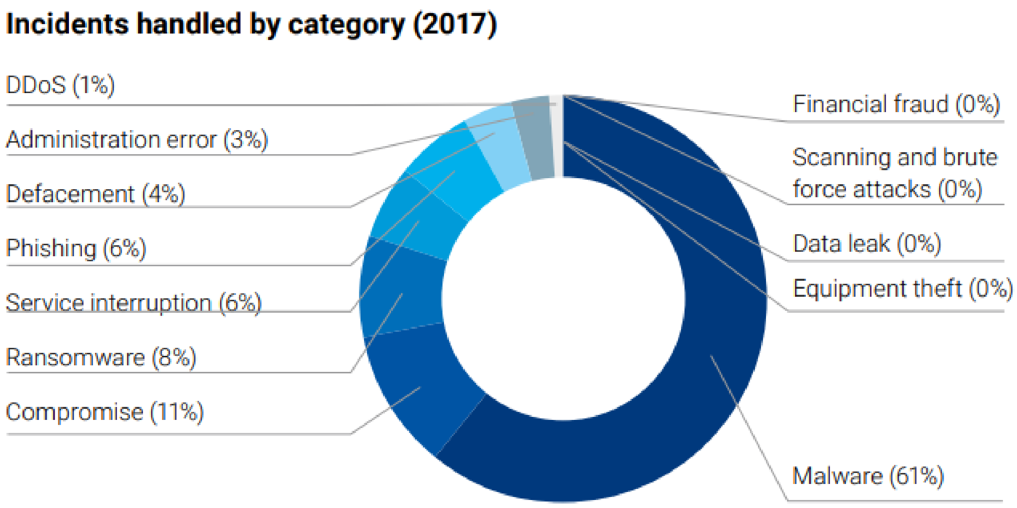

Figure 2. Incidents handled by category (2017) [2].

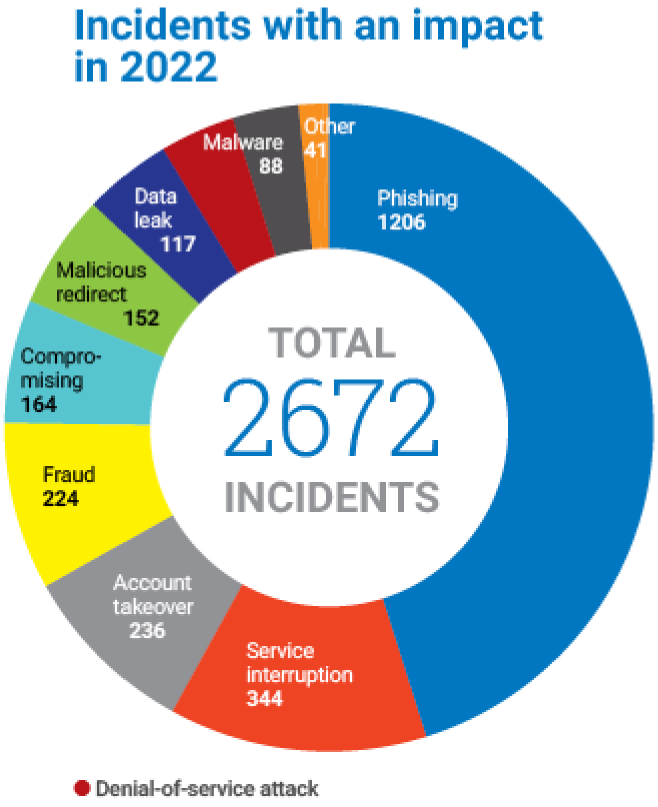

Figure 3. Incidents with an impact in 2022 [1].

When analysing reports of incidents ranging from malware attacks to phishing, data breaches, and Distributed Denial of Service (DDoS) attacks, the increasing complexity and volume of cyber threats is perceptible. The rising variety of the used methods of attacks indicates that threat actors have elaborated their operations and are employing various tactics to compromise systems.

2.1 Legislation, regulations, and standards

Estonia that is worldwide known for its digital prowess and forward-thinking approach to cybersecurity, has a well-established legal framework to govern reporting of incidents. Several laws and regulations apply, reflecting Estonia's commitment to maintaining the balance between digital innovation and security. For example, the Estonian Cybersecurity Act [3] is the most relevant act that addresses the country's approach to reporting of cyber incidents. The Cybersecurity Act mandates that all digital service providers and essential service operators must implement sufficient cybersecurity measures and report their significant cybersecurity incidents to the Estonian Information System Authority. Furthermore, the European Union's (EUs) Network and Information Systems (NIS) Directive, that dictates incident reporting as a legal requirement for operators of essential services and digital service providers in all EU member states, has been successfully adapted into Estonian law. By examining these regulations, we gain insight into the responsibilities of organizations and government entities concerning the reporting of cybersecurity incidents and how these regulations contribute to the nation's cyber resilience.

The Cybersecurity Act [3], established in 2018, and designed to enhance Estonia's overall cybersecurity posture, emphasizes the need for clear incident reporting procedures. This Act reflects Estonia's dedication to maintaining a secure digital environment and is particularly relevant in the context of the country's highly advanced digital infrastructure. In a world where cyber threats are evolving at an unprecedented pace - rapid and accurate incident reporting is crucial to ensuring resilience of the organizations. The Act provides a structured framework for addressing and reporting cybersecurity incidents, emphasizing the responsibilities of critical infrastructure operators, service providers, and government agencies. The Act encourages proactive risk management, rapid incident response, and international collaboration to counter cyber threats effectively. The Act also mandates the establishment and designation of national Computer Security Incident Response Teams (CSIRTs) and sets the expectations for their operations. For cybersecurity specialists, this Act serves as a framework that lays out their roles and responsibilities in handling and reporting incidents. Furthermore, the Act grants authorities the necessary powers to enforce cybersecurity measures and oversee compliance.

Estonian Information Security Standard (E-ITS) [4], managed by EISA, came in effect from January 2023 and replaced the IT baseline security system ISKE that was in effect between 2006 and 2022. The goal of E-ITS is to provide organizations with a tool for managing information security that is in Estonian and compliant with the legal framework of Estonia. This standard assists organizations in aligning their information security measures with their specific requirements, making cybersecurity activities achievable, even for smaller organizations in the Estonian context.

The Directive [5], adopted by the EU member states aims to standardize incident reporting and response processes across EU member states. It places obligations on Operators of Essential Services (OES) and Digital Service Providers (DSPs) to report significant incidents to the designated competent national authorities and outlines the measures to ensure the resilience and security of network and information systems. The Estonian Cybersecurity Act also incorporates elements of the NIS Directive, reinforcing Estonia's commitment to harmonizing its cybersecurity practices with those of the European Union.

International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001:2022 [6], the internationally recognized standard for Information Security Management Systems (ISMSs), plays a pivotal role in enhancing an organization's ability to report and manage cybersecurity incidents. ISO/IEC 27001:2022 mandates a risk-based approach to information security. By identifying and assessing risks, organizations can gain insights into potential vulnerabilities and threats, which are essential for effective incident reporting. The standard prescribes establishing an incident management process. This process defines roles and responsibilities, including those for reporting incidents. ISO/IEC 27001 emphasizes the importance of continual improvement. Incident reporting is not a one-time event; it requires ongoing adjustments and enhancements. Compliance with ISO/IEC 27001 often involves adhering to legal and regulatory requirements. This is crucial for reporting incidents promptly to relevant authorities, as non-compliance can result in severe consequences.

The General Data Protection Regulation (GDPR) [7] is globally one of the most known and influential data protection frameworks, impacting various facets of data management, including cybersecurity practices. While the GDPR is not solely concerned with cybersecurity incident reporting, it has engendered substantial changes in the way organizations handle data breaches and security incidents, making it a critical aspect or ensuring cybersecurity compliance. Based on the GDPR, the organizations are required to report certain data breaches to the appropriate data protection authorities within 72 hours after becoming aware of the breach. This requirement significantly impacts the incident reporting practices of organizations, prompting them to develop efficient and expedited mechanisms for identifying and responding to security incidents.

2.2 Related work

In response to the escalating threat of cyberattacks, cybersecurity incident response has garnered significant attention in research, underscoring the need for effective strategies and frameworks to combat cyber threats. Several studies have explored various facets of incident response and management, including reporting of cyber incidents, offering valuable insights into the ever-changing cybersecurity landscape.

A case study on the 2017 Equifax data breach conducted by Wang and Johnson [8] highlights the importance of communication related to cyber incidents. Despite detecting the breach on 29 July, Equifax delayed notifying the Federal Bureau of Investigation (FBI) of the breach and asking other third-parties for assistance until 2 August. Furthermore, the organization's Chief Executive Officer (CEO) was not informed of the breach until August 15, and the public statement was issued only on 7 September. This research focuses more on the public announcement of the cybersecurity incident and informing the affected citizens instead of incident reporting trends. However, the authors also emphasize the importance of promptly reporting and disclosing identified data breach incidents to avert legal penalties and negative public perceptions.

Another valuable reminder of the critical role that timely and transparent reporting plays in mitigating the impact of cyberattacks, is the 2016 Uber data breach incident. According to the press release by the U.S. Attorney's Office [9] Uber's Chief Security Officer (CSO) received the ransom demand from attackers on 14 November. Uber decided to conceal the breach from the affected customers and law enforcement and paid the attacker hoping that the attacker would delete the stolen data. The breach was discovered and disclosed by the new CEO in November 2017. Covering up the incident and data theft led to a fine, criminal prosecution, and reputational damage. Paljug and Mikac [10] also describe this cyber incident from a crisis management perspective. The authors argue that Uber is lucky to have survived considering the poor incident management. Rasalam and Elson [11] have even created a case study for students about the Equifax and Uber incidents from the perspective of management's ethical responsibility regarding cyber incidents.

A paper by Briggs et al. [12] examines the role of message design in cybersecurity incident reporting. The authors argue that the way that organizations communicate about incident reporting can influence whether employees report incidents or whether they rather cover them up. They conducted a study to investigate the factors that make messages about incident reporting effective. The decision not to report an incident was found to be influenced by the participants threat perception, the cost of responding, or the efficacy of reporting. One of the concerns for the authors was that participants were less likely to report security related error messages and more likely to report technical error messages. They conclude that the framing of the error message can significantly affect whether employees report incidents.

Koivunen [13] examined 6 real-life cases from National Cybersecurity Centre of Finland (NCSC-FI) archives, investigating the incident reporting from a different perspective. All real-life cases analysed in this study involve a third-party incident report, not by the victim itself, to NCSC-FI. The author suggests that the victim of an attack is often the last to know and organizations should accept incident reports from outside parties.

A study done by Laube and Böhme [14] investigates incident reporting from a financial perspective. A principal-agent model is developed to analyse the economic impact of mandatory data breach reporting to authorities. The authors aim to investigate the conditions under which the implementation of mandatory security breach reporting, coupled with audits and sanctions, influences firms to increase their investments in security measures and promotes the sharing of breach information. Specifically, the focus is on understanding the circumstances that lead to both a heightened overall level of information security and a reduction in social costs associated with security breaches. The authors argue that to encourage organizations to report breaches to authorities, security audits must be mandatory in addition to a breach notification law. Furthermore, when disclosure costs are greater than direct breach costs, it becomes counterproductive for organizations to report breaches to authorities. This is because the expenses of disclosure may outweigh the benefits of improving cybersecurity and preventing future breaches.

Tøndel et al. [15] conducted a literature review focusing on papers based on real-life incident management experiences and practices. They summarize key findings from 16 studies focusing on the Incident Response Lifecycle and compare those to the recommendations from ISO/IEC 27035:2011 standard [16]. They discuss all aspects of the Incident Response Lifecycle, including incident reporting.

A paper by Dezeure et al. [17] offers guidance for Chief Information Security Officers (CISOs) on effectively reporting cyber risk and its context to senior stakeholders, particularly Boards. The authors outline methods to engage in cyber risk management, communicate findings efficiently, and facilitate proper oversight. While the primary focus is on reporting to Boards, this can additionally be applied to reporting to other stakeholders like regulators, insurers, and clients.

An analysis of the United Kingdom (UK) Cyber Security Breaches Surveys from 2018, 2019, and 2020 by Kemp et al. [18] examines the likelihood of businesses reporting cybercrime victimization to external parties. According to descriptive statistics, 39.5 percent of the most disruptive situations affecting firms were reported to parties outside the organization, but only 8 percent were reported to public authorities. The results show that businesses are more inclined to report incidents like receiving fraudulent emails, hacking of their systems or bank accounts, and online impersonation of the organization compared to cases of malware infections. Furthermore, experiencing a negative impact from a cybercrime incident is positively associated with reporting to public entities. The study also highlighted the role of private cybersecurity companies and in-house cybersecurity teams in the reporting process. While businesses with outsourced cybersecurity management reported more to other organizations, they were less likely to report to public authorities. Conversely, organizations with internal cybersecurity teams showed a more positive, albeit weak, association with reporting to public authorities.

A study by Agbodoh-Falschau and Ravaonorohant [19] aims to assess the key organizational governance factors influencing the reporting of cybercrimes to law enforcement services in Canada. Their findings highlight that governance factors significantly impact cybersecurity measures thereby shaping the overall cybersecurity posture of organizations. The authors propose a framework that integrates resource-dependence theory and protection motivation theory, shedding light on the relationship between governance factors, incident intensity, and reporting to law enforcement. This framework, drawing on empirical evidence, has not been explored in the existing literature.

In an article by Easterly and Goldstein [20], it is highlighted that: “Sustainable cybersecurity will also require rethinking how governments and industries interact with one another. When most companies detect a cyber-intrusion, too often their default response is: call the lawyers, bring in an incident response firm, and share information only to the minimum extent required. They often neglect to report cyber-intrusions to the government for fear of regulatory liability and reputational damage. In today's highly connected world, this is a race to the bottom.”

In conclusion, the academic literature related to cybersecurity incident reporting is rather limited and most sources on the topic are reports addressing specific incidents' lessons learnt or postmortems. Nevertheless, these sources provide a diverse range of studies exploring various aspects of incident reporting, communication, and management. The case studies on high-profile incidents like the Equifax and Uber data breaches as well as the supply chain attack on SolarWinds underscore the critical importance of timely and transparent and most of all honest reporting of the incident to mitigate the impact of cyberattacks. The research also highlights the role of communication strategies, message design, and economic factors in influencing incident reporting behaviour within organizations. The study by Laube and Böhme emphasizes the impact of mandatory security breach reporting, coupled with audits and sanctions, on organizations' investments in cybersecurity. However, despite the valuable insights provided by existing literature, there remains a need for qualitative research to look more closely into the reasons why organizations hesitate to report cyber incidents. This study seeks to address this gap by exploring and analysing incentives that can be introduced or improved to encourage Estonian organizations to proactively report cyber incidents, contributing to a more comprehensive understanding of incident reporting dynamics.

3 Methodology

This research employs a mixed-methods approach in the form of an online survey to investigate the current landscape of cybersecurity incident reporting among Estonian public sector and government-affiliated organizations. Using a mixed-methods approach, the study combines quantitative and qualitative research techniques. Employing a combination of closed-ended and open-ended questions to collect a wide range of information, including both quantitative answers and narrative insights. Microsoft Forms was used to create the questionnaire. An overview of the survey can be found in Appendix 2 – Questionnaire. An expert interview with a representative of EISA has been conducted to validate the results of the survey.

In the scope of this survey are government-affiliated and public-sector entities. The questionnaire was distributed via e-mail to a total of 70 organizations. The e-mail addresses were gathered from the public websites of the entities and only distributed to the organizations that had contacts of a cybersecurity representative available on the website. The people who received the questionnaire were chosen according to their position within a particular organization. More precisely, positions and responsibilities that almost certainly are involved in reporting cyber incidents were the focus of attention. Those are for example chief information security officers, cybersecurity department managers, IT department managers, cybersecurity experts, etc. By reaching out to this expert community, the research aims to offer a deeper understanding of current practices, shed light on potential barriers, and, most importantly, enhance the overall cybersecurity posture of organizations.

Out of the 70 organizations approached for the study, 16 responded to the questionnaire which makes the response rate 22.8%. This means that the results of the study cannot be used for generalization for the entire public sector and government-affiliate organizations. Once the responses were collected through Microsoft Forms, the raw data was exported to Microsoft Excel for initial processing and analysis. The author utilized Excel's graphical features to create visual representations such as charts to illustrate the findings obtained from the dataset. The responses to the open-ended questions were organized based on the research questions. Afterward, the data was interpreted, exploring the connections, and drawing conclusions about the overall findings. The answers displayed in the data tables were modified only to improve grammatical correction. Additionally, some responses to the survey were provided in Estonian and subsequently translated into English to ensure data consistency.

To protect the confidentiality and privacy of the participants, ethical considerations were prioritized in this study. Ethical considerations in this study involve safeguarding respondents' confidentiality, ensuring anonymity in data analysis, and securing sensitive information shared by participating organizations. The research will adhere to ethical guidelines and data protection laws to maintain the integrity and privacy of the organizations and individuals involved. An anonymous questionnaire was utilized to make sure that no personally identifiable information (PII) was gathered throughout the survey procedure. By not collecting any PII, the study mitigated the chance of disclosing confidential information. By using this approach, all comments will remain anonymous, which prevents any response from being linked to a participant's identity or organization of employment. In compliance with ethical research guidelines, participants were also informed of the study's purpose and the confidentiality of the responses.

For validation of the obtained results, an expert interview was conducted with a representative from EISA. The expert was introduced to the results of the studies and was asked to validate the correlation between the results of the study and the trends of reporting cybersecurity incidents to EISA over the past 3 years.

The study's scope, concentrating on public-sector entities and government-affiliated organizations in Estonia may introduce certain limitations. Due to the specialized focus, the outcomes may not comprehensively represent incident reporting practices in other industries outside the public sector and government-affiliated organizations that are responsible for reporting their cybersecurity incidents to EISA since establishment of ISKE in 2004.

4 Analysis and results

The study's sample consisted of 16 organizations, including ministries, government agencies, state offices, state-owned companies, hospitals owned by local governments, and foundations established by the state. Although the sample size might appear relatively small it is important to consider the narrow focus of this study. Different organization sizes are represented in the sample, including small, medium, and large organizations. Only micro-enterprises with less than 10 employees are not present in the sample which is understandable considering the focus of the study. Many of the replies (9) came from organizations with over 250 employees, as visible in Figure 4.

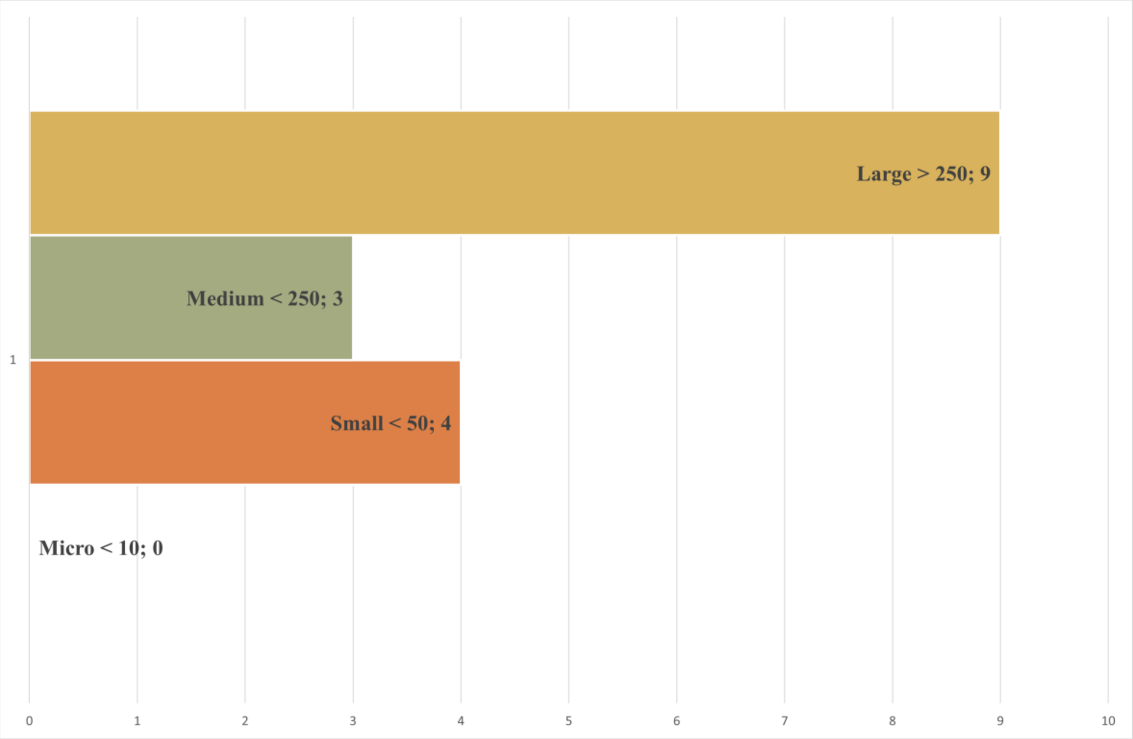

Figure 4. Size of the organization.

The people responsible for cybersecurity incident management were specifically targeted to ensure the quality of the data. The survey respondents represent various key roles related to information security and technology management within organizations. The roles listed in the open-ended answer field resulted in a wide array of job titles being reported, reflecting the diverse roles held by the respondents. To manage this diversity and facilitate a more coherent analysis, these job titles were consolidated into three primary categories: cybersecurity-related management positions, general IT management positions and data protection related positions.

Figure 5 illustrates the distribution of these roles among the survey participants. Half of the respondents hold a general IT Manager position, seven respondents are identified with the role of CISO, and one respondent holds the Data Protection Officer (DPO) position. This distribution of varied professional roles contributes to the overall diversity and expertise within the surveyed organizations.

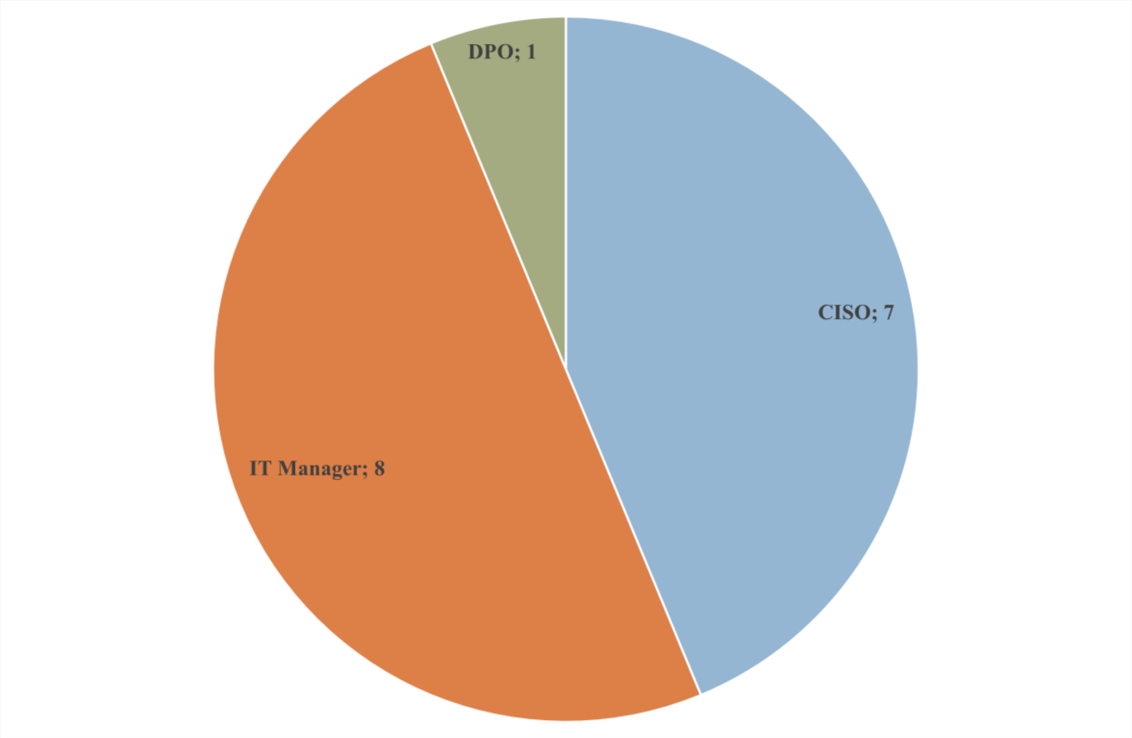

Figure 5. Role within the organization.

The field of operation might also impact how organizations handle and report cybersecurity incidents. The diverse range of various sectors in the sample of this study includes Technology and Cybersecurity, Healthcare, Education, Energy and Utilities, Public Sector, Transportation and Logistics, Natural Resources, Telecommunications as visible in Figure 6. The varied representation in the sample enhances the comprehensiveness of insights gathered, considering the unique challenges specific to each sector.

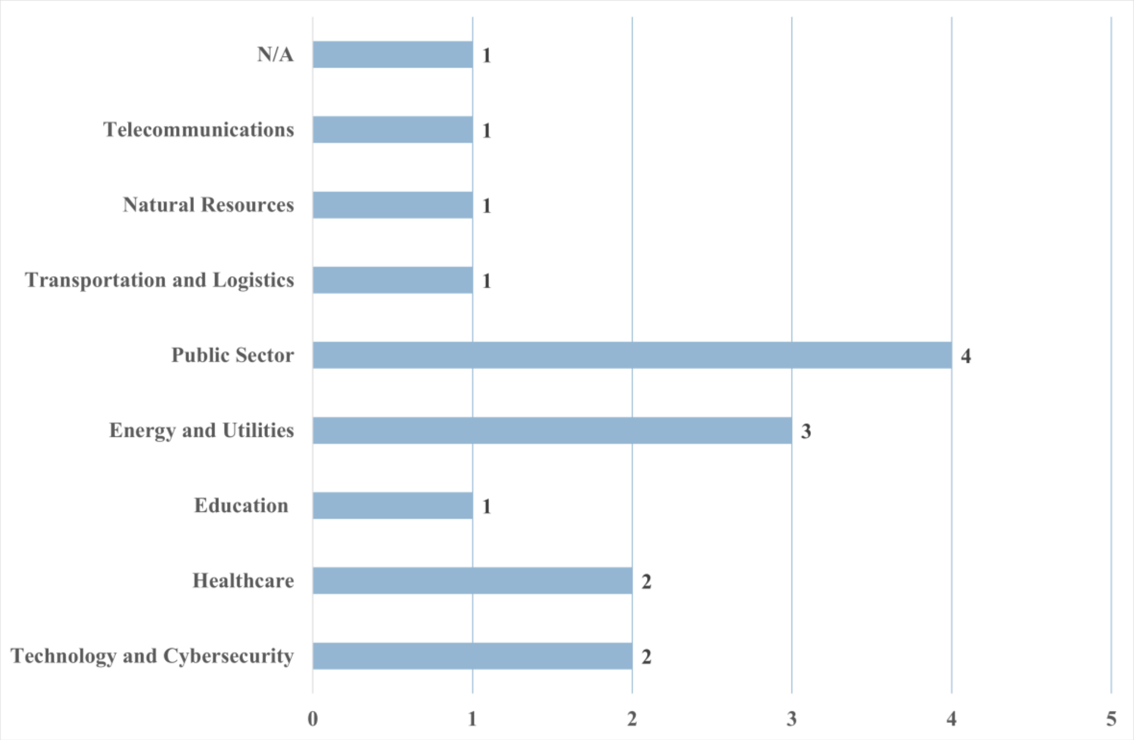

Figure 6. Field of operation.

4.1 Incident Reporting Practices

While most respondents indicated their organizations' adherence to relevant regulations, there were 2 respondents who stated that their organizations do not need to comply with any regulations, as visible in Figure 7. However, given the scope of the study, it is highly probable that these organizations do fall under certain regulatory requirements, and the respondents may not even be aware of their incident reporting obligation. This discrepancy might suggest a potential lack of awareness or understanding about the regulatory obligations pertinent to their respective sectors. This observation raises an important point about the necessity for increased regulatory awareness and education, particularly in fields where compliance is critical. It underscores the need for organizations to ensure that their employees, especially those in decision-making or influential positions, are well-informed about the legal and regulatory frameworks that govern their operations.

A total of 8 respondents mentioned that their organization must comply with E-ITS. Cybersecurity Act, Personal Data Protection Act, and Public Information Act cover a wide range of areas from cybersecurity protocols to data privacy and public information dissemination. Additionally, there were mentions of several requirements under the NIS

Directive, GDPR, and ISO27001 standard. These regulations and standards are pivotal in shaping the operational protocols for handling sensitive information and securing digital infrastructures. Furthermore, some respondents indicated mandatory compliance with various Estonian or EU regulations without delving into specific details. This indicates a recognition of a broader regulatory framework, albeit without explicit mention of individual laws or directives. This complex regulatory landscape reflects the necessity for organizations to navigate and comply with a diverse set of guidelines shaping the cybersecurity environment. The diversity of these regulations, each with its own set of guidelines and requirements, presents a significant challenge for organizations, particularly those operating across cross-border jurisdictions or sectors. It requires a diligent approach to compliance management, continual education and awareness of the evolving regulatory space, and effective implementation of compliance strategies. Organizations must not only be aware of these diverse regulations but also ensure they are integrated into their operational and security frameworks. Such comprehensive compliance is essential for protecting the organization's interests, maintaining trust with stakeholders, and upholding legal and ethical standards in an increasingly interconnected and regulated digital world.

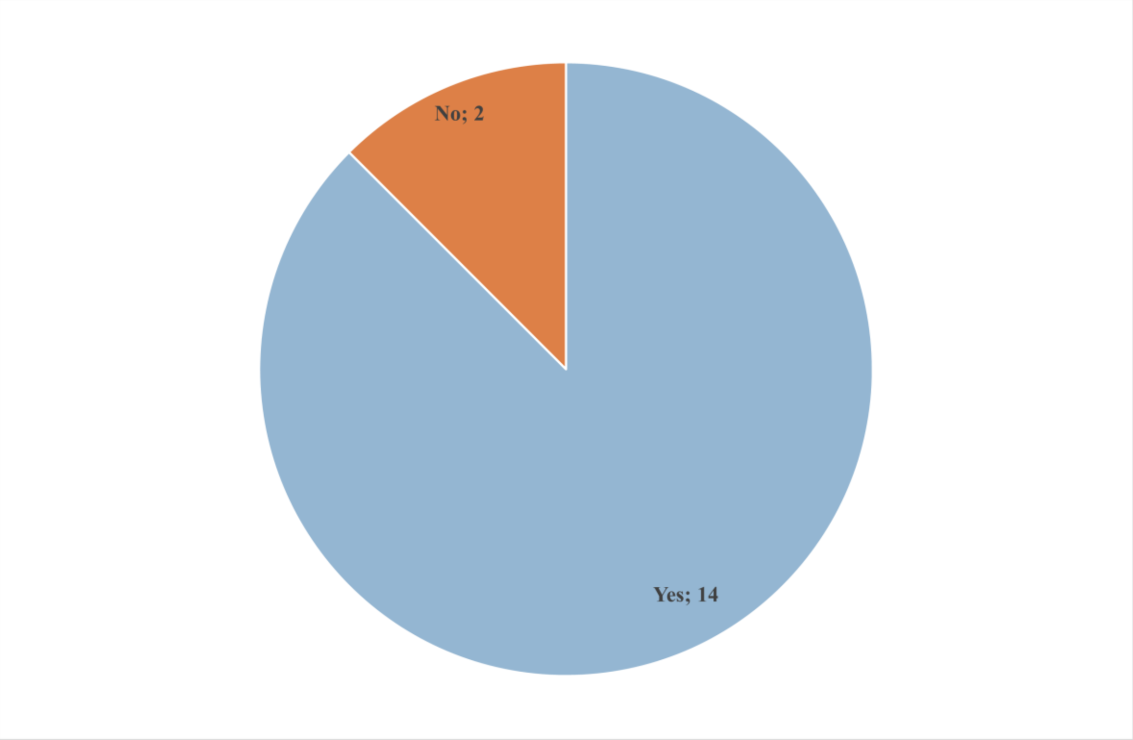

Figure 7. Organizations that must comply with requirements or regulations.

It was observed that nearly all the organizations represented in the sample have established internal incidents reporting processes, with only one respondent indicating the absence of these measures. Nevertheless, while most respondents acknowledged the existence of incident reporting processes within their organizations, 3 of the respondents refrained from providing detailed descriptions of these procedures. This reticence might be due to confidentiality concerns or the proprietary nature of their internal processes. The most common response among the participants was that their incident reporting processes are described in detail in their internal documents, though no further specifics were provided in the survey. This suggests a formalized approach to incident management, although with limited external visibility into the exact nature of these processes. Additionally, 3 respondents highlighted that their processes involve notifying external entities such as EISA, CERT-EE, or other regulatory bodies like DPA in the event of an incident. This reflects a broader engagement with national and international cybersecurity frameworks and underlines the importance of collaboration with external agencies in incident management and response.

As for the applicability of these protocols, responses indicated a range of targets within the organizations. Some respondents stated that their processes apply to all employees, encompassing every individual regardless of their role. Others specified that the processes are particularly relevant for users and IT staff, as well as colleagues who are directly involved in detecting or responding to cybersecurity incidents. A few responses even extended the scope to include ministry and government-level entities, suggesting a comprehensive and wide-reaching approach to incident reporting and management. Overall, these findings reveal a good level of awareness and implementation of internal incident reporting processes across the surveyed organizations. Although specific procedures were not elaborated, it is encouraging to note that such procedures have been established. Since only 3 participants opted not to provide a response, indicating a generally high level of engagement and commitment to cybersecurity practices among the surveyed entities. This reflects positively on the cybersecurity posture and readiness within these organizations, underscoring the importance of proactive measures in the current cybersecurity landscape. An overview of the provided descriptions is visible in Table 1.

Table 1. Application of incident reporting protocols.

To employees and IT staff
All workers
Regarding information security incidents, informing CERT-EE and related partners, if the incident leads to disruption or interruption of the provision of vital services, then also informing the Health Board.
The institution's internal regulations oblige all employees to inform about information security incidents
Notifying cert@cert.ee of e-mails that seem suspicious. there are no other protocols
Internal rules
If incident -> notify EISA. There is one contact person who's doing the communication
Reporting protocols and guidelines are aimed at users and IT staff
Reporting form in document management system. For all employees.
Processes for how and to whom cyber incidents and data protection violations are reported are agreed upon in internal documents.
The protocols/guidelines are aimed at all the colleagues that might have connection to detecting or responding to incidents.
They are aimed at ministry and government

A total of 12 organizations reported experiencing a cybersecurity incident within the past year, as visible in Figure 8. Most of them, 11 organizations, took the proactive step of disclosing these incidents to external entities or authorities. This action demonstrates a commitment to transparency and regulatory compliance, as well as an understanding of the importance of sharing information about cybersecurity threats.

However, 1 organization chose not to report the incident externally, and although the questionnaire included a space to provide reasons for not reporting, the organization did not specify why they chose not to disclose the incident. The lack of elaboration from this organization is particularly noteworthy, as understanding the barriers and concerns that deter organizations from reporting cybersecurity incidents is crucial for the study. Without this information, it becomes challenging to fully comprehend the factors that influence an organization's decision to withhold information about cybersecurity incidents.

Furthermore, while several respondents did report incidents, many chose not to disclose detailed information about the specific nature of these cybersecurity incidents in the survey. This restraint might be attributed to concerns about confidentiality, the sensitivity of the information, or organizational policies regarding information disclosure. Among those who did provide descriptions, a diverse range of incidents was highlighted, visible in Table 2. These included phishing campaigns, disruptions in IT services due to technical issues, and unintentional data exposure due to misconfigurations. Additionally, some organizations faced availability incidents, while others reported violations of physical perimeter security requirements and malware infections.

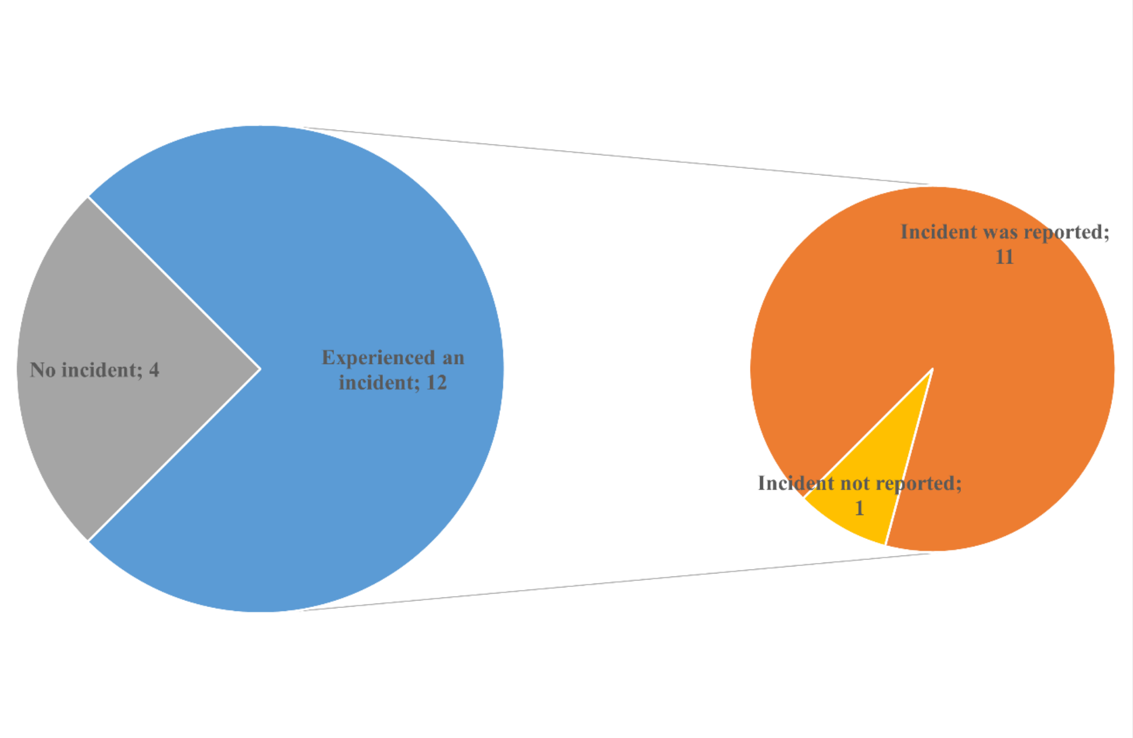

Figure 8. Incidents experienced and incidents reported.

Table 2. Descriptions of incidents experienced in the past year.

Phishing campaigns - user feedback and automated feedback from monitoring
Smaller interruptions of IT services, which so far have not been related to an external attack or the examples given in the question, but to technical problems with the IT infrastructure.
Possible and very scope + time limited unintended data exposure due to misconfiguration. Not malicious.
Availability incidents, in all cases related to ISPs service
We define cybersecurity incidents all incidents even the reason is personal, device, or software fault. We have had no cyber incidents what are caused by external factors, but we had incidents caused by personal or device failure for instance.
Violation of physical perimeter security requirements
Among other types of malware infections were detected via regular scans.

Among the 4 participants who reported not experiencing any cybersecurity incidents in the past year, 3 indicated having monitoring systems in place, while 1 did not provide information regarding the presence or absence of monitoring solutions. In author's opinion, this suggests that these organizations possess the capability to detect potential cybersecurity incidents. However, the author views this with a degree of scepticism. Given the prevalence and sophistication of cyber threats in the current digital landscape, it seems plausible that at least some suspicious activities or anomalies would have been flagged by these monitoring systems. The absence of any reported incidents, despite having monitoring mechanisms in place, raises questions about the used baselines of criteria to classify events as incidents. Adding to this perspective, one participant elaborated that their monitoring is conducted by a third-party service provider. According to this respondent, any suspicions raised through this external monitoring are then investigated by their internal IT team. They noted, "So far there have only been suspicions, which are not incidents." This statement implies a distinction being made between suspicious events and incidents, suggesting a threshold or criteria that an event must meet to be classified as an incident.

When queried about the responsibility for reporting a cybersecurity incident to management within their organizations, a majority of 14 respondents identified the IT/security team as the primary entity responsible for such reporting, as visible in Figure 9. Additionally, one respondent specifically mentioned CISO as the responsible party.

Contrastingly, one organization presented a different approach, stating that they do not have a designated department or role specifically assigned for reporting cybersecurity incidents. In this case, the responsibility is somewhat ambiguously covered by the IT department. This lack of a clear, designated reporting channel could potentially lead to inefficiencies or delays in communicating important security information to the management.

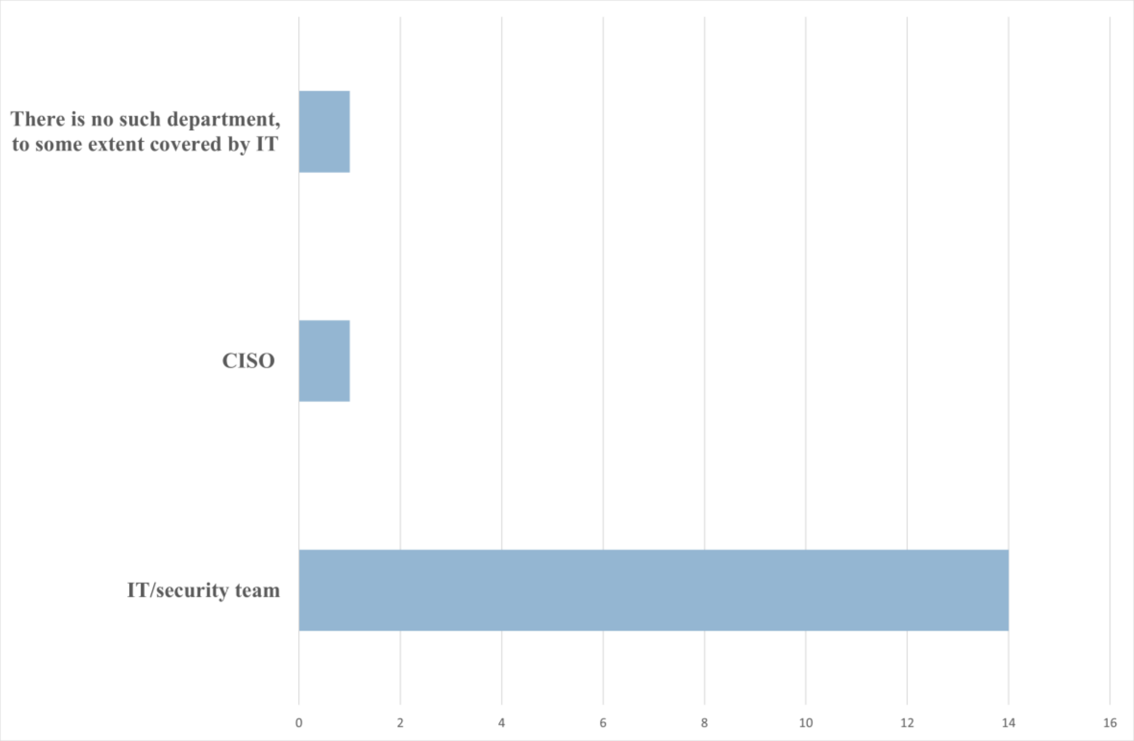

Figure 9. Responsible position for reporting cybersecurity incidents to management.

In terms of reporting a cybersecurity incident to regulatory authorities, 11 respondents identified the IT/security team as the responsible party, visible in Figure 10. This finding suggests a common organizational practice where the teams directly involved in cybersecurity and IT management are also entrusted with the task of communicating with regulatory bodies. The IT or security team's involvement in this process is justified, given their expertise and firsthand knowledge of the incidents, ensuring accurate and timely reporting to authorities. In addition to the IT/security team, three respondents pointed out that their senior management representative plays a key role in this process. This could indicate that in these organizations' cybersecurity incidents are not seen as just technical issues, but also as matters of strategic importance that warrant senior management's attention and intervention. Interestingly, the responses also included two mentions of a DPO or IT manager/CISO as the responsible position for reporting the incidents to regulatory authorities. The author expresses scepticism regarding the technical expertise of a DPO in terms of their ability to provide detailed and technically nuanced reports of cybersecurity incidents to regulatory authorities. This concern stems from the typical role of a DPO, which is often more focused on compliance with data protection laws and regulations rather than the technical aspects of cybersecurity.

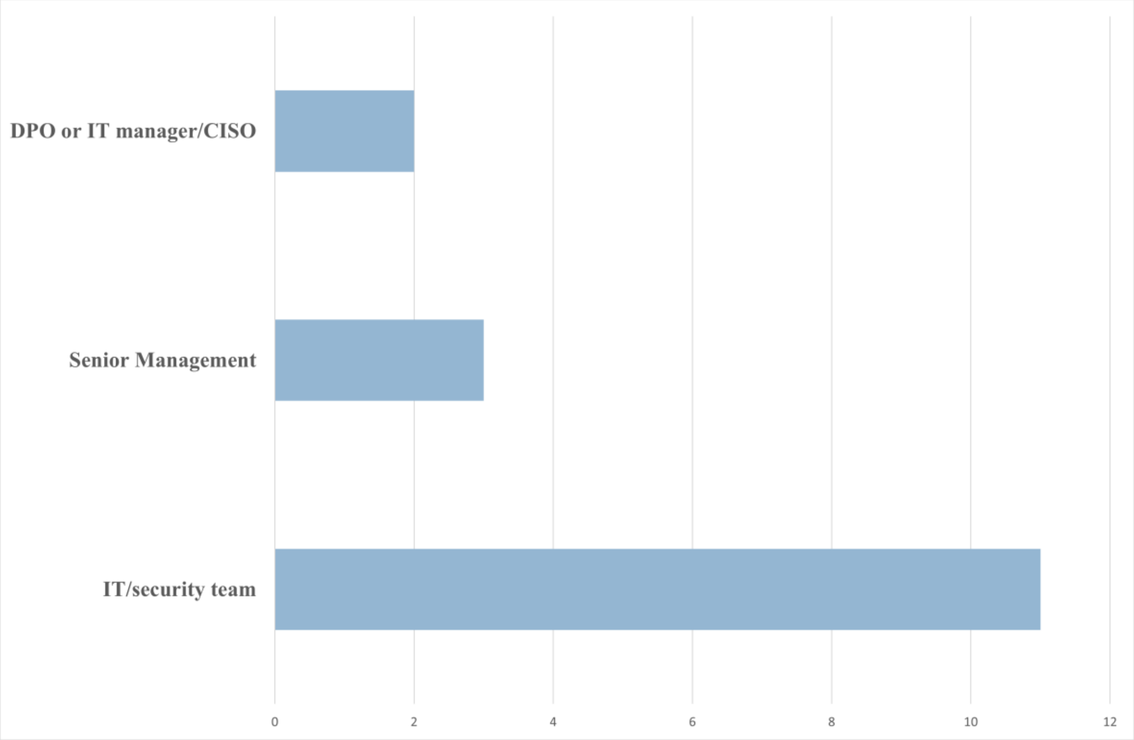

Figure 10. Responsible position for reporting cybersecurity incidents to regulatory authorities.

Regarding the authorization for reporting to regulatory authorities, 11 organizations indicated that the IT/security team holds this authority, as visible in Figure 11. This reflects a common organizational structure where the teams directly involved in managing cybersecurity risks and implementing security measures are also entrusted with the critical task of the authorization of reporting to authorities. The remaining responses attributed this to various management roles, including CISO, DPO, IT manager, and higher executive management. This can indicate a broader approach, where senior personnel or those in specialized roles are tasked with the responsibility of authorizing communications with authorities. One organization, however, chose not to disclose this information.

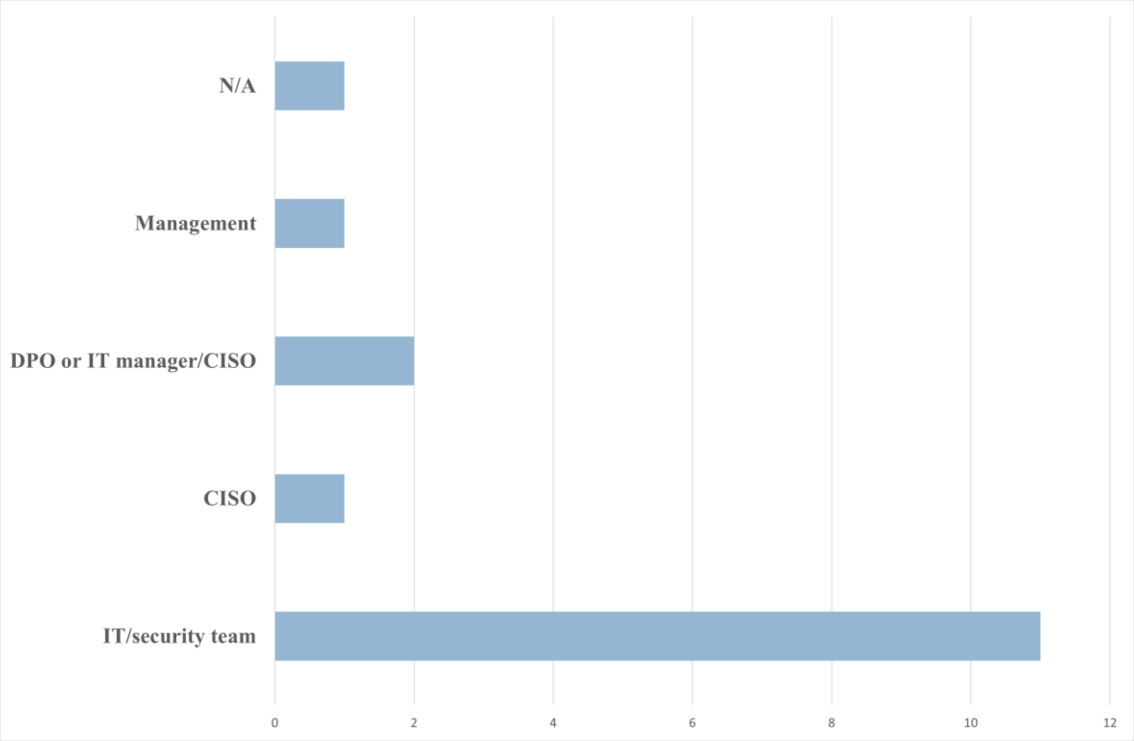

Figure 11. Position authorizing reporting cybersecurity incidents to authorities.

For organizations that specified the entities or authorities to which they report cybersecurity incidents, the majority, consisting of 9 organizations, mentioned reporting their incidents to the EISA, visible in Figure 12. Interestingly, 4 organizations indicated reporting to CERT-EE, which is part of EISA. The author finds it understandable that many organizations reported their cybersecurity incidents to EISA, the central authority in Estonia's cybersecurity framework, and CERT-EE, as a specialized emergency response team within the EISA structure, as these choices align closely with the stipulations of the Estonian Cybersecurity Act. Furthermore, 4 organizations specified the Data Protection Inspectorate (DPI) as their point of contact for reporting these cybersecurity incidents. The involvement of DPI, responsible for data protection oversight, underscores the critical intersection of cybersecurity with data privacy. This indicates that for these organizations, incidents might have had data protection implications, necessitating a report to the data protection regulatory body.

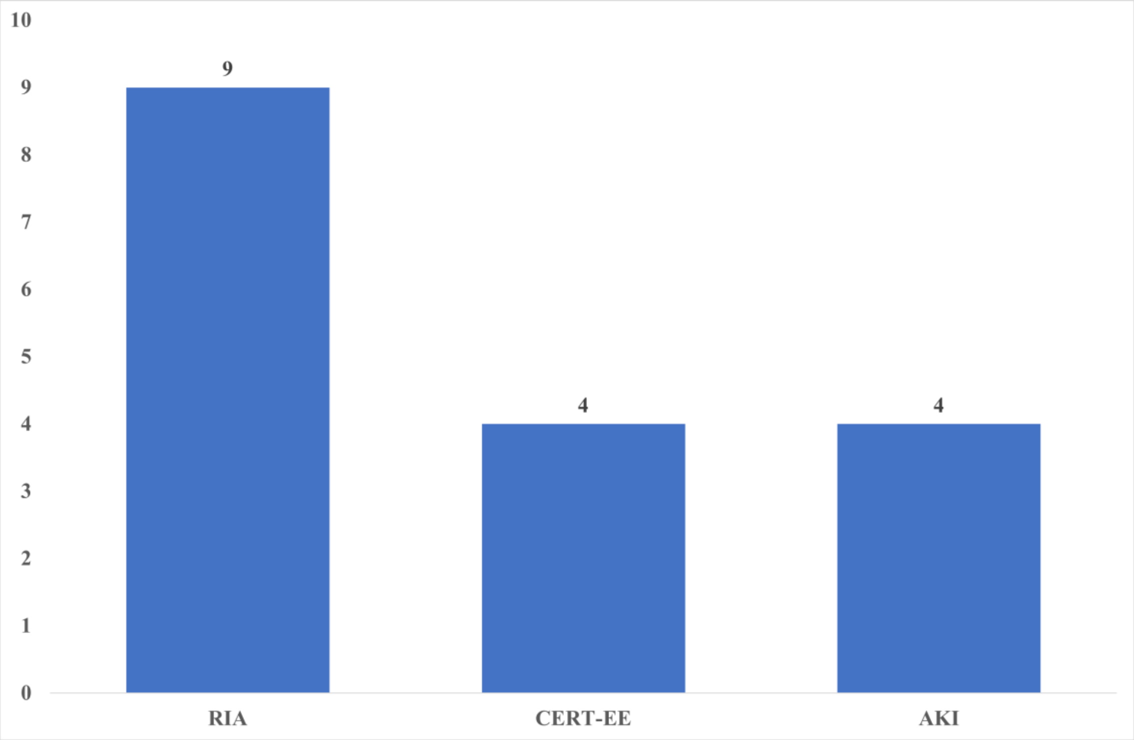

Figure 12. Regulatory authorities where cybersecurity incidents were reported to.

4.2 Barriers to Reporting

The overview of the survey participants' perspectives on their decision-making processes regarding the reporting of cybersecurity incidents can be seen in Table 3. These responses reveal an approach to incident reporting that is heavily influenced by the severity and impact of the incidents on the organizations’ operations. Several respondents highlighted that the decision to report is contingent on the seriousness of the incident, with a commitment to disclose incidents externally when they significantly disrupt daily operations. However, there is also an acknowledgment of incidents that are not reported due to their perceived minor nature or internal resolution. This indicates a level of ambiguity and complexity in determining the reportability of incidents, underscoring the need for clear guidelines and criteria.

Additionally, there are mentions of practical considerations, like personal convenience, and the need for employee training to recognize incidents that must be reported, suggesting that factors beyond the incident itself, such as organizational culture and capacity, play a significant role in the decision-making process.

Furthermore, a few respondents acknowledged a sense of obligation towards reporting cybersecurity incidents, particularly when guided by regulatory requirements or organizational policies. This indicates an understanding that, in the absence of legal or procedural mandates, certain incidents might not be reported to external authorities.

The author anticipated more detailed responses to the open-ended question regarding primary reasons for not reporting cybersecurity incident. However, out of 16 respondents, only 12 chose to provide answers to this question. The lack of detailed elaboration left the author with a somewhat incomplete picture of the full range of barriers and challenges organizations face in this area.

Table 3. Primary barriers to reporting.

Everything depends on the seriousness of the incident(s)
We always do
Notifications are not sent if it is an incident, the causes of which are clearly internal to the organization and the impact of the incident is not significant.
There hasn't been anything to report…Yet
Minor incidents, minimal risk, and no significant influence.
In our case none. Incidents with real impact have and will be reported.
Not mandatory = Won't report
Employees need instructions to recognize what really are incidents.
Personal convenience.
It is not always clear whether the potential impact of an incident is such that it needs to be reported
It depends on the cybersecurity incident and whether it should be reported to external partners.
Obligation from law and procedures

Many respondents, 10 out of 16, associate incident reporting with reputational damage, as visible in Figure 13. Those 6 respondents who did not perceive incident reporting as linked to reputational damage provided additional insights that shed light on different perspectives and organizational cultures. Some comments suggested a more open and transparent approach to handling security incidents, such as "Communication about security incidents is not shamed". This comment implies a culture where openness about cybersecurity issues is not viewed negatively but perhaps seen as a sign of diligence and transparency. Another respondent pointed out “It is a regulated obligation. We can have external help when we report.”. This highlights that for some organizations, the decision to report is less about reputational considerations and more about compliance with legal and regulatory requirements. Additionally, the comment "Incidents and related notifications to competent authorities are restricted information meant for internal use only" reflects a stance where the confidentiality of incident reporting is paramount.

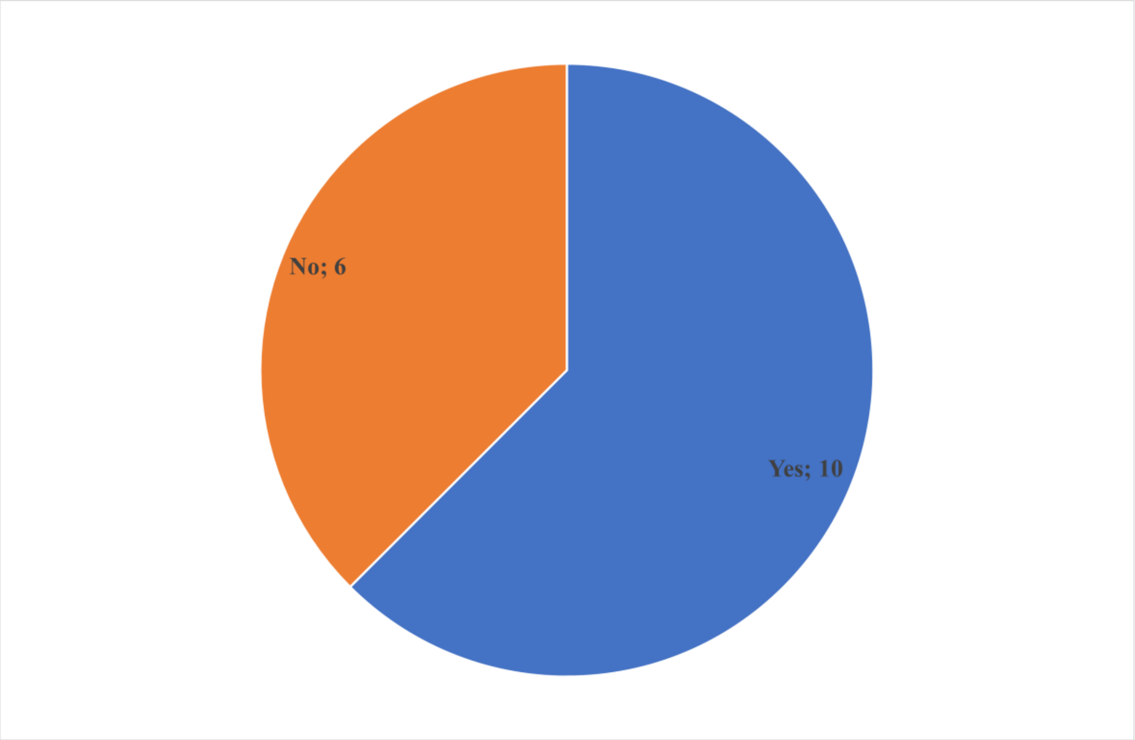

Figure 13. Concerns about reputation damage associated with reporting incidents.

The average significance of the concern about reputational damage associated with cyber incident reporting on a scale of 1 to 5 is 3.4, as visible in Figure 14. This indicates a moderate to significant level of worry among the respondents about the potential negative impact on their organization's reputation when a cybersecurity incident is reported. According to the author's perspective, an average score like this suggests that while reputational damage is not overwhelmingly seen as a critical deterrent, which would be closer to 5, it is nonetheless a substantial factor in the decision-making process around incident reporting. From one side, there is a need for transparency and compliance with regulatory requirements that mandate reporting of certain incidents. From the other side, there is apprehension about how the public disclosure of a security breach could affect the organization's public image.

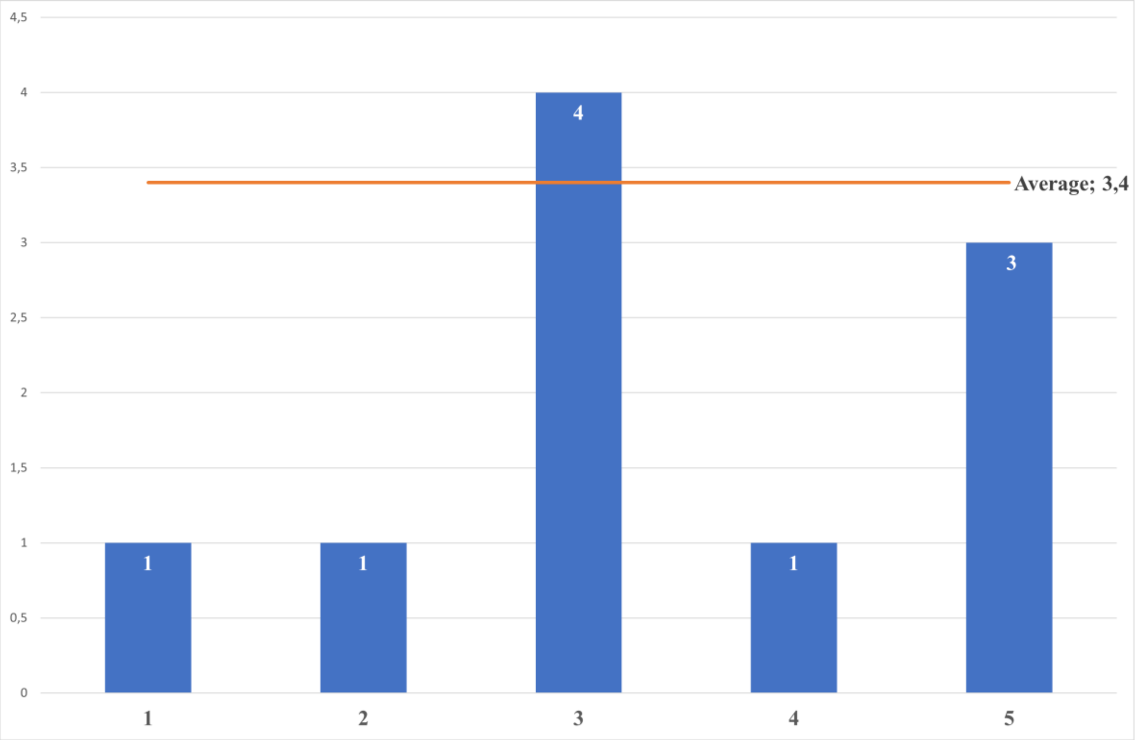

Figure 14. Level of concern about reputational damage.

The incentives that would encourage reporting cyber incidents have been gathered to Table 4. A total of 10 respondents took the effort to answer this question, a range of perspectives emerged, reflecting diverse motivations and considerations in the decision-making process related to incident reporting. One respondent highlighted their existing cooperation with EISA in reporting incidents, suggesting that established relationships and collaboration with cybersecurity authorities can be an incentive. Another respondent pointed out that while concern for reputation is always a factor, it has not significantly influenced their substantive decision-making regarding incident notification. They emphasized that the concern for reputation exists but is balanced by a pragmatic approach to decision-making, which includes an analysis of the potential impact on reputation to prepare for the aftermath of reporting. The sentiment that by protecting their own organization, they also contribute to the broader cybersecurity community was expressed, indicating a sense of collective responsibility. Legal obligation was cited as a clear incentive, with some respondents noting the importance of adherence to legal requirements in their decision to report incidents. A few respondents suggested that authorities could provide more positive examples of reported incidents and emphasize the overall positive effects of reporting. The simplicity of the reporting process was mentioned as a potential incentive, implying that an uncomplicated reporting procedure could encourage more organizations to report incidents. Finally, the obligation of state institutions to comply with legal requirements was reiterated, underlining the regulatory framework as a key driver in the decision to report cybersecurity incidents. The concept of mutual benefit was also highlighted, with the belief that widespread reporting among organizations helps in building a stronger defence against shared threats. On the other hand, some respondents felt there was no need for additional incentives or 'candies’, as the obligation to report significant incidents is clear and always adhered to.

Table 4. Incentives that would encourage incident reporting.

The organization is already cooperating with EISA in reporting incidents
Although the answer to question 17 was "yes", in the case of essentially no notification, the concern for reputation has not influenced the substantive decision of the need to notify. Concern for reputation always exists to some extent until reporting of incidents has reached the status of a general norm of behaviour in society, but since this concern does not negate the effect and coverage associated with the incident, in recent years, decision-making has been pragmatic and limited to analysing the impact on reputation to be ready for what follows.
By protecting ourselves, we also protect others, etc.
Legal obligation.
Authorities provide more positive examples of reported incidents and the positive effects of reporting in general. Now the focus is more on the negative impacts or aspects.
The benefit is when others also report; with all those reports, we help each other to avoid threats.
There's no reason for any kind of benefits/encouragement - incidents must be reported
Uncomplicated process.
I don't see the need for so-called candies. If the nature of the incident falls under the reporting obligation, we always report it.
As a state institution, we are bound by legal requirements.

The majority, 15 out of 16, of organizations believe that reporting cyber incidents can lead to improved cybersecurity practices and resilience, as visible in Figure 15. The consensus reflects on an understanding that incident reporting contributes to a larger pool of knowledge and experience, which can be invaluable in understanding emerging threats, identifying common vulnerabilities, and developing more effective defence strategies. On the other hand, one respondent did not agree that sharing incident information can lead to improving overall cyber resilience. The reasoning provided by this participant was straightforward: "It does not help."

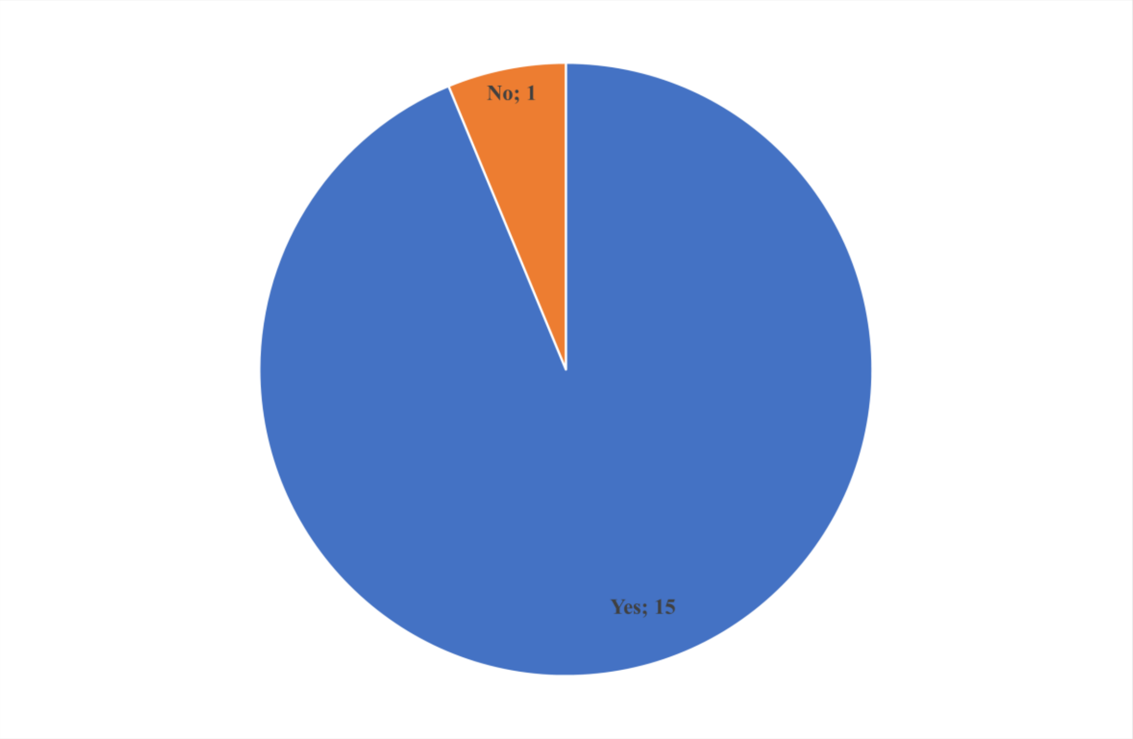

Figure 15. Relevance of reporting in order to improve overall cyber resilience.

10 respondents also elaborated on how they see incident reporting improving the overall resilience, an overview of all the responses can be seen from Table 5. A recurring theme in the responses is the importance of learning from the experiences of others. Respondents pointed out that incident reporting facilitates feedback from other organizations, which can be instrumental in understanding and implementing best practices. They can put into use for defending their own organizations. This collaborative approach allows for a more comprehensive and proactive response to emerging threats, especially with faster information about zero-day security problems. The respondents emphasized that the more incidents are reported, the more useful information becomes available for the prevention and resolution of various issues. This process enables organizations to learn from what has happened to others, rather than facing these challenges in isolation. The role of regulatory bodies was also mentioned, with respondents acknowledging that incident reporting helps these bodies gain a better overview of the cybersecurity landscape. This, in turn, enables them to offer targeted assistance and guidance in case of incidents. The process of reporting itself was seen as beneficial, requiring organizations to analyse incidents, identify patterns, and draw conclusions. This analytical approach contributes

to a deeper understanding of cybersecurity incidents and fosters a more informed and strategic response.

Table 5. How reporting cybersecurity incidents contributes to a higher cyber resilience.

1) feedback from other organizations 2) best practices 3) faster information about 0day security problems
The more information is given about various incidents, the more useful information about the prevention and resolution of various incidents becomes public, and the opportunity to learn from what happened, instead of trying everything on your own, increases.
Shared experience
Learning from other people's mistakes. But would prefer to learn from other people's successes when dealing with incidents.
It's helping others with similar situations, it's a good idea to learn from others
It helps the regulatory body to get a better overall overview and offer any kind of assistance in case of an incident.
We can receive external information and knowledge we didn't have before.
Each notification requires analysing the incident, finding patterns, and drawing conclusions.
The awareness of incidents helps other partners to realize that these cases are not isolated and as the saying goes, there are no borders or time zones in the cyber domain.
Better overall awareness

4.3 Incident Reporting Culture

8 of the respondents view the incident reporting culture in their organization as “Good”, “Positive” or “10/10”. This indicates a level of confidence and satisfaction with the systems in place, implying that these organizations likely have well-established protocols and a proactive approach to handling cybersecurity incidents. 3 respondents evaluate it as “Satisfactory” or “OK”. This may suggest that while the basic mechanisms for incident reporting are in place and operational, there is still room for improvement. The assessments from the remaining respondents depicted a less favourable view of their incident reporting cultures. Descriptions such as “Should be better”, “Is generally low - users do not understand its meaning”, “Employees just do not understand the importance of reporting and measuring,” and “Sometimes they still try to push one or the other 'under the rug', but every year the situation improves. In general, there is a feeling that most of the incidents in the organization are reported.” Such responses highlight potential

deficiencies in internal communication, training, or the overall integration of reporting protocols within the organization. Given that the respondents of the survey are in a managerial role, who are typically key figures in shaping and implementing cybersecurity cultures, policies, and practices within their organizations, the author expresses curiosity about the varying levels of satisfaction with incident reporting cultures. For the organizations where the incident reporting culture is not perceived good, the author wonders about the specific challenges or barriers that these IT managers or CISOs are facing in improving this culture. Understanding these challenges could be key to developing more effective strategies and approaches to improve the incident reporting culture in line with the expectations and standards of cybersecurity leaders.

15 out of 16 organizations reported having training programs or awareness raising campaigns in place to promote incident reporting among employees, while only 1 organization mentioned not having any training or awareness raising activities for the employees. All the provided details about the different training and awareness campaigns are listed below in Table 6. Several organizations emphasized the importance of regular and mandatory training and knowledge testing, with one specifying that such training is conducted annually. Both internal and third-party provided training were listed. There was a mention of conducting one or two awareness-raising campaigns per year, which are also integrated into the training program for new employees. The use of more interactive and engaging methods was also reported, such as gamified solutions for end-users to identify and report real and simulated malicious email-based threats.

Table 6. Cybersecurity training programs and awareness raising campaigns.

Internal training and knowledge test every year
There are various of them, and we won't go into too much detail, but on average one or two awareness-raising campaigns are carried out per year, and the corresponding elements are also included in the training program for new employees.
We launched the "Äripäev" cybersecurity e-training, the participation was low until the completion of the course was ordered
More spam reporting
For example, for end-users, a gamified solution is in place to report on real and simulated malicious e-mail-based threats.
Internal training
We tell employees that reporting is the most important thing, in how everyone can help others to stay secure.
The training program will be implemented and mandatory for all employees in the company's internal e-learning environment.
We have a mandatory information security course and test for employees.
Compulsory e-learning every year with sitting an exam.
Phishing email campaigns.
Online courses

4.4 Future improvements

12 respondents chose to answer what changes they believe are needed to facilitate incident reporting and address concerns related to underreporting, the overview of these answers is visible in Table 7. Many emphasize the importance of raising awareness, educating, and encouraging employees to report their cybersecurity related concerns. Several respondents also noted that the process of reporting should be simplified and implementing effective monitoring systems would be of great assistance. The notion of implementing effective high-tech monitoring systems is also mentioned, indicating a belief that technology can play a significant role in detecting and managing cybersecurity incidents, reducing reliance solely on human reporting. It is also argued by one respondent that the consequences of not reporting to the authorities should be reduced and should not be used as a threat mechanism, but a possible chance of collaboration to achieve improvement.

Table 7. Improvements or changes needed to facilitate incident reporting.

Encouraging and promoting employees' reporting
Furthermore, the impact of the "consequences" of mandatory notifications imposed by certain laws on the organization could be reduced, there is still some stigmatization after such notification or monitoring processes initiated by supervisory authorities very soon after the notification.
More notifications and training (also at the national level)
Regular training
More awareness on reporting incl. clear reporting channels and well-defined reporting thresholds. Also, positive examples received via or due to incident reporting.
Reporting should be made as simple as possible. More regulations to force reporting and information sharing.
Invest in High-tech monitoring, do not rely on people.
Improvements should be constant as a part of internal processes. Raising awareness of end users.
Educate employees and make the reporting process easier.
Organizations must learn to better recognize incidents and develop skills to assess potential impacts.
Awareness raising.
No changes needed

4.5 Additional comments

In the additional comments section, two observations were pointed made. One respondent mentioned that there must be a trust chain between users and IT staff and less shaming when an incident occurs. Another respondent mentioned that reporting should be a top priority focus for the security teams.". These statements also reflect on the suggestions and concerns mentioned in the previous results as well as concerns of reporting established from the literature.

4.6 Validation of the study results

A semi-structured expert interview with a representative of EISA was carried out. The goal of the interview was to validate the results of the study with the observations related to reporting of cybersecurity incidents made by EISA over the past 3 years. The results of the study were introduced to the representative of EISA, and he was asked to provide his opinion in an open discussion format. The interview commenced with five pre-planned questions, shown in Appendix 3 - Expert interview questions, that were directly related to the primary findings of the survey. The semi-structured nature of the interview allowed for the introduction of additional questions during the conversation, based on the expert's responses and the evolving dialogue. The subsequent sections detail the responses obtained during this interview, providing a qualitative validation of the survey results, and contributing to a comprehensive understanding of cybersecurity incident reporting practices in government-affiliated organizations.

The expert agreed that regulatory compliance influences organizations behaviour, if there is no obligation for reporting their incidents, then most organizations choose not to report them. Furthermore, it is up to the reporter to interpret the definition of a cyber incident and the decision to report will be made based on this. They noted that the scope of regulated entities will expand and it's possible that in the future the visibility will also expand. Similarly, there is a need for standardized understanding of cyber incidents and their impact levels across sectors and to ensure the data in reported incidents is processable. Furthermore, he disagreed with the statement that the reporting process is too complex and could discourage reporting. There is an online reporting form on the CERT-EE website, it's also possible to report via email or a phone call. The expert pointed out that proper internal incident management system should be implicated and when correctly set up, the report for notifying authorities will already exist as a by-product.

Emphasis was placed on the importance of learning from shared experiences. However, the expert has observed that while some organizations have well-established learning processes, others lack this practice. They noted that at the end of the mitigation phase all participants are understandably tired and that it is uncomfortable to learn from their own mistakes by going through them in detail. Additionally, a balance between maintaining the organization's privacy and community learning must be achieved as they are mutually exclusive. The expert also agreed that employee training is important for improving the reporting practices. He noted that EISA has a unique Cyber Reserve and for the professionals volunteering for this initiative, they are offering training on both incident response as well as specific technical topics.

The expert did not agree that reputation damage would have an impact on incident reporting in the public sector. They stated that the customers, or end users of the systems, of the organizations in this scope cannot opt out of using these services. The organizations in the public sector aim to be seen as reliable, but their unique societal role diminishes the impact negative media portrayal would have on their reputation.

5 Discussion

This chapter will provide an overview based on the research questions stated at the beginning of this study:

1. What are the key factors influencing an organization's incident reporting practices?

2. What are the primary barriers and concerns that deter organizations from reporting cybersecurity incidents?

3. What incentives can be introduced or improved to encourage organizations to report cyber incidents more proactively, ultimately leading to enhanced cybersecurity practices and resilience?

What are the key factors influencing an organization's incident reporting practices?

In the sample consisting of ministries, government agencies, state offices, state-owned companies, and hospitals owned by local governments or foundations established by the state, most respondents acknowledged the need to comply with regulations. The presence of regulatory requirements and organizational policies shapes the reporting behaviour. In cases where external reporting is mandated, there seems to be a greater inclination to comply. This suggests that in the absence of such mandates, organizations might choose not to report certain incidents, pointing to a potential area of vulnerability in cybersecurity practices. Although 2 participants indicated no requirements for the organization, they do have to comply at the minimum with the Cybersecurity Act, E-ITS, and Personal Data Protection Act. The lack of acknowledgment of these requirements by some organizations might suggest a lack of awareness, potentially influencing their reporting practices. As also stated by the expert, organizations tend to refrain from reporting cybersecurity incidents in the absence of mandatory reporting obligations.

The descriptions given by the participants on how reporting incidents helps improve cyber resilience underscores the collective and knowledge-sharing aspects of incident reporting. Organizations emphasize the value of feedback from other entities, allowing for the exchange of best practices and insights into addressing 0-day security issues promptly. The sentiment is strongly in favour of shared experiences and learning from both mistakes and successes. By making incident information public, organizations can contribute to a collective understanding of cybersecurity threats and enhance preventive measures. The notion of shared learning is reinforced, with an emphasis on avoiding redundancy in dealing with incidents. Additionally, respondents highlight the broader awareness that incident reporting generates, not only within their organization but across partners and regulatory bodies.

Furthermore, the survey responses indicate that factors beyond the incident's nature, such as organizational culture and capacity, influence reporting decisions. The emphasis on practical considerations like personal convenience and employee training highlights a gap in the readiness of organizations to identify and report cybersecurity incidents effectively. This gap can be addressed by fostering a culture of awareness and providing adequate training to employees.

What are the primary barriers and concerns that deter organizations from reporting cybersecurity incidents?

The survey results indicate that concerns about reputation damage significantly influence organizations' decisions to report cybersecurity incidents. With 62.5% of respondents expressing this worry, it's clear that the potential impact on an organization's public image is a key factor in the reporting process. This concern is particularly pronounced in the private sector, where reputation can directly affect business outcomes. Interestingly, the expert's perspective suggests that public sector organizations may be less influenced by reputational concerns due to their unique societal roles, indicating a divergence in attitudes based on the nature of the organization.

Participants in the survey offered diverse perspectives on the reasons for not reporting cybersecurity incidents. It is evident that the severity and impact of incidents play a crucial role in the decision-making process. Some respondents indicated a discernment based on the seriousness of incidents, with a commitment to reporting when the impact is significant. Others emphasized internal incidents with no substantial external repercussions as not warranting notifications. A few respondents cited a lack of incidents to report or considered minor incidents with minimal risk as non-reportable. This reliance on severity as a criterion, however, leads to a notable ambiguity in the reporting process, as less impactful incidents often go unreported. This finding underscores the need for more defined guidelines and criteria to aid organizations in determining when to report an incident.

For some, the decision hinged on the mandatory nature of reporting, aligning with legal and procedural obligations. The survey also highlighted the need for clarity and structured guidelines for employees to effectively recognize and assess incidents. It was noted that personal convenience might sometimes influence the decision to report an incident. These responses suggest that reporting decisions are shaped by a blend of factors such as incident severity, legal mandates, and internal organizational policies. While the author appreciates the insights provided by the participants, the absence of a response from the one organization that chose not to report an incident is particularly noticeable. This absence prevents a complete understanding of the factors influencing reporting decisions, especially in cases where incidents are not disclosed. The absence of this perspective suggests there may be other, unexplored reasons behind the decision not to report, which could provide valuable insights into organizational behaviour and risk management in the context of cybersecurity.

What incentives can be introduced or improved to encourage organizations to report cyber incidents more proactively, ultimately leading to enhanced cybersecurity practices and resilience?

The responses to the question regarding benefits or incentives to encourage proactive reporting of cyber incidents reveal a mix of perspectives among the organizations surveyed. Some organizations already have a cooperative relationship with EISA in reporting incidents, emphasizing the importance of existing collaborations. Concerns about reputation, while acknowledged, are seen as secondary to the need for substantive reporting. Legal obligations are highlighted as a key motivator, underlining the importance of regulatory compliance. Some respondents emphasize the collective benefit of reporting, indicating a sense of shared responsibility in protecting the broader community from threats. A few organizations express a straightforward approach, stating that incidents must be reported as an obligation, with no need for additional incentives. This suggests a commitment to compliance irrespective of external rewards. Overall, the responses reflect a combination of legal obligations, collaborative considerations, and a recognition of the collective impact of incident reporting.

Many respondents emphasize the importance of encouraging and promoting employees to report incidents. They suggest reducing the potential negative consequences of mandatory notifications to minimize stigmatization. Additionally, there is a call for more comprehensive training programs at both the organizational and national levels, with an emphasis on regular training sessions. Creating awareness about reporting, establishing clear reporting channels, and setting well-defined reporting thresholds are seen as essential. Some respondents suggest the need for more regulations to enforce reporting and information sharing. Simplicity in the reporting process is advocated, with suggestions to invest in high-tech monitoring to complement human efforts. The expert's perspective differed on the complexity of the reporting process, highlighting available reporting channels and the importance of an internal incident management system. Continuous improvement, employee education, and the need for organizations to better recognize and assess incidents are also highlighted. Overall, the consensus is on a multifaceted approach involving education, technology, and regulatory support to enhance incident reporting.

5.1 Limitations

The limitations of this study warrant careful consideration when interpreting its findings. Primarily, the study is constrained by its focus on organizations that are subject to specific information security requirements and regulations applicable to Estonian public sector and government-affiliated organizations. This focus inherently excludes a significant portion of entities, particularly those that are not bound by such stringent regulations. This limitation poses a challenge in generalizing the study's findings to a wider array of organizational contexts, especially those operating under different legal and regulatory frameworks.

In addition, the sample size of 16 Estonian organizations cannot be used for generalization for the entire public sector and government-affiliate organizations in order to draw comprehensive conclusions regarding cyber incident reporting practices. Organizations that chose to participate in the study might inherently differ in certain aspects, such as their approach to cybersecurity and incident reporting, from those that did not participate. This selection bias could skew the findings and limit their applicability to the broader population of organizations.

Last of all, the lack of detailed responses to the open-ended question regarding primary reasons for not reporting incidents leaves a gap in understanding the full spectrum of challenges organizations face in this domain. Only a limited number of the respondents provided insights, indicating either a reluctance to disclose such information or a lack of clear understanding of the barriers themselves. This limitation in data points to the need for further research to fully grasp the complexities and nuances of cybersecurity incident reporting in organizational settings.

5.2 Future work

Based on the narrow scope of this study, future research can consider incorporating a broader range of organizations, both within and outside the public sector, to gain a more comprehensive understanding of incident reporting practices across various sectors as well of the barriers in reporting the incidents.

Possible future studies can conduct a comparative analysis between different countries or regions within the EU. This comparative approach can uncover variations in reporting practices due to differing regulatory frameworks, cultural influences, or organizational structures.

While this study used an online survey for data collection, future research could incorporate only qualitative subject matter expert interviews for data gathering. This could provide a more valuable insights into the underlying motivations, barriers, and experiences related to incident reporting.

The results of this study can be shared to EISA to serve as possible course of action when planning the activities to improve reporting of cybersecurity incidents.

6 Conclusion

The significant increase in reported cyber incidents to CERT-EE, coupled with the changing nature of incident types, highlights a pressing need for enhanced cybersecurity measures and underscores the importance of researching incident reporting practices among Estonian government and government-affiliated organizations to strengthen overall cybersecurity resilience. Qualitative research was conducted to identify the barriers that hinder transparent reporting and the incentives that could encourage more proactive disclosure. The sample of this study consisted of 16 public-sector and government-affiliated entities. For validation of the obtained results, an expert interview was conducted with a representative from EISA. Key findings from this study can be summarized as four main points. Firstly, a strong emphasis on regulatory compliance among organizations. Additionally, incident reporting is valued for its collective and knowledge-sharing aspects, fostering the exchange of best practices, and contributing to a broader understanding of cybersecurity threats. Furthermore, a significant concern is potential reputation damage, with 62.5% of respondents expressing apprehensions about its impact on organizational decision-making. Incentives for proactive reporting encompass existing collaborations, legal obligations, recognition of the collective benefit, and a focus on encouraging and training employees. In conclusion, while the survey sheds light on the complexities and varied factors influencing the reporting of cybersecurity incidents, it also highlights the need for further research. A more comprehensive understanding of these factors, including those that lead organizations to refrain from reporting, is crucial for developing effective strategies and guidelines to enhance cybersecurity incident reporting practices.

References

[1] Estonian Information System Authority, "Cyber Security in Estonia 2023," 2023.

[2] Estonian Information System Authority, "Annual Cyber Security Assessment 2018," 2018.

[3] Estonian Parliament, "Cybersecurity Act," 2022.

[4] Minister of Entrepreneurship and Information Technology of the Republic of Estonia, "Estonian information security standard," 2022.

[5] European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *OJ L,* vol. 194, p. 1–30, 2016.

[6] International Organization for Standardization, "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 2022.

[7] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," *OJ L,* vol. 119, p. 1–88, 2016.

[8] P. Wang and C. Johnson, "Cybersecurity incident handling: A case study of the Equifax data breach," *Issues in Information Systems,* vol. 19, no. 3, pp. 150-159, 2018.

[9] U.S. Attorney's Office, Northern District of California, "Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records," 5 October 2022. [Online]. Available: https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach.

[10] K. Paljug and R. Mikac, "Contemporary crises: Case study of uber," *Contemporary Macedonian Defense,* vol. 20, no. 39, pp. 93-106, 2020.

[11] J. Rasalam and R. J. Elson, "Cybersecurity And Management's Ethical Responsibilities: The Case Of Equifax And Uber," *Global Journal of Business Pedagogy,* vol. 3, no. 3, pp. 8-15, 2019.

[12] P. Briggs, D. Jeske and L. Coventry, "The Design of Messages to Improve Cybersecurity Incident Reporting," in *International Conference on Human Aspects of Information Security, Privacy, and Trust,* vol. 10292, Vancouver, Canada, Springer, 2017, pp. 3-13.

[13] E. Koivunen, "Why Wasn't I Notified Information Security Incident Reporting Demystified," in *Nordic Conference on Secure IT Systems,* Espoo, Finland, Springer, 2010, pp. 55-70.

[14] S. Laube and R. Böhme, "The economics of mandatory security breach reporting to authorities," *Journal of Cybersecurity,* vol. 2, no. 1, pp. 29-41, 2016.

[15] I. A. Tøndel, M. B. Line and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security,* vol. 45, pp. 42-57, 2014.

[16] International Organization for Standardization, "ISO/IEC 27035:2011 Information technology — Information security incident management," 2011.

[17] F. Dezeure, G. Webster, J. Trost, E. Leverett, J. P. Gonçalves, P. Mana, G. McCord and J. Magri, "Reporting Cyber Risk to Boards," Eurocontrol, 2022.

[18] S. Kemp, D. Buil-Gil, F. Miró-Llinares and N. Lord, "When do businesses report cybercrime? Findings from a UK study," *Criminology & Criminal Justice,* vol. 23, no. 3, pp. 468-489, 2023.

[19] K. R. Agbodoh-Falschau and B. H. Ravaonorohanta, "Investigating the influence of governance determinants on reporting cybersecurity incidents to police: Evidence from Canadian organizations' perspectives," *Technology in Society,* vol. 74, 2023.

[20] J. Easterly and E. Goldstein, "Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products," Foreign Affairs, 1 Febuary 2023. [Online]. Available: https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Marita Müüdla

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Reporting of cybersecurity incidents among Estonian government and government-affiliated organizations”, supervised by Sille Arikas
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

04.01.2024

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Questionnaire

Section 1: General Information

1. Field of Operation

2. Number of Employees

3. Your Position/Role within the Organization

4. How long have you been with the organization?

Section 2: Incident Reporting Practices

5. Does your organization have to be compliant with a certain set of information security requirements or regulations?

    a. If yes, please list them.

6. Have you established incident reporting protocols or guidelines in your organization?

    a. If yes, please describe them. Whom are they aimed at?

7. Have you experienced any cybersecurity incidents in the past year?

    a. If yes, please briefly describe the types of incidents (e.g., data breaches, malware infections, how did you detect the incidents).

    b. If not, do you have logging and monitoring set up?

8. Who within your organization is responsible for reporting a cybersecurity incident to management?

    a. IT/security team

    b. Legal Department

    c. Other

9. Who within your organization is responsible for reporting a cybersecurity incident to regulatory authorities?

    a. IT/security team

    b. Legal Department

    c. Senior Management (member)

    d. Other

10. Who within your organization authorizes reporting a cybersecurity incident to regulatory authorities?

    a. IT/security team

    b. Legal Department

    c. Senior Management (member)

    d. Other

11. Did your organization report these incidents to any external entities or authorities?

    a. If yes, please specify the entities or authorities.

    b. If no, please provide reasons for not reporting.

Section 3: Barriers to Reporting

12. What are the primary reasons for not reporting cybersecurity incidents?

13. Are there concerns about reputation damage associated with reporting incidents?

    a. If yes, how significant are these concerns on a scale of 1 (not significant) to 5 (very significant)?

    b. If no, please elaborate.

14. What benefits or incentives would encourage your organization to report cyber incidents more proactively?

15. Do you believe that reporting cyber incidents can lead to improved cybersecurity practices and resilience?
    a. If yes, please explain how.
    b. If no, please explain why not.

Section 4: Incident Reporting Culture

16. How would you describe the overall incident-reporting culture within your organization?
17. Are there training programs or awareness campaigns in place to promote incident reporting among employees?
    a. If yes, please provide details.

Section 5: Future Improvements

18. What improvements or changes do you think are needed to facilitate incident reporting and address concerns related to underreporting?

Section 6: Additional Comments

19. Please use this space for any additional comments or insights regarding incident reporting in your organization.

Appendix 3 - Expert interview questions

1. In your experience, have you observed similar themes as highlighted in this study, particularly regarding the challenges and practices in cybersecurity incident reporting among government organizations?

2. Does your experience align with this study's finding that regulatory compliance significantly influences the incident reporting behaviour of government organizations?

3. The study indicates that concerns about reputation damage significantly impact incident reporting decisions. Have you witnessed similar concerns in your role?

4. The study suggests that the complexity of reporting processes can be a barrier. Do you agree with this, and what improvements do you recommend?

5. The findings indicate a need for better organizational recognition of incidents for effective reporting. How does this compare with your observations in the field?