Sara Boddy

CASE STUDY: THE DECISION-SUPPORT FRAMEWORK AND NIS2, CER, AND DORA INCIDENT REPORTING OBLIGATIONS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Boddy, Sara
Tapaustutkimus: Päätöksentekoa tukeva viitekehys ja NIS2, CER ja DORA poikkeamien raportointien vaatimukset
Jyväskylä: Jyväskylän yliopisto, 2024, 69 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Paananen, Hanna

Euroopan unioni on sitoutunut parantamaan kyberturvallisuutta jäsenvaltioissaan säätämällä lakeja, jotka vaikuttavat organisaatioiden kyberturvallisuuden valmiuksiin. Näitä lakeja ovat muun muassa Network and Information Security 2 direktiivi (NIS2), Critical Entities Resilience direktiivi (CER) ja Digital Operational Resilience asetus (DORA). Nämä lainsäädännöt vaativat, että organisaatiot raportoivat kyberturvallisuuspoikkeamista viranomaisille. Tällä hetkellä on vain vähän ohjeistuksia, jotka auttaisivat organisaatioita tunnistamaan, miten poikkeamat tulisi raportoida viranomaisille. Uusien lainsäädäntöjen myötä on entistä tärkeämpää, että organisaatioissa ymmärretään, miten kyberturvallisuuspoikkeamat tulee raportoida viranomaisille. Tämän tutkimuksen tavoitteena on selvittää, ovatko organisaatioiden nykyiset raportointiin liittyvät käytännöt linjassa päätöksentekoa tukeva viitekehyksen kanssa, ja edellyttääkö uusi lainsäädäntö muutoksia kyseiseen kehykseen. Tämä pro gradu -tutkielma toteutettiin tapaustutkimuksena, joka alkoi kattavalla kirjallisuuskatsauksella, jossa tarkasteltiin olemassa olevaa tutkimusta poikkeamien raportoinnista ja lainsäädännöistä. Aineisto kerättiin kyberturvallisuuden ammattilaisilta puolistrukturoiduilla haastatteluilla. Haastateltavat ovat havainnoineet kyberturvallisuusharjoituksia, joissa simuloidaan tosielämän kyberturvallisuuspoikkeamia. Aineisto analysointi suoritettiin deduktiivisena koodauksena. Tulokset osoittavat, että päätöksentekoa tukeva viitekehys vastaa osittain todellista toimintaa, mutta yksityiskohdat vaihtelevat poikkeamakohtaisesti ja organisaation prosessien mukaan. Keskeiset löydökset korostavat, että selkeät roolit ja vastuut, vakiintuneet kommunikaatioreitit, monipuolinen tiimi ja poikkeamaan liittyvän ydinryhmän asiantuntevat henkilöt ovat olennaisia. Tiimin henkilöiden on ymmärrettävä lainsäädännölliset velvoitteet ja heillä on oltava kokemusta poikkeamien hallinnasta, jotta organisaatio pystyy toimimaan uuden lainsäädännön vaatimusten mukaisesti.

Asiasanat: Poikkeamien ilmoittaminen viranomaisille, Poikkeamien ilmoittaminen, NIS2, CER, DORA, Tapaustutkimus

ABSTRACT

Boddy, Sara
Case study: The decision-support framework and NIS2, CER, and DORA incident reporting obligations
Jyväskylä: University of Jyväskylä, 2024, 69 p.
Cyber Security, Master's Thesis
Supervisor(s): Paananen, Hanna

The European Union is committed to enhancing cybersecurity across its Member States by introducing legislation that impacts organizations cybersecurity preparedness. These laws include the Network and Information Security 2 Directive (NIS2), the Critical Entities Resilience Directive (CER), and the Digital Operational Resilience Act (DORA). These legislations mandate that organizations report cyber incidents to authorities. Currently, there are few guidelines available to help organizations understand how to report incidents to authorities. With the new legislations, it becomes even more crucial for organizations to comprehend how to report cyber incidents effectively to authorities. This research aims to determine do organizations current practices align with the decision-support framework and does the new legislations warrant adaptions to the framework in question. This thesis was conducted as a case study, beginning with a comprehensive literature review on existing research on incident reporting and the legislations. Data was gathered through semi-structured interviews with cybersecurity professionals who have observed cybersecurity exercises simulating real-life cyber incidents. The data was analyzed using deductive coding. The results indicate that the decision-support framework partially corresponds to real-life operations; however, the specifics vary depending on the particular incident and the organization's processes. The key findings highlight that clear roles and responsibilities, established communication paths, a diverse team, and knowledgeable individuals in the core group related to the incident are essential. These team members must understand the legislative obligations and have experience in incident management, making sure that the organization can effectively handle the complexities of reporting under the new legislations.

Keywords: Incident reporting to authorities, Incident disclosure, NIS2, CER, DORA, Case study

FIGURES

TABLES

CONTENTS

1 Introduction

Criminal activity online has been increasing exponentially, with cyberattacks causing significant damage across various sectors (Cascavilla et al., 2021). High profile cases such as NotPetya encrypted files of multiple large companies such as Maersk; the Colonial pipeline ransomware attack disrupted oil delivery for six days; and cyberattacks on Ukraine's power grid lead to widespread power outages. (Anderson, 2020; DarkReading, n.d.; Tsvetanov & Slaria, 2021.) However, it's important to note that not all cyber threats come from malicious attacks. Many interruptions can result from non-malicious activities such as technical failures, system malfunctions, and human errors (Joint Task Force Transformation Initiative, 2012).

To combat disruptions in the cybersphere, organizations have employed various cybersecurity measures and follow industry best practices. These practices include conducting regular risk assessments, regularly updating and patching systems, and conducting employee training to recognize and respond to cyber threats. It is particularly vital for critical infrastructure not only to maintain security but also to recover from incidents swiftly. Despite these efforts, there remains a gap in investment and focus on cybersecurity between regions. According to the European Parliament, EU businesses invest less in cybersecurity compared to US businesses (European Parliament, 2021b.) This leads to the EU creating new legislation to encourage organizations to enhance their cybersecurity measures and fight cybercrime and privacy infringements which improves organizations resilience. (Andreasson & Fallen, 2018.)

Among these initiatives are the Network and Information Security Directive 2 (NIS2), the Critical Entities Resilience Directive (CER) and the Digital Operational Resilience Act (DORA). These legislations were put in force in 2023. NIS2 and CER takes effect in October 2024 and DORA in January 2025. They focus on strengthening cybersecurity all across the EU by obligating organizations to adopt various cybersecurity measures (European Parliament, 2021b). One of these measures is to report major or significant incidents to authorities. Although incident notifying is just one part of these legislations, it is essential. By mandating incident reporting, the EU and Member States can, for example, exchange threat intelligence, enhance cross-border cooperation, thus fostering a more

secure cyberspace for all citizens. Furthermore, these legislations include sanctions to ensure compliance, highlighting the importance of these cybersecurity measures.

Some of the existing literature and research have primarily concentrated on data breach notifications under the General Data Protection Regulation (GDPR) (Grey & Brown, 2020; Kapoor et al., 2018b). Furthermore, there are few guidelines available for organizations on reporting cyber incidents to authorities (Cichonski et al., 2012; European Banking Authority, 2021; Institute for Security and Technology & Cyber Threat Alliance, 2023; Maniati & Tringali, 2019). This may be due to the previous narrow scope of organizations required to notify authorities and the fact that previous legislations have not been very stringent — that is, the obligations have not been very detailed.

As more sectors are mandated to report cyber incident notifications and the requirements for these notifications become more stringent, organizations must incorporate these requirements into their cyber incident management processes. The research on notifying incidents to authorities is lacking verification on whether the frameworks or guidelines work. Thus, the research questions for this study are:

- Do organizations practices align with the decision-support framework in reporting cyber incidents to authorities?
- How do these practices fail or succeed?
- Do the legislations, NIS2, CER, and DORA, warrant adaptations to the decision-support framework in reporting incidents to authorities?

This thesis is a case study where it seeks to find out whether organizations practices align with Kulikova et al. (2012) decision-support frameworks in the context of reporting cyber incidents to authorities and how they fail or succeed. Additionally, it will explore how new legislations such as NIS2, CER, and DORA might influence the decision-support framework.

Cyber incidents are sudden and unexpected events that often remain undisclosed to the public until organizations decide it is necessary to inform about them, due to their highly confidential nature and the potential for significant financial and reputational damage. An efficient way to train organizations key members about cyber incidents and get them to review their current processes is through cybersecurity exercises. These exercises are training events where participants confront a cyber incident, allowing them to review, evaluate, and validate their processes and documentation for managing such incidents (Aaltola & Taitto, 2019; Karjalainen & Kokkonen, 2020). Therefore, the data for this thesis was collected from individuals who have observed various cybersecurity exercises to gain valuable insights into organizations' current practices and processes regarding incident reporting to authorities. The interviews were conducted as semi-structured interviews.

The results of this thesis will provide important insights within the cybersecurity research field, particularly regarding cyber incident notifications and the requirements of new legislation. The focus is specifically on incident notifications

and does not determine whether an organization falls under the scope of these legislations.

The thesis is structured into six main chapters. The second chapter introduces the research and existing literature on incident reporting and the decision-support framework, focuses on NIS2, CER, and DORA legislations, first providing a general overview of these legislations and then detailing the specific requirements for reporting incidents to authorities and describing cybersecurity exercises. The third chapter explains the methodology used in this thesis. The fourth chapter presents the results from the interviews and includes the analysis. The fifth chapter contains the discussion as well as the limitations of the research. Finally, the sixth chapter concludes the thesis.

2 Literature review

This thesis involved a comprehensive review of relevant literature, guidelines, frameworks, reports, legislation, and research. Key frameworks and guidelines were sourced from respected organizations and institutions such as the European Network and Information Security Agency (ENISA), the National Institute of Standards and Technology (NIST), and various National Cybersecurity Centers. Legislations were examined through the European Union's official websites and recent studies focusing on these laws. Given the recent enactment of these legislations, the literature review focusing on legislations primarily used studies from 2023-2024. These studies were identified by searching for the legislation's names, using either their acronyms or full names. The research materials, including conference papers, were sourced from databases such as Google Scholar, Science Direct, and ProQuest. The author used search terms such as 'incident reporting to authorities', 'incident disclosures to authorities', 'incident notifying to authorities', or 'external incident notifying', either individually or a combination of various forms. To ensure a thorough review the literature review included studies spanning several years.

The literature review is structured into four primary sections. The first section explores the importance of reporting incidents to authorities, discussing the motivations behind relevant legislations and reviewing the existing literature on this topic. The second section introduces the decision-support framework from Kulikova et al (2012). The third section focuses on the new legislations that impact how incidents should be reported to authorities. The fourth and final section examines cybersecurity exercises, familiarizing the reader with the concept.

2.1 Reporting incidents to authorities

As the cybercrime industry is continuing to grow. Cybersecurity Ventures estimates the damages of cybercrime to cost 9.5 trillion dollars in 2024. (Freeze, 2023) Cybercriminals employ various methods to harm organizations, such as ransomware, distributed denial of service (DDoS), SQL injections and phishing.

Cybercrime and accidental or mismanagement of systems can affect systems' confidentiality, integrity, and availability (CIA). This means that the organization's primary goals in cybersecurity is to preserve the CIA of their whole ICT infrastructure. Several frameworks can help organizations maintain their ICT systems' security, such as the National Institute of Standards Frameworks (NIST), COBIT, and ISO27001 standards. (Karyda & Mitrou, 2016.) Unfortunately, even relying on standards or employing the best technical measures to secure the organization is not always enough to stop cyber-attacks. There are several different ways to bypass different security measures, such as social engineering or exploiting vulnerabilities that have not been detected by the system owner.

Suspicious IT events must be investigated and identified. After the incident has been verified, a series of information exchanges follow. (Karyda et al., 2016.)

These events might be malicious and are thus handled as cyber incidents. The impact of a cybersecurity incident can be very damaging to an organization. They can lead to financial losses, legal actions, privacy violations, and damage to reputation. (Falowo et al., 2022.) On a larger scale, regarding society, incidents can considerably impact the provision of essential services and the security of supply (Valtioneuvosto, 2022).

A cybersecurity incident is an event identified as impacting an organization and leading to the need for response and recovery. In addition, it is determined as an occurrence that may or has endangered the confidentiality, integrity, or availability (CIA) of systems or one system. (National Institute of Standards and Technology, 2018; National Institute of Standards and Technology, 2020.) ENISA defines it in more detail. According to ENISA (2017), anything that may impact either the functioning components or basic components of cyberspace, regardless of whether it is a natural occurrence or man-made, or of malicious or non-malicious intent, accidental, or occurred due to incompetence, is a cyber incident. (Tirtea, 2017.) The Finnish National Cyber Security Centre (2019) defines a cybersecurity incident more broadly than the other institutions. It is defined as anomalies in the organization's IT environment affecting its operations. (Traficom, 2019.) In literature, Luttgens et al. (2014) define a computer security incident as something that has the intent to cause harm, has been performed by a person, and 'involves a computing resource'. In their opinion, a computer security incident is not caused by natural disasters or system failures with no culprit behind it. (Luttgens et al., 2014, p. 24.) Koivunen (2012) p. 55 defines a network and security incident to be types of 'situations where effects harmful to security have manifested or have had the potential to manifest in the networks or networked information systems'.

Incident management is a comprehensive process aimed at restoring the normal operations of an entity and minimizing the impact of incidents as swiftly as possible (Brewster et al., 2012; Cusick & Ma, 2010). This process covers all stages of an incident lifecycle, including planning, training, awareness raising, detection, response, and learning from the incidents (Hove, et al., 2014). According to Siregar & Chang (2019), incident management involves six essential practices: analyzing incident-related information to specify the incident, communicating with relevant entities, collecting and safeguarding related information, implementing short-term containment solutions, eliminating the incident's access, and restoring IT systems to normal operations.

Incident response primarily aims to reduce the impact on digital assets and restore IT systems to their normal functionality (Ahmad et al., 2020, 2021). Mitropoulos et al. (2006) define incident response as a process aimed at reducing the damage from security incidents and enhancing the learning from these events (Mitropoulos et al., 2006). The phases of incident response include preparation, identification, containment, eradication, recovery, and follow-up, which are essential for effective management (Ahmad et al., 2020, 2021; Cichonski et al., 2012). A key aspect of incident response is learning from previous incidents to prevent future occurrences (John R. Vacca, 2013). Alternatively, they can be more prepared in case it happens again. The Incident response plan should include the key elements: responsibilities, roles, and authorities (Anson, 2020).

Interestingly, some sources, such as the Cyber Security Coalition (2016), argue that incident management encompasses the same phases as incident response, suggesting that incident management should include an incident response plan detailing the organization's primary goals for protection—covering systems, networks, products, and outlining responsibilities and the engagement of possible external experts. The National Cyber Security Centre of the UK (2019) notes that Incident Management and Incident Response are often used interchangeably. Incident Management is described as having a broader scope, managing all stages of the process, and handling all aspects of the incident, including communications, reporting, and media interactions. Conversely, Incident Response is identified as a more technical component within the broader Incident Management framework, following the same phases as defined by NCSC-UK (2019) and Ahmad (2020).

In this thesis, the terms Incident Response and Incident Management describe the overarching process of managing incidents, separate from the technical operations level of incident management or response. This distinction highlights the strategic, as opposed to the technical, approach to managing incidents within an organization.

A part of the incident response plan is sharing information with outside parties. One of these parties can be the authorities, such as the National CERT, i.e., the Computer Emergency Response Team. Reporting incidents to authorities is crucial in improving the overall cybersecurity of Member States and organizations within the EU. By reporting cybersecurity incidents, the authorities can help investigate a cyber incident, raise awareness of the attacks to other organizations and entities, and learn about malicious actors by investigating the attack (Seng, 2023). Policymakers can benefit from identifying the current threat landscape, what it can do to defend itself from those threats, identifying possible damages of threats, and regarding the threat landscape in policy making. (Wolff, 2014.) It can also help in preventing other attacks. (Clausmeier, 2023). Lehto et al. (2017) agree that incidents should be managed and analyzed, and preparedness would improve. The paper emphasizes that reporting incidents should be incorporated into legislation. Situational awareness sheds light on the current environment, events, and impacts on operations (Pöyhönen et al., 2019). Evesti et al. (2017) discuss in their paper that Cybersecurity situational awareness refers to the knowledge of activities within a networked system, the current estimated security level, and identifying causal connections that realize observed risks. They also highlight that cybersecurity situational awareness is understood differently within the cybersecurity industry, i.e., 'from high-level risk analysis to security administration level log analyses'. (Evesti et al., 2017.) Information exchange is considered a part of cyber situational awareness in Franke & Brynielsson's study (2014).

Wolff (2014) highlights the importance of gathering data on security incidents and breaches to apply security measures to mitigate the current risks in the cyber landscape. She mentions that many organizations use best practices, such as NIST's frameworks, to apply relevant security measures, but they are often extensive and might not fit a smaller organization. Thus, for example, smaller organizations might benefit from learning about the current risks in the

cybersecurity landscape from concrete data. The current data on security threats could help tailor specific security controls for organizations. Other benefits would be for technology and internet companies to develop their products and identify third-party companies that have failed their due diligence in cybersecurity. (Wolff, 2014.)

In the US, organizations from the Cybersecurity sector came together to develop an incident reporting framework in 2023 for the Cybersecurity and Infrastructure Security Agency (CISA), which is responsible, e.g., cybersecurity protection in the US. It can also be used by national cybersecurity authorities that want to implement mandates and procedures for reporting cybersecurity incidents. According to the report, reporting incidents to national cybersecurity authorities has four purposes. The first is noticing trends in cyberattacks. This creates a better understanding of the adversary's actions, e.g., sector targeting or victims. The second benefit is that the authorities, either the government or the national cybersecurity authority, can warn other organizations about current threats. (Institute for Security and Technology & Cyber Threat Alliance, 2023) This was demonstrated in Finland by the Finnish Cyber Security Centre warning the public in October 2023 about a sophisticated phishing campaign (Traficom, 2023). The third purpose is responding to attacks. Reporting incidents could improve the asset and threat response activities. The last purpose is to learn from the attacks, e.g., harm and impact. (Institute for Security and Technology & Cyber Threat Alliance, 2023.)

Recent studies and reports indicate that there is a gap in the reporting of cyber incidents to the relevant authorities, highlighting a crucial area for improvement. Based on Keeper Security's report, 48% of respondents did not report cyber incidents to the relevant authorities. The research was conducted in North American and European companies. (Benfield, 2023.) A study conducted in 2019 of German blue-chip companies suggests that many cybersecurity incidents were not reported to authorities in 2005-2018 (Georg-Schaffner & Prinz, 2022). ENISA's service Ciras shows that in 2023, 754 incidents were reported by critical service providers (ENISA, 2023). So, there is still room for improvement in reporting incidents to authorities.

It is essential to remember that reporting incidents depends on jurisdiction and sectors, as well as defining what type of incidents should be reported. Another important point is that the time frame in which an incident should be reported may differ depending on jurisdictions. (Clausmeier, 2023.) Since 2018, organizations have had an obligation to report personal data breaches to authorities and the people affected by the GDPR act. They have 72 hours to report the incident to relevant authorities and must inform the people affected within a reasonable timeframe, avoiding unnecessary postponement. A personal data breach means the natural persons' data might have been accidentally or unlawfully destructed, lost, altered, unauthorizedly disclosed, accessed, transmitted, stored, or 'otherwise processed' (Schmitz-Berndt & Anheier, 2021). This thesis will not further study the GDPR act or the notification because it focuses on new legislations. However, it should be mentioned that the European Parliament wants to align reporting obligations in the upcoming legislations with GDPR (Schmitz-Berndt et al., 2021). This is why they focus on significant incidents, i.e., causes or has the

possibility of causing harm. It is also good to understand that cybersecurity and data protection laws can apply to the same incident. The laws are applicable in cases of personal data breaches and incidents that fall under reporting obligations within cybersecurity law. (Andreasson et al., 2018.)

To combat cybercrime and privacy infringements and possibly gather better intelligence about the threat landscape, the European Union is trying to fight cybercrime and privacy infringements by introducing legislation. It in itself improves organizational resilience. (Andreasson et al., 2018.) With new legislations, the EU wants to make reporting easier for organizations by creating a single point of contact. It means the incidents are reported to one authority instead of several notifications to different authorities. Streamlining incident reporting by aligning timeframes and incident types improves organization resource allocation and response actions. (Schmitz-Berndt, 2023b.)

Within organizations, reporting cyber incidents to authorities has been a small part of Incident Management. In many cases, cyber incident reporting to authorities has been mentioned briefly in guidelines and frameworks (Cichonski et al., 2012; European Banking Authority, 2021; Institute for Security and Technology & Cyber Threat Alliance, 2023). The gap in guidelines and frameworks is likely because there has not been much legislation governing precisely how, to whom, and when to report incidents, i.e., the obligations were looser. Nevertheless, this does not mean there has not been a discussion about incident reporting. Luiifj et al. (2021) mention in their analysis of critical infrastructure incidents that the incident reports should include the same metrics so that comparisons and impact assessments can be made. They highlight a discussion around this within the financial sector. EBF, the European Banking Federation, proposed a harmonized incident reporting guide in 2019. Within this report, they emphasize that Member States should harmonize the thresholds for reporting and create a common taxonomy for cybersecurity incident reporting. The motivation behind these requirements is that in case of a cyber event, organizations might have to report to different supervisory authorities to comply with, e.g., different timelines, communication means and datasets. See Figure 1. They emphasize that the reporting becomes even more fragmented when the organization operates in different countries with different jurisdictions. With a transparent incident reporting model, organizations would clearly understand what to report, to whom, and when. In addition, the reporting model would enable aligning procedures within organizations that operate in different countries. (Maniati & Tringali, 2019.)

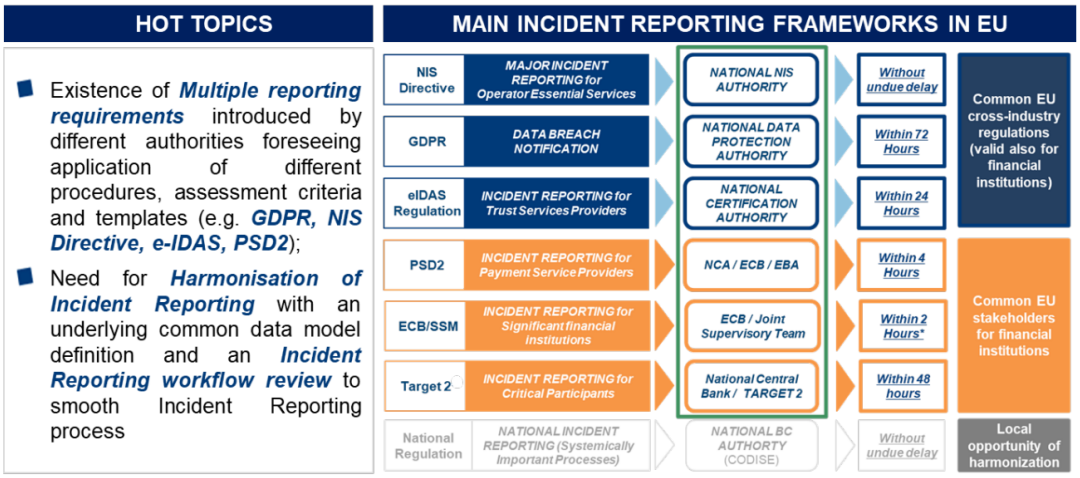

FIGURE 1 Comparison among Incident Reporting schemes (European Banking Federation, 2019)

In conclusion, the growing rate of cybercrime and evolving threat landscape forces organizations to be prepared for cyber incidents. Current security frameworks alone cannot stop cyberattacks. Thus, the EU is enhancing the overall cybersecurity within Member States by enacting legislation that obliges organizations to implement cybersecurity measures. Among these measures is reporting incidents to authorities, which aims to create a better understanding of the threat landscape for the EU and support organizations during crises. Furthermore, the EU aims to streamline the reporting process for organizations by establishing a single point of contact for incident reporting and simplifying the notification procedures. The reporting obligation among other changes in the legislations are intended to enhance cybersecurity and ensure a safer digital environment for all of EU's citizens.

2.2 Research of notifying authorities of incidents and incident management

More research needs to be done specifically on reporting cyber incidents to authorities. There has been some research regarding GDPR and its changes to incident management, reporting data breaches to authorities or individuals whose data has been breached, and general incident management. Notifying authorities is often seen as a part of communication in incident management.

NIST's Incident Handling Guide emphasizes organizations' need to establish clear policies for reporting incidents to authorities, suggesting a proactive approach to incident management (Cichonski et al., 2012). This stance is further complicated by the GDPR, as Grey et al. (2020) study about GDPR and reporting in IT consulting firms regarding data breaches to authorities argues that the regulation mandates a revision of incident response phases traditionally outlined by frameworks such as NIST, ISO 27000/27001, and ENISA. Part of the Incident

Response process should include reporting the incident to authorities. The authors suggested more research to develop an incident notification framework.

The most prominent aspect in literature and studies is incident management policy or process. (Bartnes Line et al., 2016; Khurana et al., 2009; Line et al., 2014; Luttgens et al., 2014). Organizations should be prepared for incidents by having a reporting process to ensure the process creation does not happen in the middle of an actual incident. An essential aspect is to know who should be informed of the incident and see the person responsible for external communication. (Luttgens et al., 2014.) Line et al. (2014) found in their study concerning organizations operating industrial control systems that there is a lack of documented policies within incident response, especially when IT system maintenance is outsourced. Khurana et al. (2009) suggest a model that includes the roles and responsibilities of the people and organizations involved and a process that includes the phases of the incident response and investigation as well as the responsibilities since they found managing all tasks related to the incident challenging for organizations. The tasks could be evidence gathering, restoring services, sharing data and logs, or information sharing. These tasks are primarily organized into phases, such as preparation and analysis. However, large-scale attacks might be difficult since several phases occur simultaneously. Using a checklist also emerged in some studies. Kapoor et al. (2018b) recommend using checklists to guide a complex process and instructions that are easy to follow during a crisis. The incident response plans that should also be created as checklists are disaster recovery plans, crisis communication plans, and business continuity plans.

The existing literature did not adequately address the information that should be provided to authorities. Some studies, like Lif et al. (2020), compared different cyber incident reports in their paper. The Incident Report is used to document the incident and share information. The templates were from Safe Cyber (military-civilian Cybersecurity Defense exercise), iPilot (cybersecurity exercise), Locked Shields (NATO cybersecurity exercise), MSB (Swedish Civil Contingencies Agency), and United Kingdom's National Cyber Security Centre and some frameworks developed by researchers. They identified five categories used to document the incident and share information: Basic information, incident description, consequences of damages, effect on operations and communications, and the actions taken or planned. However, the information did differ in these templates because the templates were designed for different sectors and purposes, i.e., military or research.

This variability can lead to complications in communication between stakeholders, such as the incident management team, the rest of the organization, and external stakeholders. One issue was sharing correct information for the appropriate people. (Hove, et al., 2014). Information-sharing was also present within the team itself. Aoyama et al. (2015) observed management challenges that rose from a critical infrastructure training event simulating a cyber incident where participants were divided into offensive and defensive teams. They found that if there is no communication path between task groups and managers specifically for a crisis or too little or too much information is shared, it can affect decision-making. Decision-making can affect the notification of authorities of incidents.

Furthermore, the Ministry of Finance Finland shared a report in 2017 on managing cyber incidents. The report includes an example framework of the communications strategy for incidents. The strategy should include the target group, communication channels, roles and responsibilities, and specific requirements. (Ilkka et al., 2017.)

Some authors pointed out the human aspect of the incident response process that affects the handling of the incident. Some were related to the incident manager. Besides having an up-to-date contact list to identify the correct people within the organization to aid with incident management and have a skilled and trained incident handler to identify critical people without the help of a plan and procedure since it might be challenging to document as they depend on the current situation at hand. (Hove et al., 2014.). The incident manager should know who should be informed of the incident and know the person responsible for external communication (Luttgens et al., 2014). The incident management teams themselves should be diverse. It is more common in large or medium-sized companies to collaborate with legal than small businesses. Large organizations should include collaboration between different stakeholders, such as legal or HR, in their incident management tools. (Staddon & Easterday, 2019.) Bartnes et al. (2016) found in their paper that when studying Norwegian electric power companies, organizations should create cross-functional teams to improve incident management practices. Creating cross-functional response teams means people making decisions should include individuals from various functional areas. Since each might have their own goals in an incident, they should employ organizational-wide goals. Luttgens et al. (2014) agree; in their opinion, incident response requires stakeholders from various areas in the organization, such as legal, human resources, and public relations, though public relations and human resources might not be a part of an investigative or remediation team. (Luttgens et al., 2014 p. 26.)

Organizations are concerned about the absence of people aware of the Incident Management Process (Line et al., 2014). In Nyman & Grosse's study (2019) concerning GDPR and incident management in IT consulting firms, one company said they only had two people with knowledge about IT incident management and raised the issue of their possible absence in an incident. Staves et al. (2022) analyzed UK-centric incident response guidelines and standards related to industrial control systems in their paper. Most of the guidelines, around 80%, discussed the importance of roles and responsibility assignments and documentation—only around 34% of the documents covered resource availability. Resource availability places enormous emphasis on allocating resources to different individuals (or non-humans). Regarding notifying authorities, Kapoor et al. (2018b) mention about GDPR that organizations should know the regulations, familiarize themselves with the notification requirements, and assign roles and responsibilities.

There was also a noticeable lack of training for personnel involved in incident response. Developing specific plans for different scenarios may not be possible or valuable, so the incident handlers should be trained, for example, by rehearsals. (Hove, et al., 2014) Kapoor et al. (2018b) highlighted a lack of following or using their existing incident response plans. Employees might not be aware of

incident response documents or be well-established. Another aspect that influenced incident management was the lack of employees trained for incident response. The training activities within organizations do not consider incident management. (Line et al., 2014.) Anson (2020) recommends training people not directly on the Incident Response Team but other stakeholders whom the Incident Response Team needs to interact with. The Incident Response Team should work closely with other business operations and stakeholders. Kral (2011) recommends in the SANS Incident Handler's Handbook that organizations have training for incident handling. They describe that the CIRT, i.e., Computer Incident Response Team, must know what to do in case of a real-life incident. Organizations should learn from past incidents and preparedness exercises (Bartnes et al., 2016; Kapoor et al., 2018b). Nyman et al. (2019) recommend involving experts and people new to the field in the Information Security Incident Management process and document causes and consequences to create organizational learning. Jones (2020) reminds that organizations who rehearse and maintain incident management protocols ensure identifying and mitigating impacts of security events. NIST 800-53 recommends testing incident response in organizations through, e.g., tabletop exercises (National Institute of Standards and Technology, 2020b).

The findings highlight the necessity for distinct incident management policies, as recommended by standards and frameworks like NIST, ENISA, and ISO. However, there is a noticeable discrepancy between these guidelines and their real-world application. Issues such as ambiguous roles within incident management teams, insufficient documentation and training, and the lack of a systematic method for managing communications during incidents are prevalent. These challenges point towards a need for future research focused on refining incident notification frameworks, enhancing the integration of cross-functional teams, and improving organizational training to prepare for and manage security incidents effectively.

2.3 The decision-support framework for disclosing security incident information

There is a limited number of frameworks for reporting cybersecurity incidents to authorities. Governments, agencies, and public authorities have guidelines that often focus either on one specific legislation or provide a checklist for organizations that only include minimal information for incident reporting (Cichonski et al., 2012; European Banking Authority, 2021; Institute for Security and Technology & Cyber Threat Alliance, 2023). Most likely this is because there can be several legislations in one country affecting one company that, in addition, operates in various countries. The nuisance for organizations is that they might have to report incidents to several different actors, i.e., in Finland to CERT-FI, the Data Protection Ombudsman, and others in several different countries.

Kulikova et al. (2012) have created a decision-support framework for disclosing security incident information. The framework focused on incident

notifying or reporting, considering internal and external stakeholders. It does not focus primarily on notifying authorities of an incident but instead on the overall incident disclosure of an organization. The decision-support framework introduces four steps for organizations to report incidents to relevant entities. They highlight that the content, time frame, and audience might differ with incident notifications, so it is essential for organizations to create a strategy for incident reporting. (Kulikova et al., 2012.)

The first step entails the formation of the Incident Response Team (IRT). Before this, the security incident should be confirmed, and the severity must be evaluated. This can be done by, for example, using the IT service. Depending on the organization's processes, the confirmation of the security incident can be done by external or internal parties. The severity should be assessed based on the business impact the incident causes. Organizations often use confidentiality, integrity and availability of IT systems impact scoring to define the impact. After the incident has been confirmed and the impact assessment is done, the company should form its IRT. The list of participants should be pre-defined and depend on the impact of the incident. For example, suppose the incident is severe for the organization's operation. In that case, the team should include several relevant stakeholders, i.e., the IRT, legal, senior management, and corporate communications. (Kulikova et al., 2012.)

The second step is to assess the specifics of the incident and the organization's priorities. The specifics of the incident are gathered with the help of a questionnaire, and the organizational priorities determine what the organization wants to achieve with the disclosure strategy. The questionnaire provides information for the organization, i.e., allocates resources and determines if external disclosure is required. The questions provided in the decision-support framework can be specified or lengthened depending on the organization, e.g., its industry and data. The questionnaire is as follows:

- 'How was the incident discovered? (e.g., internally, by law enforcement, media, or hacker)
- Which locations does the incident cover?
- What is the attack result? (e.g., unauthorized access, misuse of data, disruption of services)
- Does the incident present a material risk?
- Is external help required for the incident mitigation?
- Can voluntary sharing anyhow benefit the company?' (Kulikova et al., 2012.)

The incident response priorities are: 'restoring operations quickly, avoiding regulator and auditor scrutiny, restoring damaged reputation, avoiding media coverage, minimizing customer impact, minimizing direct incident costs, identifying root cause vulnerability and prosecuting those responsible' (Kulikova et al., 2012

p. 109). These should guide the company in managing its resources and priorities in an incident. (Kulikova et al., 2012.)

The third step is strategy mapping for incident disclosure. This includes a knowledge database, disclosure strategy mapping, and incident status updates. The knowledge database refers to a database that, depending on the organization, contains the compliance aspect, i.e., external disclosures: who to report to, when to report, and what content. The database could include notification templates, available communication channels, and message templates to customers who should be notified, among other things. The disclosure strategy mapping refers to when the IRT has gathered relevant information from the knowledge database, and they can decide on the optimal incident disclosure strategy. The incident status update means that the IRT should be able to receive status updates from, e.g., the IT team if the specifics of the incident change. (Kulikova et al., 2012.)

The last step is post-disclosure learning. As the name suggests, companies will learn from each disclosure and its related activities. It should include all the decisions made, for example, disclosure audience, content, timeframe, and methods. The most important aspect is to go through each step of the incident. Make sure the disclosure strategy was followed, and if not, why, and then summarize the key findings of the incident and the disclosure approach. This information can be stored in the Knowledge Database later on. (Kulikova et al., 2012.)

2.4 EU legislations

Following the findings that emphasize the need for clearer incident management policies and reporting, this chapter will explore how the European Union is tackling these issues with new legislation. These laws are designed to enhance cybersecurity practices across Member States as one of the EU's priorities is digital transformation. This means the EU wants to:

> 'strengthen Europe's capabilities in new digital technologies, open new opportunities for businesses and consumers, support the EU's green transition and help it reach climate neutrality by 2050, support people's digital skills and training for workers, and help digitalise public services, while ensuring the respect of basic rights and values'. (European Parliament, 2021a)

The EU recognizes the impact of cybersecurity on ordinary consumers. The aim is to protect both people and organizations against cyber threats. (Europen Parliament, 2022.) Thus, the EU has adopted several legislations to ensure that companies will strengthen their cybersecurity. The EU highlights the importance of critical infrastructure in terms of essential services and critical sectors. (European Parliament, 2021b.)

This thesis addresses three of the different EU legislations that are aimed at strengthening European people's and European businesses' cybersecurity: Network and Information Systems 2 Directive (NIS2), Critical Entities Resilience Directive (CER), and Digital Operational Resilience Act (DORA). Furthermore, they are referred to by their acronyms. NIS2 and CER are directives, whereas DORA

is a regulation. A Directive means that the Member States are bound to the objectives set out in the directive, and they have to amend their legislation based on the directive, i.e., the directive is not directly applicable. Regulation, on the other hand, is directly applicable. Member States do not have to amend their legislation based on the regulation. (European Union, 2022a, 2022b.)

These directives focus on strengthening cybersecurity and ensuring resilience. It could be argued, in simplistic terms, that the three legislations focus on critical sector entities, but NIS2 might also affect other organizations. The focus on critical entities is understandable since any effect on the providence of essential services might severely impact one or multiple societies (Luiijf et al., 2021).

All of the three legislations have some obligations for organizations to report or notify incidents to authorities. In this thesis, they are only addressed in incident reporting to authorities. The interpretation of the law is not addressed in this thesis, i.e., whether an organization falls under NIS2, CER, or DORA, or what type of incident is considered significant or a major ICT-related incident. In the following chapters, each legislation is explained on a high level, and each of the legislations requirements for reporting incidents are described.

2.4.1 Network and Security Directive 2 (NIS2)

The NIS2 directive was put in force in 2023 by the European Union. The EU is strengthening cybersecurity requirements for medium-sized or large businesses that operate and provide services in core sectors. (European Commission, 2023b; Europen Parliament, 2022). The directive is a new version of a previous NIS directive. The new version has three main things it will improve. First is the preparedness of Member States to adopt a national cybersecurity strategy. The directive also requires Member States to create a more straightforward process for handling risks and incidents by appointing a national 'Computer Security Incident Response Teams (CSIRTs)', as well as a national cybersecurity authority and 'single point of contact (SPOC)' (European Commission, 2023a). The SPOC will ensure cooperation between the Member States authorities and other relevant authorities (European Commission, 2023a). The directive's second enhancement is national cooperation between Member States and their CSIRTs through the NIS Cooperation Group. Lastly, NIS2 expands the scope of NIS by adding more sectors and creating a size threshold, ultimately leading to more companies reporting security incidents. (European Commission, 2023a.) In addition, the Member States must determine which essential and important entities are subject to NIS2 (Singh, 2023).

NIS2 also imposes obligations on statutory bodies. It means it is harder to delegate responsibility to an employee, for example, an information security employee. (Wanecki et al., 2023.) Singh refers to the same aspect in his paper. Management bodies should have regular training to understand and oversee cybersecurity risks. He also mentions that they are held to account if they do not comply with the obligations of NIS2. Depending on the Member States ' laws, they might be fined or liable for breaches. Singh recommends that organizations start

amending or preparing their plans to meet the requirements of NIS2. (Singh, 2023.)

2.4.2 Reporting obligations in NIS2

The previous NIS directive, as mentioned above, did not cover as many sectors and entities, which also meant reporting obligations. Previously, the reporting obligations were to notify authorities of incidents that had 'a significant impact on the continuity of the essential services they provide'. (Council Directive 2016/1148/EC, 2016.) The significance of the impact was evaluated based on the number of users the incident had affected, the duration of the incident, and the geographical spread (Council Directive 2016/1148/EC, 2016).

In the new NIS2 directive, article 23 defines obligations for reporting incidents. One of the first things an organization has to take care of is to communicate without undue delay or within 24 hours to important entities about a significant incident. An incident is considered significant if the company has or will suffer significant financial loss or severe operational disruption, or a natural or legal person could be affected or could be capable of being affected by causing considerable material or non-material damage. (Council Directive 2022/2555/EC, 2022.)

The directive also states that organizations have a time limit to report certain information about the incident if it is considered significant. In 24 hours, they must report the incident to CSIRT or another similar authority and indicate if they suspect it is malicious or unlawful or might have a cross-border impact. (Council Directive 2022/2555/EC, 2022.) The previous directive, NIS, had no time limit but stated 'without undue delay' (Singh, 2023). The 24-hour time limit makes the legislation more straightforward. It also includes two other notifications. In 72 hours, the organization must update the information they have provided and give an initial assessment containing the severity, indicator of compromise, and impact if they are aware of it. (Council Directive 2022/2555/EC, 2022.) The last notification is the final report. The organization's time limit for this is one month after the incident or, if not possible, within one month as soon as they have identified the root cause. The final report includes a more comprehensive view of the incident, including the severity and impact, the root cause, measures on how the organization is mitigating the incident, and, if possible, additional information about the cross-border impact. (Council Directive 2022/2555/EC, 2022.) The organizations must also notify the authority of relevant status updates, or if the authority requests. (Council Directive 2022/2555/EC, 2022.)

The European Commission's aim is clearly to increase the reporting of incidents. It mandates that incidents must be reported not only when they have caused substantial or considerable harm but also when there is a potential for such harm. (Schmitz-Berndt, 2023a; Schmitz-Berndt et al., 2022; Council Directive 2022/2555/EC, 2022.) This is noteworthy because, as Schmitz-Berndt explains, organizations are required to issue a notification within 24 hours of discovering an incident (Schmitz-Berndt, 2023a). This stipulation implies that within a very short time, organizations must assess and understand the impact of the incident.

Furthermore, the EU aims to streamline the reporting process compared to the previous NIS legislation, introducing specific requirements regarding the timelines and content of reports to simplify compliance (Singh, 2023). This adjustment increases the reporting of incidents and facilitates a more efficient and clear process for organizations.

NIS2 is an EU-wide legislation, but it has also reached other countries. For example, the reporting framework created by US-based cybersecurity organizations also refers to NIS2. It discusses what kind of incidents should organizations report and refers to NIS2's definition of a substantial cyber incident. (Institute for Security and Technology & Cyber Threat Alliance, 2023.)

2.4.3 The Critical Entities Resilience Directive (CER)

In 2023, the European Parliament put in force the directive on the Resilience of Critical Entities, known as CER (European Commission, n.d.). Member States have until 2025 to amend their legislation based on CER (Valtioneuvosto, 2022). As the name suggests, the directive aims to create a stronger resilience for critical entities against threats, such as insider threats or terrorist attacks (European Commission, n.d.). The focus points for the critical entities are preparedness, international cooperation, and response (European Commission, n.d.). It aims for critical infrastructure to manage risks, recover swiftly, and maintain operations in case of an incident (Pallagi et al., 2023).

Member States need first to identify critical entities. These entities then have to improve their resilience by focusing on technical, organizational, and security issues and notifying incidents to authorities. The Member States must provide support for these entities in this process. To create better cooperation across Member States and the European Commission, the Critical Entities Resilience Group is established. (European Commission, n.d.) CER applies to 11 different sectors: digital infrastructure, banking, energy, financial market infrastructure, water, energy, health, space, transport, wastewater, and food (Singh, 2023). CER complements NIS2 (Pursiainen & Kytömaa, 2023; Singh, 2023). This means some organizations fall under both legislations (Vandezande, 2024).

2.4.4 Reporting obligations CER

CER also obligates organizations (critical entities) that fall under the legislation to notify competent authority about incidents that either have a potential to significantly disrupt or does significantly disrupt the provision of essential services. Significant disruption means it is left for the organizations to determine whether the incident is or could be a significant disruption. They should evaluate the number or proportion of users that are affected, the duration of the disruption, and the 'geographical area affected' and consider whether the area is geographically isolated or not. (Council Directive 2022/2557/EC, 2022.)

The first notification should be done within 24 hours after becoming aware of the incident, and a more comprehensive report within a month. Unlike NIS2, CER does not state a 72-hour notification. (Council Directive 2022/2557/EC,

2022.) Both notifications should include information for the authority to 'understand the nature, cause and possible consequences of the incident'. It should also include information from which the authority can determine whether there is a cross-border impact. (Council Directive 2022/2557/EC, 2022.)

2.4.5 The Digital Operations Resilience Act (DORA)

The Digital Operational Resilience Act (DORA) is an EU-wide regulation. As pointed out earlier, a regulation is directly applicable in Member States. It was put into force in 2023 and will apply as of January 2025. The regulation aims to build stronger resilience in the financial sector. (Eiopa, n.d.) The financial sector does not refer only to traditional financial sector entities such as banks or investment firms but also to organizations such as trade repositories, e-money institutions, and credit rating agencies (Clausmeier, 2023). The finance and banking sector suffers from many cyberattacks since the industry is very lucrative for criminals. Accessing financial sector entities, criminals can access large amounts of capital. (Clausmeier, 2023; Singh, 2023.)

The regulation focuses on managing risks, testing resilience, sharing information, and supervising critical third-party vendors (Eiopa, n.d.). The European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority are preparing policy measures. These measures facilitate the implementation of DORA (Eiopa, n.d.). Compared to NIS2, the DORA requirements for organizations are much more detailed. Additionally, the latter will take precedence if there is an overlap within NIS2 or DORA. (Clausmeier, 2023.)

2.4.6 DORA reporting obligations

The harmonizing of reporting requirements is crucial. DORA aims to do this with financial institutions (Clausmeier, 2023). The problem has been that the EU-wide legislations for the financial sector has been incomplete. Certain areas, such as incident reporting and digital operational resilience testing, overlap or have gaps. (Eiopa, n.d.) The regulation requires organizations to inform the competent authority about major ICT-related incidents. A major ICT-related incident 'means an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity'. (Council Directive 2022/2554/EC, 2022)

DORA requires financial entities to make three notifications of incidents to the relevant authority. The first is the initial notification, and the second is an intermediate report that includes updates on the incident, such as if the status has changed or new information is available. The last one is the final report, which includes the root cause. The first notifications must include information about the incident to the extent that an authority can determine the significance and evaluate if there is a cross-border impact. The second report should be sent when there is a significant or relevant status change regarding the incident, when new information is available, or when the authority requests information.

(Clausmeier, 2023; Council Directive 2022/2554/EC, 2022) The final notification should be done after the root cause analysis is complete and when the actual impact figures of the incident are available. The last report does not consider whether the organizations have set any mitigation measures in place. (Clausmeier, 2023.) Unlike NIS2 and CER, DORA does not mention a timeframe in which an organization has to report incidents. This is left to ENISA and ECB in Europe to decide the reporting timeframes (Council Directive 2022/2554/EC, 2022). The European Supervisory Authority, or ESA, will specify the notification's details later.

2.5 Incident reporting obligations in all three legislations

The three legislations, NIS2, CER, and DORA, the EU has put in force have specific obligations for reporting incidents. They all have a definition for a specific incident to report, be it a significant incident, an incident that significantly disrupts the provision of essential services, or a major ICT-related incident. Figure 2. shows the timeframes and contents of each legislation notification. DORA's timeframes have not yet been published while this thesis was written.

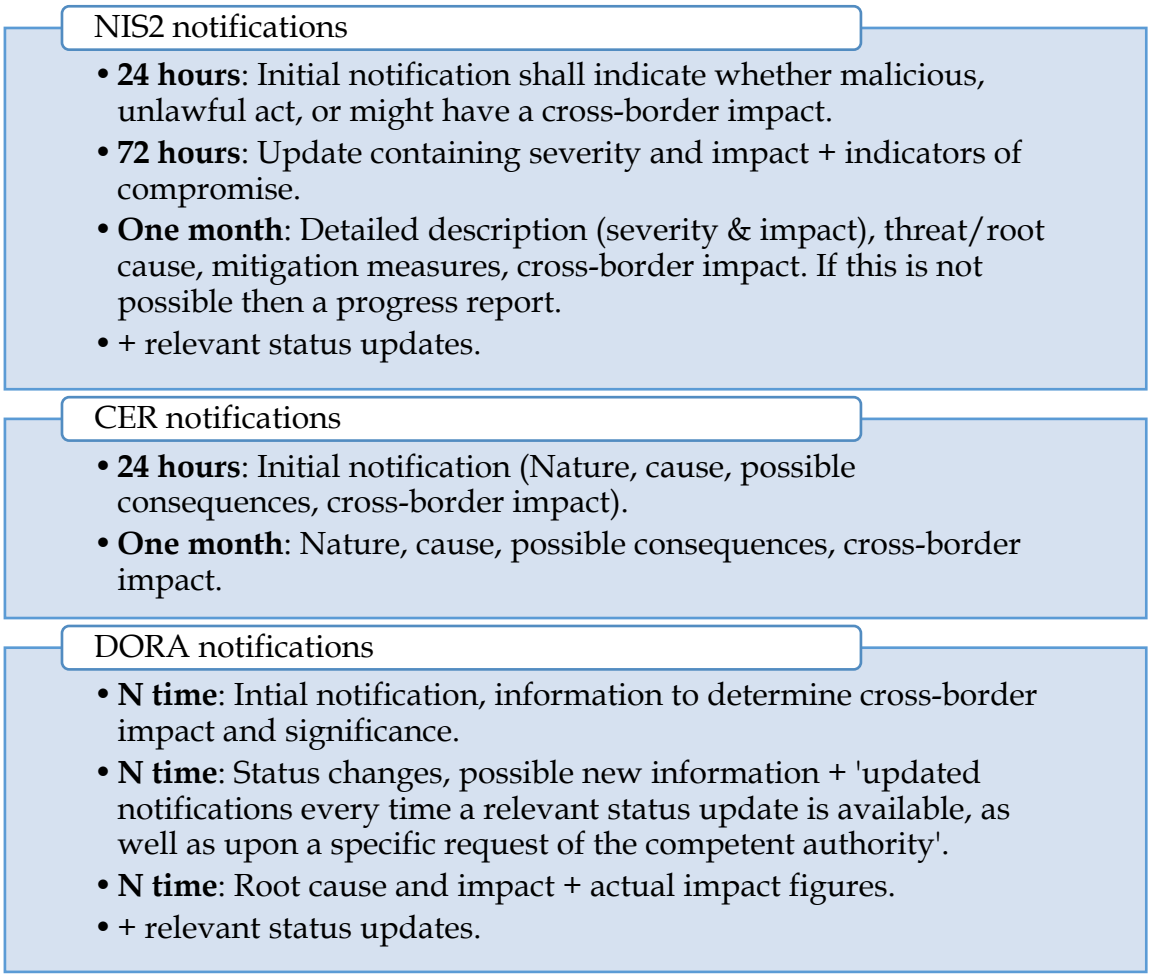

FIGURE 2 Notification timeframes

While the legislation may not introduce substantial changes for organizations operating within the critical sector, NIS2 notably expands the scope of what constitutes critical entities. Organizations affected by this or any of the three key legislations must be precise about when, to whom, and what to report. This includes understanding the specific content of each notification, the timelines for these notifications, and identifying the appropriate entity for reporting. They must also determine which types of incidents warrant such reporting.

Reporting obligations are well-established for organizations within the EU. As mentioned in this thesis, the GDPR mandates a notification timeframe of 72

hours. Compliance with the legislative requirements of other jurisdictions, such as the US or India, is also necessary for organizations operating internationally. While larger organizations with substantial resources may find it relatively easy to navigate these requirements, smaller organizations, particularly those in countries with limited resources to support businesses, may face challenges.

It is crucial to acknowledge that during a significant incident, the primary focus for organizations is often on maintaining business continuity. In scenarios where preparedness is lacking, some aspects, like notifying authorities, might be overlooked. To avoid potential sanctions, organizations must be equipped to assess whether an incident should be reported quickly, what information needs to be included, and to whom it should be sent. The procedures they adopt should detail the required information for notifications, any necessary follow-up, and the associated timelines. Organizations can streamline procedures and enhance compliance efficiency by adhering to regulations and managing this information effectively.

2.6 Cybersecurity Exercises

Organizations must be prepared to handle cyber incidents effectively and understand the processes and procedures for managing such crises. As new legislations that affect incident management are introduced, understanding these procedures is more important than ever. This comprehension can be achieved through targeted training. One form of training for incident management is through cybersecurity exercises. This section outlines what cybersecurity exercises are, which is essential for this thesis as the data was collected from experts who participated in such exercises. More details about methodology are provided in Chapter 3.

Cybersecurity exercises are sessions where organizations test their resilience and preparedness against an incident. It simulates a fictitious situation that enables the organization and participants to test or develop their capabilities against disruptions. (Aaltola et al., 2019; Mäses et al., 2021; Traficom, 2019.) Cybersecurity exercises are training events in which the participants learn about an organization's procedures in case of an incident (Mäses et al., 2021; Ouzounis et al., 2009).

Cybersecurity exercises are used as tools for training cybersecurity professionals and other stakeholders in an organization (Aaltola et al., 2019; Karjalainen et al., 2020). Cybersecurity exercises are a tool for situational awareness and incident preparedness (Dewar, 2018). Some papers describe them as active learning tools (Brajdic et al., 2021; Dewar, 2018). Active learning means a tool that aims to achieve more than what is possible, i.e., through lectures. This means the participants in an exercise can put their knowledge into practice and test their preparedness in a crisis. The exercise brings different types of threats and risks associated with real life. (Dewar, 2018.)

There are several types of cybersecurity exercises, such as tabletop, premortem, functional, technical, or capture the flag. The type of exercise depends on the organization’s needs. (Hautamaki et al., 2019; Traficom, 2019.)

Cybersecurity exercises are beneficial in evaluating, reviewing, and finding deficiencies in plans and processes. Regardless of which type they are, cybersecurity exercises help build knowledge about an organization's strengths and weaknesses in their operations, enhance the cooperation between different stakeholders, provide a chance to exchange insights between participants, and enable the evaluation of current processes. (Dewar, 2018; Ogee et al., 2015.) The organization's personnel should understand their roles and responsibilities, the plans and processes should be validated, and the system or system components should be operational as described in the plan (Aoyama et al., 2017; Grance et al., 2006).

There is a discussion about who should participate in the exercise. Pargman (2020) writes that the participants of a cybersecurity exercise should be the executives who are in charge and have a responsibility in the response plan. Coden et al. (2023) discuss in their paper that tabletop exercises should also include employees from different departments, such as operations and administration, among others. They believe having only the incident response or crisis management team is not enough. Gurnani et al. (2014) do not specify which people from the organization should attend but emphasize that exercises will improve employees' preparedness in a cyber crisis when all the stakeholders are present. ENISA's report aligns with the views of Gurnani et al., highlighting the benefits of involving stakeholders from diverse sectors within the organization to enhance cooperation. The report particularly stresses the importance of recognizing the cross-border nature of cyber incidents, noting that effective collaboration among stakeholders is essential in such contexts. (Ogee et al., 2015.) The Finnish National Cyber Security Centre states that the exercise participants should depend on the objectives. If the objective is to improve, e.g., managing a crisis, it should include the management team and communications. Communication is recommended in every situation since it is a crucial stakeholder when an organization suffers an incident. (Traficom, 2019.)

The organization's needs and participants could be interpreted as the objectives of the exercise. White et al. (2004) and Dewar (2018) argue that the format of the exercise, i.e., tabletop or capture the flag, depends on the objectives. Suppose the objective is to increase awareness about cybersecurity among participants and educate them on the organization's incident management processes or procedures. In that case, the tabletop exercise is most suitable, but if the goal is to test the ability to detect an attack, another exercise format is better. Mäses et al. (2021) agree; in their paper, they use an example that if the objectives are more people-oriented, then a tabletop exercise would be more suitable than a technical objective, such as improving technical capabilities of a system.

2.6.1 Tabletop exercise

To validate Incident Response plans, organizations should conduct a cybersecurity exercise. (Brajdic et al., 2021) The tabletop exercise is the most effective option for reviewing and understanding procedures and processes (Schreider, 2019). Tabletop exercises are conducted around a table, meaning the participants are in the same meeting or around a table. There is always a facilitator who leads the

exercise. (Brajdic et al., 2021; Dewar, 2018; Schreider, 2019.) ENISA's report by Ouzounis et al. (2009) agrees and adds that tabletop exercises are simulations where participants become familiar with the procedures. MITRE (2006) and NIST (2014) define tabletop exercises as events where participants discuss their roles in an emergency and their responses to the situation. (Grance et al., 2006; Kick, 2014) The Finnish National Cybersecurity Centre (2019) defines tabletop exercises as discussion-based exercises that do not involve a technical environment. The participants are presented with a scenario, and they talk it through. The outcome of the exercise is to create a plan for cybersecurity incidents or check the current plan and evaluate its up-to-datedness. (Traficom, 2019.) Angafor et al. (2020) discuss in their paper that the definitions for a tabletop exercise differ between scholars. In their study, they refer to tabletop exercises as training activities where, e.g., various stakeholders and CSIRT gather to discuss, evaluate, test, and review actions for handling threats against information security management systems. (G. Angafor et al., 2020.)

A cybersecurity exercise scenario is a fictitious situation of an incident, and the exercise is built around the scenario (Grance et al., 2006). The scenario is typically built around the business, i.e., the scenario is life-like. Cybersecurity exercises should be realistic, challenging, and relevant to create a better learning experience (Angafor et al., 2020b). The scenario should be realistic and relevant to the participants. The goal of the exercise plays a crucial role, which is why the scenario should be adaptable according to the objectives and support the objectives. (Aoyama et al., 2017; Mäses et al., 2021.) According to NIST, the scenario should encourage responses (Grance et al., 2006). Some events, known as injections, change the course of the scenario, and the participant's reactions and responses are followed and analyzed to evaluate how prepared the participants are for the injections (Gurnani et al., 2014).

In tabletop exercises, the participants understand their own and other participants' responsibilities and roles and improve their decision-making skills (Angafor et al., 2020, 2023; Aoyama et al., 2017). Tabletop exercises can also benefit participants in terms of collaboration and communication skills (Angafor et al., 2020). Through tabletop exercises, participants understand the incident response process. Tabletop exercises are vital for the Incident Response team and other stakeholders to remember and understand the plans and processes an organization has in place for responding to incidents. This also gives the participants confidence in themselves and the organization when dealing with incidents. (Angafor et al., 2020; Anson, 2020.)

On an organizational level, tabletop exercises can be used to evaluate an organization's resilience, i.e., how an organization responds to unexpected events (Aoyama et al., 2017). The exercise enables the organization to test, evaluate, and update its Incident Response plans and see if they apply to a real-life incident. Part of this is identifying weaknesses. (Angafor et al., 2020, 2023; Grance et al., 2006.) In Angafor et al. (2023) study, the cybersecurity exercise got the managerial staff to evaluate the organization's readiness and ability to identify, respond, and recover from incidents and strengthen their defenses against similar attacks by creating Action Plans.

ENISA's guide (2009) for cybersecurity exercises states that one of the most common measures tested in cybersecurity exercises is communication procedures between different organizations. This includes, e.g., CERT's, authorities, customers, and suppliers. The reason for testing communications between organizations is that these entities should be notified in the event of an incident. The testing includes ensuring they have the current contact details and that people can be reached. (Ouzounis et al., 2009.) Participants can identify communication channels that should be created in an exercise (Dewar, 2018). By exercising, for example, crisis communication, the organization can develop a toolbox for different kinds of crises. This toolbox may help the organization save time during a crisis. The toolbox may include the target groups, communication needs, and priorities for each crisis situation (Tuomala et al., 2021). Many other reports of exercises do not highlight the importance of communications between organizations. Notifying authorities is just one part of incident management. But now that the EU has introduced new legislation that obligates organizations to notify relevant authorities about incidents and has added timeframes for notifications, the communications aspect of an incident response plan raises the importance of communications.

2.6.2 Objectives and outcome

One of the most critical aspects of cybersecurity exercises is the objectives (Aaltola et al., 2019; Furtună et al., 2010). The objectives determine what the participants and the organization will benefit from the exercise (Kick, 2014; Ouzounis et al., 2009). NIST argues that in a tabletop exercise, the objective should be to validate the IT plan and other related policies (Grance et al., 2006). On the other hand, Finland's National Cyber Security Centre does not state any specific objectives in its exercise report but recommends that the objectives should come from safety, testing a process, competence development, or increasing the performance of some operations (Traficom, 2019). Karjalainen et al. (2020) argue that the learning objectives of cybersecurity exercises can be from an organizational or an individual perspective, but they both should be about competence development.

Dewar (2018) categorized in his report five different objectives for cybersecurity exercises: Identification, testing mechanisms and/or procedures, drills, to increase communication and cooperation, and lastly, development of policies and procedures. Identification refers to an exercise that aims to highlight and identify either technical or systemic vulnerabilities, information-sharing mechanisms, or procedural flaws. Technical or systemic vulnerabilities focus on finding vulnerabilities within the IT infrastructure, i.e., zero-day vulnerabilities. The information-sharing mechanism refers to sharing information about a cyber incident between the public and private sector. This way, participants can identify problems with channels and the absence of channels and recognize the most effective channels. The third issue, i.e., procedural flaws, aims to identify problems in practices, policies, procedures, or processes that can affect the incident response negatively. The second part, 'testing mechanisms and/or procedures,'

refers to testing the elements that have already been identified and making sure they are working as intended. Mechanisms can either mean testing technical tools or how the people involved in the incident respond to the situation. It can also refer to a cyber exercise that tests if legislation related to cyber incidents is 'fit for purpose' or testing compliance. Drills focus on the mechanisms mentioned earlier and procedures to be used to ensure readiness if an incident occurs. The mechanisms and/or procedures are not just tested but exercised. The fourth aim related to the information-sharing mechanisms is highlighted as one of the most important objectives. Participants' cooperation with each other is essential because the decision made in an incident cannot be made by just one person but is discussed amongst multiple individuals. However, communication is not just within the Incident Response group or the organization but also with different actors: the private and public sectors. Dewar writes that two benefits arise from these types of exercises: Identifying problems related to effective communication between actors and identifying inefficient decision-making processes, resulting in a hindered response to cyber events. The fifth focuses on developing a policy that efficiently responds to cyber incidents. This does not involve focusing on current policies but creating a new one based on the cyber exercise simulation.

According to MITRE, cybersecurity exercise objectives define the outcome. The outcome should be to make participants aware of cyber threats and cybersecurity and evaluate the response plans. (Kick, 2014.) Mäses et al. (2021) agree that the objectives are linked with the outcome. They discuss that the objectives should be SMART, i.e., 'specific, measurable, assignable, realistic and time-related'. Aaltola et al. (2019) also refer to the SMART learning outcomes regardless of the type of education it is (Aaltola et al., 2019) Wilhelmson et al. (2011) add one more aspect to the measurable objectives, i.e., SMARTA. The last letter represents adequate, i.e., the objectives should fit the purpose. NIST explains that the outcomes are derived from the report made after the exercise. The report includes, for example, the organizers' observations and recommendations for the IT plan. The outcomes would be to improve or update the IT plan or other documents related to the exercise, briefing managers, or other actions. (Grance et al., 2006.) Finland's National Cyber Security Center briefly mentions the outcomes of a tabletop exercise as answers to questions or a list of things that must be clarified (Traficom, 2019). The orientation of participants also affects the learning outcomes or the qualities of the exercise, i.e., how realistic, challenging, or relevant it is (Hautamaki et al., 2019; Mäses et al., 2021). Dewar (2018) states that realism and a sense of urgency are not as prominent in tabletop exercises since they are discussion-based

In conclusion, the cybersecurity exercise is closely tied to its objectives. The objectives determine which type of exercise is most suitable and what should be achieved. Tabletop exercises are highly recommended for testing and evaluating incident response plans. These exercises provide a structured environment where participants can fully understand the plan's details, and their roles in it and learn about the roles of other stakeholders. This setup prepares participants to act effectively and collaboratively during a cyber incident. Additionally, tabletop exercises identify gaps in current response strategies and create a deeper understanding of potential real-world challenges, enhancing overall

preparedness. Such training enables organizations to prepare for incident management and understand their existing processes and procedures. This training also allows organizations to assess whether their plans are insufficient regarding complying with new legislation.

2.7 Literature review conclusion

The literature review has covered four main sections: the importance of reporting incidents to authorities, the decision-support framework, the new legislations (NIS2, CER, and DORA), and familiarizing the reader on cybersecurity exercises. As the literature review demonstrates, the legislations will bring considerable changes on how organizations report cyber incidents to authorities. They expand the scope of organizations required to report incidents, detail the specific information that must be disclosed, and define the timelines for these notifications. This creates a need for having a structured approach to reporting incidents. Research has been conducted on incident management focusing on the best strategy to handle incidents and data breach notifications.

While there are existing guidelines and frameworks, none fully consider the obligations introduced by the new legislations. Therefore, the thesis examines the comprehensive decision-support framework to determine whether organizations' current practices align with the decision-support framework and to identify potential pitfalls and success factors (Kulikova et al., 2012). Given that the decision-support framework was established before the enactment of NIS2, CER, and DORA, the thesis also explores how these new mandates might influence the adaptation of the decision-support framework.

To improve the understanding of how organizations manage cybersecurity incidents, the literature review included a detailed examination of cybersecurity exercises. These exercises are essential for training organizations employees and observing their responses to simulated cyber threats. The literature review provides insights into how these simulations help organizations, for example, test their incident response strategies, improve their communication, and identify weaknesses. The introduction to exercises was relevant as the data for this thesis was collected from observers of these exercises.

3 Methodology

The methodology chapter of this thesis is structured into four sections: The first section explains the method for the study, the second describes the data collection methods, the third focuses on the interviews conducted, the fourth describes the methods of analysis used, and the final section assesses the trustworthiness of the study.

As previously noted in this thesis, little research has been done into notifying incidents to authorities and related legislations. This thesis aims to enrich the scientific field by addressing the research questions: **Do organizations practices align with the decision-support framework in reporting cyber incidents to authorities? How do these practices fail or succeed? Do the legislations, NIS2, CER, and DORA, warrant adaptations to the decision-support framework in reporting incidents to authorities?** The study approaches to finding answers to these research questions by conducting a case study. The basis of the study is the decision-support framework of Kulikova et al. (2012) for disclosing security incident information, referred to as the decision-support framework. The scope of the thesis is limited to the actions taken up to the point of incident disclosure. The post-disclosure phase which involves retrospective learning and strategy adjustments, falls outside the boundaries of this study. Including this phase would broaden the scope and potentially dilute the specific focus on pre-disclosure decision-making dynamics and regulatory compliance. Therefore, to keep a focused analysis on the specified objectives, this work will not delve into post-disclosure learning.

A case study approach was chosen due to the possibility of using the decision-support framework as a lens within its real-life contexts. The framework in question has not been evaluated or reviewed by seeing how it would apply in practice. A case study focuses on either one case or several cases. The case is always linked to the research question in trying to understand and solve the case. (Eriksson & Kovalainen, 2008) According to Eriksson and Koistinen. (2014), case studies are particularly suited to addressing "what," "how," and "why" questions, or the researcher does not have that much control over the events, or in case the empirical studies are lacking on the subject or the phenomena is currently in this current time and current life. (Eriksson & Koistinen, 2014, p. 4) Qualitative data is often used in case studies but does not count out quantitative data (Eriksson et al., 2014, p. 4). By studying a case, the researcher aims to create an understanding of the phenomena without trying to generalize the information (Saaranen-Kauppinen & Puusniekka, n.d.).

Eriksson et al. (2014) differentiate between two main types of case studies: intensive and extensive. Intensive case studies focus on gaining a deep contextual understanding of one or a few cases, often to study something unique. On the other hand, extensive case studies aim to find similar qualities in certain phenomena or processes and create new theoretical ideas or concepts by comparing several cases. An extensive or comparative case study ultimately focuses on testing former theories or, in a new environment, complements them. It can also involve developing or testing new theories or creating new explanatory models.

(Eriksson & Koistinen, 2014, p. 18-20, 11) Thus, this thesis is an intensive case study, focusing on gaining understanding on how organizations practices align with the decision-support framework and whether the legislations warrant any changes to the framework.

Case studies are not straightforward processes; they are iterative, often requiring the researcher to revisit various stages of the research process, such as redefining questions. Good research questions will guide how the data for the study is gathered, the analysis is conducted, the conclusions are constructed, and the report is written. It is adaptive, allowing research questions to evolve based on emerging data during the study. (Eriksson et al., 2014, p. 22-24) As the research process progressed, the author continuously refined the research questions and evaluated frameworks or guidelines based on the literature review to select the most suitable one for the thesis. This iterative process helped to ensure that the study remained aligned with the insights from the literature review.

A well-crafted initial research question helps focus the literature review, ensuring it is directly relevant to the study's topics. In this study, the author has familiarized themself with existing research and literature to establish a solid foundation for the study. A literature review enables the researcher to explore existing research on the topic, examining the perspectives from which it has been studied and establishing how the current study aligns with these previous works (Hirsjärvi et al., 2009, s. 121).

Another critical aspect of case study research is the selection of cases. As noted by Eisenhardt (1989), choosing appropriate cases is vital as it defines the population from which the research sample is drawn, reduces irrelevant variability, and helps define the limits for applying the findings broadly. This selection process is crucial for ensuring that the study remains focused and its findings are robust and applicable within the defined limits. In line with the critical selection of the cases, the author chose a cybersecurity company that has several professionals who have experience in conducting or observing a variety of cybersecurity exercises. The company in question offers cybersecurity exercises as a service. The exercises simulate a crisis which the participants then must solve by following their own processes and documentation. These exercises vary in duration from an hour to a full day and can be conducted online or on-site. This choice ensures that the professionals involved have the relevant expertise needed to enrich the study's findings and contribute important perspectives on reporting incidents to authorities. By focusing on a single company that has conducted multiple cybersecurity exercises, the study benefits from rich and comprehensive data.

3.1 Data collection

The data for the thesis is gathered through semi-structured interviews. Collecting data from actual cyber incidents presents considerable challenges. Real-life cyber incidents occur constantly but unpredictably, often remaining undisclosed to the public until there has been some official communication from the organization.

Cybersecurity exercises create fictitious scenarios that imitate actual cyber incidents to simulate real-life conditions. These exercises enable organizations to, for example, test their incident management process. Consequently, the author decided to collect data through interviews with observers who have participated in cybersecurity exercises. This approach allows gaining insights from situations that closely resemble real-life cyber events, as obtaining data from actual cyberattacks would be exceptionally challenging. It would require access to confidential information about an organization's incident management process and knowledge of when a cyberattack has occurred or is occurring.

Four of the seven interviewees have participated in less than ten cyber exercises. The rest have participated in over 15 exercises. The interviewees' roles have differed from that of observers to facilitators. The nature of the exercises have been quite similar. Most were primarily tabletop exercises with some technical components, focusing mainly on incident or crisis management.

Qualitative interviews are utilized to understand activities conducted, describe phenomena and events, or provide interpretations of phenomena (Sarajärvi & Tuomi, 2017). Therefore, the author has chosen qualitative methods for their ability to delve deeply into these aspects. Semi-structured interviews were chosen for the research because it was beneficial to gather data concerning multiple cybersecurity exercises to see how organizations handle incidents. In addition, delving deeper into the answers is beneficial when the research field of the subject is limited. Semi-structured interviews allow some consistency since a similar set of questions is used in each interview. (M. Myers, 2009.) The interviews comprised a set of similar questions, enabling exploration of the specific areas of interest.

Interviews are beneficial since the interviewer is verbally interactive with the interviewee; thus, the interviewer can clarify questions or explain things if they are not understood. The interview can be very flexible, and the interviewer can finetune the order of questions and interpret the responses better than in a survey questionnaire. The interviewee can freely talk about the subject. The interviewer can clarify the answers, dig deeper into the answers, or ask a follow-up question. (Hirsjärvi et al., 2009 p. 204-205; M. Myers, 2009.)

The cons are that the interviewee might consider answering in a socially acceptable way, the interview is a time-staking process, and maybe the most important one, the answers must be interpreted in a way where the interviewer considers cultural settings and other factors that may affect the interpretation (Hirsjärvi et al., 2009, p. 206-207). Myers and Newman (2007) point out nine issues linked to interviews. One of these is that the interviewee might be under pressure regarding time and within the timeframe. They also have to give and create an opinion. A lack of trust is also problematic if the interviewee is a stranger, which can lead to them not giving out information they might regard as sensitive. There might also be an issue with time if the interviewer does not have enough time to interview the participants. The interviewer might also affect the interviewee's behavior or their answers with their behavior. Another important issue is for the interviewer to understand that they are creating knowledge for the scientific community in the interview. They also mention language as an issue. The meaning of words might be interpreted differently

depending on the person. The interviewee and interviewer might understand them differently. Insulting the interviewee might also be a scenario that will affect the whole interview. To address these issues, the study was designed with careful planning and execution. Participants were informed from the start that their responses would be anonymized, encouraging them to answer freely without fear of identification. Sufficient time was allocated for each interview to allow for comprehensive discussions. The interviewees' linguistic background with the interviewer, who all shared the same mother tongue, Finnish, and cultural background as the interviewer, enhanced the accuracy of interpreting responses. Additionally, the semi-structured interviews enabled the interviewer to dive deeper with follow-up questions, ensuring clarity. A conscious effort was made not to rush the interviewees, allowing them to express their thoughts and opinions fully.

The number of interviews does not determine whether enough data has been gathered. Instead, the essential aspect is to have a good number of interviewees so that no new insights can be gained. However, it is important to note that the interviewer has to consider why the specific number of interviewees is enough for their research and have good reasons for this. (M. Myers, 2009.) In this study, the consistency among interviewees' answers suggests that an adequate number of interviews have been conducted, which ensures that no further unique insights are likely to be uncovered.

Meeting invitations for the interviews were sent via email (Appendix 1). The invitation explained to the participants that they consented to the study by accepting the invitation to the meeting. It is essential to allow the participants to decline the interview (Hirsjärvi et al., 2009, p. 20). All of the individuals who received an invitation accepted it.

3.2 Interviews

The interviews were divided into four sections: basic information and the phases of the decision-support framework by Kulikova et al (2012) for disclosing cyber incidents. The first section, basic information, included the number and types of exercises observed by the interviewee and questions concerning relevant legislation and the nature of these exercises. The sections were designed to explore the tasks associated with the decision-support framework's first, second, and third steps. Details of these questions are available in Appendix 2.

The interviews were conducted using Microsoft Teams, with one session additionally held in person. This platform was chosen for its convenience and functionality, including recording and transcribing sessions. All interviews were recorded with the consent of the participants. In addition, they were informed that recordings would be deleted once transcriptions were completed and that all data would be anonymized. The interviews took place in April 2024. Before each session, interviewees were briefed on the study's purpose. Most of the interviews lasted for about an hour. Only one interview lasted for 30 minutes.

A validation step was added to the interview process to boost the reliability of the data collected and ensure a thorough comprehension of the responses. This

step allowed interviewees to review the transcriptions to confirm their statements' accuracy and intent. This method provides an opportunity for interviewees to clarify their responses, correct any inaccuracies, and add additional comments if necessary. The transcriptions were accepted without any modifications.

3.3 Method of analysis

In qualitative studies, the analysis starts with interviews where the interviewer examines responses, paying attention to what the interviewees mention about the studied phenomena. This involves, for example, noting both similarities and inconsistencies among the responses. (Hirsjärvi et al., 2009, p. 136.) Each interview was transcribed using Microsoft Teams' transcription function. The author reviewed these transcripts, correcting inaccuracies such as Teams' misinterpreted words or incomplete sentences while listening to the recordings. Additionally, the author removed irrelevant words related to the responses, such as 'niinku' or 'tota', which translates to 'like' or 'erm'. Transcriptions were anonymized, labeling the participants as Interviewees 1-7. The interviewees' numbering was randomized using a formula in Microsoft Excel. The anonymized transcriptions were sent out to the interviewees, who were given one week to review them.

Initially, the transcribed responses were analyzed using Microsoft Word in the interviewees' native language, where the author color-coded each relevant answer according to the steps of the decision-support framework by Kulikova et al (2012). These responses were then transferred to Microsoft Excel for further coding, aligning with the original interview phases. To ensure the accuracy of the translation, the author converted the answers into sentences and translated them into English, preserving the original meaning.

The analysis utilized deductive coding, a method where the researcher classifies and creates a specific label for any features, instances, issues, or themes. Often, in case studies where the study tries to improve or test a theory, the coding is preplanned and systematic, i.e., deductive. (Eriksson et al., 2008, p. 128.) Deductive coding means the researcher will have predefined categories from the literature or theoretical framework to organize the data. The researcher creates the codes from the research question and then sorts and organizes the data. When the codes relate to previous theory or research, the researcher must understand the theory or research well. (Bingham, 2023; Eriksson et al., 2014, p. 35; Eriksson et al., 2008, p. 128.) In qualitative data, the data is broad, enabling coding from multiple perspectives and highlighting that the researcher is constantly making choices. The research problem and the questions are constantly refined as the researcher gets acquainted with the data. (Juhila, n.d.)

This detailed coding process facilitated the merging and interpretation of data, a critical step in identifying fundamental phenomena under study (Hirsjärvi et al., 2009, pp. 149, 152). However, deductive coding faces criticism for potentially overlooking valuable insights due to its reliance on predetermined codes. Such criticisms emphasize the risk of data fragmentation and the loss of a

holistic view. To address these issues, researchers are encouraged to revisit the original data frequently to understand the phenomena being studied thoroughly. (Linneberg & Korsgaard, 2019.) The study noted this by comparing the theory to the exercise observations and finding challenges and success factors. In addition, the author went back and forth between coded answers and the transcriptions to ensure the data was correctly coded.

Another concern with deductive coding is its subjective nature. While inherent in qualitative research, researchers can mitigate this by striving for objectivity and constantly reflecting on their analytical choices. (Linneberg & Korsgaard, 2019.)

TABLE 1 Example of analyzed and reduced data

Original answer	**Code**
too many people who want to guide the situation by their own goals	Roles and responsibilities; Documentation;
impact, how significant and critical the systems are, criticality levels,	Impact assessment;
if no templates, then someone knowledgeable in the exercise or part of the process	Experience;

3.4 Study trustworthiness

Eriksson et al. (2008) recommend continuous assessment of trustworthiness throughout the study. To assess trustworthiness, the researcher must consider reliability and validity (Hirsjärvi et al., 2009, p. 231). Reliability refers to the consistency and dependability of the analytical procedures used in the research. In essence, it indicates whether the methods used, if repeated, would yield the same results. Validity, on the other hand, refers to whether the research findings are accurate and truthful. (Myers, 2009.)

In qualitative research, the concepts of reliability and validity often have different interpretations than their use in quantitative contexts. Nevertheless, Hirsjärvi et al. (2009) mention that reliability and validity should be evaluated in qualitative research. In qualitative research, some literature proposes other means to evaluate trustworthiness: credibility, transferability, dependability, and confirmability (Eriksson et al., 2008, p. 294-295; Sarajärvi et al., 2017). Credibility involves ensuring that the researcher is well-acquainted with the subject matter, establishes clear links between observations and categories, and gathers agreement or near agreement from other researchers on interpretations based on the same data. Transferability assesses the ability to relate findings to prior research, highlighting contextual similarities. Dependability requires the researcher to report the research process transparently, while confirmability demands alignment

between data and interpretations for the reader's understanding. (Eriksson & Kovalainen, 2008, p. 294-295)

To enhance the trustworthiness of this thesis, the author carefully considered the selection of methods from the start and detailed each phase of the research to ensure repeatability. Transparency was maintained throughout the research process. The interview questions are provided in Appendix 2, demonstrating that they were considerately crafted. In invitations and during the interviews, it was clearly communicated to the interviewees that their data would be anonymized. Furthermore, the author allowed sufficient time for the interviewees to respond to questions without feeling rushed.

To ensure clarity and mutual understanding, the author occasionally sought clarification on specific terms used during the interviews. This was especially prominent when discussing the Incident Response Team. The definition was clarified in the interviews with the participants through discussion.

The interviewees were selected based on their diverse experiences in multiple cybersecurity exercises and organizations. This approach was intended to gather a comprehensive understanding of the phenomena. However, a potential limitation noted in the data analysis was the impact of interviewees' long-term memory on the accuracy of their insights, given the period of the observed exercises. This variability was acknowledged as a possible constraint on the study's findings.

4 Results and analysis

The results and analysis chapter is divided into four sections focusing on the steps of the interviews. The analysis focuses on Kulikova et al (2012) decision-support framework in practice – the success factors and the challenges organizations have had regarding reporting incidents to authorities. The interviewees are referred to as I1-7.

4.1 Interviewee's thoughts on incident reporting

Many of the exercises have included notifying incidents to authorities but very lightly. As found in the literature review, incident management does not focus much on notifying authorities of incidents. Instead, it is seen as a small part of it. This trend is also evident in the exercises conducted.

Notifying authorities has focused on the cybersecurity company's professionals checking whether the exercise participants remember to make the notifications. Many exercises have not considered the notifications further, e.g., what information should be included in the notification or who should report it. It was also discovered from the interviews that the notifications often focused on GDPR data breaches rather than cyber incidents being notified to National CERT's. The interviewees explained that this might have resulted from earlier directives, such as NIS, which did not have a broad scope, and many organizations did not fall under it. Some larger exercises, particularly those involving public administration, emphasized notifying authorities and explored the notification process in more depth. In these exercises, representatives from authoritative bodies, such as someone from the National CERT, are often included to enhance the realism of the notification process.

Most interviewees agreed that the new legislations will change exercises but only slightly. They believe that organizations that fall under the legislation will lead to supervising reporting to authorities more prominently in exercises. This also means the legislations might impact the organizations' processes and documentation. Some interviewees hoped that the legislations would also increase the amount of cyber exercises. A few interviewees noted that some exercises emphasize determining the significance of an incident, which is relatively ambiguously defined in the relevant legislations.

4.2 Step one: Impact assessment and forming the Incident Response Team

The first part of the decision-support framework of Kulikova et al. (2012) was to confirm the incident, make the impact assessment, and form the Incident

Response Team (IRT). Many interviewees shared a common understanding that prior to forming the IRT, standard IT incident handling procedures are typically followed. This process begins with either an end-user or IT staff reporting an event, followed by IT investigating the incident. Upon confirmation of the incident, it is then escalated. Interviewees also noted that the specifics of these procedures can vary depending on the organization's documented processes and the nature of the incident.

Interviews revealed that in cybersecurity exercises, incidents are usually confirmed before being escalated to the IRT based on the organization's process. While a few exercises begin at the initial discovery of an anomaly or suspicious event by an end-user or IT, most start after the incident has already been confirmed, at which point the Incident Response Team is convened. Two interviewees noted that participants sometimes delay recognizing an ongoing incident despite being aware they are part of an exercise focused on incident management. However, other interviewees mentioned that the exercise context often leads participants to acknowledge the incident and initiate the management process quickly.

> 'What is the possible impact, and do we have an incident or not?' (I2)

> 'An exercise is an abnormal situation because it is already known that it is a real incident.' (I6)

Most interviewees emphasized that the formation of the Incident Response Team depends on the organization's pre-defined roles and responsibilities as outlined in the documentation. The most frequently mentioned roles include Incident manager, Crisis manager, or Major Incident Manager, depending on the situation, along with someone from the Information Security team such as the CISO. Other key roles include someone responsible for IT, and the business owners, i.e., the area the incident affects, and someone from communications. A few interviewees also mentioned someone from legal or privacy although these were generally not considered essential to the IRT. Two interviewees mentioned external partners, e.g., IT software suppliers.

Additionally, there were mentions of an HR representative, risk management, and a customer representative. Several participants underscored the importance of an incident manager who facilitates communication between the incident management and technical teams. In larger public administration exercises, there can be incident managers for business, IT, cyber, and a crisis manager, and each of these managers gathers their group. As Kulikova et al. (2012) decision-support framework suggests, the structure of the IRT can vary based on organizational and impact-specific requirements. The decision-support framework mentions that the IRT should at least include someone from incident response management, privacy office, communications, senior management, and legal department.

> 'There must be people from higher up that have enough say in the organization.' (I4)

> 'It depends on the people's abilities and what roles have been pre-defined.' (I6)

When discussing potential issues in forming an Incident Response Team, two interviewees highlighted that the exercise setting could lead participants to form the team prematurely. However, most had not recognized this. On the other hand, various interviewees pointed out that the IRT was not formed due to either a lack of process or an inadequate one. Moreover, they also mentioned a lack of experience as a contributing factor, leading to people not understanding who should be a part of the IRT. Two interviewees suggested that a fear of disturbing higher-ups or a preference to resolve the incident independently could hinder the initiation of the process.

> '[talking about forming the IRT too early] In none of the exercises I have been to, has that ever happened.' (I2)

> 'I have to say that there have been very big differences in how long it takes to organize and get some ideas about who is in the core group and who the parties that need to be informed are. It is noticeable if there have been incidents, so they organize much faster.' (I3)

In conclusion, the effectiveness of the incident management process relies on well-documented procedures that outline the steps for incident escalation and the formation of the IRT. Cybersecurity exercises typically adhere to the decision-support framework that initiates by gathering information and assessing the impact, guiding the formation of the IRT. The specific processes involved can vary significantly depending on organizational practices.

Within this documentation, the precise definition of roles and responsibilities is crucial for identifying which people should form the team. These roles generally align with the suggestions made in the decision-support framework; however, there is often an inconsistency between the framework's suggestions and actual practice. For example, fewer participants incorporate a legal team member, and the inclusion of business-side representatives to evaluate the impact on operations is overlooked in the framework. Despite these inconsistencies, the decision-support framework serves as a guideline, emphasizing that the specific implementation depends on the organization's unique needs and the nature of the incident, as well as highlighting that specific specialists should invited in the second step while forming a better situational picture of the incident.

Additionally, the strength of the incident management process is significantly enhanced by the prior training and experience of the team members. Those who have engaged in training exercises or have real-life experience in managing incidents bring a practical understanding of how to form the IRT effectively.

4.3 Step Two: Figuring out if incident must be notified and prioritizing actions

The second part of the decision-support framework is determining whether the incident must be notified and to whom. This is supported by gathering more information about the incident: risks, impacts, incident discovery through a

questionnaire, and prioritizing the things necessary to the organization in the incident, such as reputation, restoring operations, minimizing customer impacts, and identifying root cause vulnerability.

Most interviewees expressed that participants initially lacked sufficient information about the incident when the team was formed. They pointed out that while organizations often have documentation that can aid in gathering information about the incident, assessing its impact, and guiding the incident management group, this documentation may be inadequate, forgotten by participants, or unused. Typically, participants begin to collect more detailed information about the incident through discussions and collaboration with stakeholders once the team is established. This information gathering can be further complicated by unclear roles, responsibilities, priorities, or outsourced IT. One interviewee highlighted that the organizational process can vary, with some having specific documents that include a checklist of questions essential for assessing the incident.

> 'Some organizations have had some sort of 'collect this information' type of forms. Which are very important, and they have then been better organized because they have been able to ask the right questions.' (I5)

There were numerous mentions of issues within the group, with communication problems emerging as the most significant concern. Many interviewees pointed out that the lack of communication or poor communication quality within the group or towards other stakeholders posed challenges. Some exercises involving the participants were conducted in multiple rooms, exacerbating communication issues by potentially preventing crucial information from reaching all relevant parties. Additionally, communication effectiveness can be compromised when IT services are outsourced.

> 'When starting the process, they might make assumptions. That I assumed that you would do this, and you assumed that I would do this which in practice leads to no one doing anything.' (I2)

> 'We had a big exercise… where the organizations were put into different rooms… When we had the end discussion, the crisis management group complained about not hearing anything from IT. And the IT complained about why the crisis management group never asked anything. So, both were quiet, and both wondered why nothing was heard. It is simple things like this that can make this thing fall apart.' (I6)

Some interviewees noted that participants sometimes overstep their responsibilities, inferring the duties of others. Most interviewees emphasized the importance of the incident, crisis, or major incident manager being experienced and capable of effectively managing the situation. The incident manager should direct the conversation to prioritize the primary goal of restoring operations to normalcy. The ambiguity of the roles and responsibilities can lead to individuals steering the group's actions toward their personal objectives or confusion regarding who is responsible for what. One interviewee noted that discussions often become overly technical, focusing too much on IT, which can alienate those not IT-oriented, further complicating the understanding of the situation.

> 'They just have not said things out loud. It feels like things are self-evident even though they are not, or people might understand things differently.' (I2)

> 'The closer the people working with the incident are to the [exercise] group, the more efficient the communication and integrity of the information.' (I4)

The second question of part two asked participants how the IRT decides when to notify the authority. Responses primarily centered on GDPR obligations, as many organizations are not subject to other reporting requirements like NIS. For those organizations that are, interviewees noted that recognizing the need for notification under NIS can be challenging and often depends on the expertise of specific individuals. In contrast, the need for GDPR-related data breach notifications is generally more recognized. For example, in the public administration sector, responders are trained to identify when a GDPR notification is necessary; however, there is no formalized process for reporting broader cyber incidents because it has not been needed.

> 'And I think the GDPR is somehow stuck in people's lizard brains, that what were the twenty-four hours, seventy-two hours. And then there are sanctions for what happens if you do not do this.' (I3)

> '[talking about public administration exercises] That then if there were a cyber incident, then there is no such path. There has been no reason for it to exist. It has not been taught. There is no process. There is a process for this data breach.' (I1)

> '[talking about GDPR] Yes, and there is a bit of a fear that it could lead to sanctions and all sorts of things if it is not dealt with in time.' (I7)

Four interviewees highlighted a general lack of a reporting culture within organizations, with the decision to notify authorities often arising from internal discussions. Typically, this process involves consulting with the privacy officer or a legal team member who recognizes the need for actions such as a data breach notification. In these instances, the communications personnel are also frequently involved in crafting the notification. In public administration exercises, trained individuals usually deliberate on these matters within their teams. A few interviewees noted that the criticality of the sector also plays a significant role, as those operating in more critical sectors tend to grasp better the importance of notifying authorities with, for example, the NIS legislation. Moreover, a few responses suggested that the notification procedures should ideally be documented to guide the IRT's actions.

> 'But even if there are no guidelines, there is usually someone at the exercise who at some point will raise the point that, hey, should we make these notifications? So, it is someone's job description in some way or another. For example, on the legal side, someone will take it into account based on their professional skills.' (I7)

Kulikova et al. (2012) decision-support framework prioritization is related to the organization to determine its incident disclosure priorities, focusing on harm mitigation, regulatory compliance, cost-efficiency, and reputation. When

interviewed, all respondents agreed that the most critical objective is to restore operations to normal. Five interviewees pointed out that organizations make required notifications when necessary but generally assign a lower priority to this task since it is more important to restore the operations. Additionally, some interviewees noted that the authority's response can impact the notification process. If the notification is perceived merely as an additional burden without benefitting the organization, there tends to be a greater reluctance to report it immediately.

> 'Problem-solving. That is their focus. They focus on what they see in front of them. Regulatory notifications, if you do not consider GDPR, it does not contribute to the problem-solving in any way.' (I4)

> '[talking about GDPR data breach notification] At this point we would inform authorities. But of course, restoring the critical function of society has been the main point of the exercise, that is where what we have been focusing on.' (I5)

The key to a successful IRT can be traced back to the challenges identified: establishing clear communication pathways and having clearly defined roles and responsibilities. However, the interviewees also highlighted a crucial factor: the experience level of the participants significantly enhances incident management. Furthermore, two interviewees emphasized the importance of team chemistry and whether the participants know each other. It is vital that no one dominates the discussions and that all members consider and listen to each other's opinions, fostering a collaborative environment.

> 'It usually is apparent if they have exercised in the past or if they have encountered a real incident. Either way, the IRT usually works very efficiently and can solve the problem immediately.' (I5)

> '[talking about incident management] But this is largely about the group's decision-making and communication, successful communication.' (I4)

In conclusion, the decision-support framework underscores the importance of documentation in determining whether incidents should be reported to authorities. It suggests that organizations employ an 'Incident Specific Questionnaire' to aid in making these determinations. However, during exercises, the necessary documentation that could facilitate information gathering about the incident is often lacking, underutilized, or found to be inadequate. Proper documentation not only aids in decision-making but also clarifies responsibilities for IRT members, guiding them in gathering the essential information needed for notifications.

Experience and expertise also play critical roles. A seasoned incident manager can effectively steer discussions toward critical issues, while experienced legal counsel is crucial for gathering information influencing the decision to report an incident.

The prioritization in the decision-support framework often takes a backseat during exercises, primarily because the immediate goal is to restore operations. The situation's urgency frequently leads to ambiguities in understanding what

should be prioritized. Regarding the notification of authorities, this task is often deemed a low priority in most exercises. The focus tends to remain on restoring normal operations, as notifying authorities is perceived to offer little benefit to the organizations.

4.4 Step three: Incident disclosure strategy mapping

The third part of the decision-support framework involves creating a strategy for incident disclosure mapping. This includes finding possible notification templates, deciding on the disclosure strategy, and possibly updating the incident details later. The primary concern raised by interviewees is that many organizations do not have established documentation or processes for notifying authorities about incidents. In addition, the situation's urgency might present a challenge in deciding whether to report the incident. Most interviewees have noted that organizations often lack specific templates for notifying authorities. Some participants said there is no need for a template because the authorities often have a web form for notifications. Four interviewees mentioned that in some exercises, participants have utilized existing communication plans or other documentation related to customers or internal organization. However, one interviewee pointed out that this repurposed documentation is often outdated, which has resulted in the lack of use of it. Two interviewees noted that larger organizations are often better prepared because they have more resources at their disposal. Furthermore, one participant highlighted that complications could arise when outsourced IT providers fail to deliver critical information needed for effective communication with authorities.

> '[asking whether organizations have had any templates for notifying authorities] Yeah, so no… Sure, there may be an old cobweb-filled excel somewhere with some text about ransomware and some numbers on the back, but I have never seen an exercise where anyone ever took it out and started deciphering it. It is pretty much living in the moment, and being in the moment, like okay, what is this all about and then make decisions based on it.' (I4)

> 'That I would say that perhaps rather than templates, rather instructions that explain where to notify and what to notify.' (I7)

> 'And then sometimes they were so badly out of date that they could no longer be used.' (I6)

> 'The bigger the organization, the better they tend to have all the templates created and prepared because they have the resources to do it.' (I7)

> 'And similarly, if there is no administrative thought that we will get this kind of information, it is quite a common observation in exercises that the information would not even be technically available. For example, a log from 4 days ago is needed. So, the logs really only last twenty-four hours. So, the operations do not support them.' (I5)

> 'There may be templates for forming the situational picture, yes, but there are no templates for reporting to the authorities.' (I1)

Many interviewees observed that in numerous exercises, the exercise does not focus on what specific information should be reported to the authorities. Typically, it is merely mentioned that participants would notify the authorities without a thorough discussion of the report's contents. Most interviewees noted that in scenarios where the report's content is discussed, substantial information is available about the incident, often including details about the impact, business context, affected systems, and potential threats. The issue with notifying is exacerbated by the fact that many participants, inexperienced in incident management, are often unsure about the necessary details to report or the information required for notifications. Three interviewees mentioned that in some exercises, participants notified the authorities quite early before having a complete understanding, leading them to define it more accurately later. One interviewee suggested that this approach might vary depending on the organizational culture.

> 'Well, yes, in the situations I have been in, they have made the notification when they have quite good information about what has happened. Nevertheless, of course, I do not know if it relates to the game somehow because of the virtual time.' (I2)

> 'Not all exercises have even gone to the level of even considering whether we have all the necessary information or what are we even reporting other than just reporting.' (I3)

Interviewees did not recognize any need to create a plan to update information to authorities. This is primarily because incident reporting is viewed as a minor component of overall incident management. However, one participant mentioned that updating authorities has been incorporated and carried out consistently throughout the exercise day in some public administration exercises.

In conclusion, most organizations lack specific templates for reporting incidents to authorities, often due to low priority. Additionally, while GDPR mandates notification, exercises frequently skim the surface of what specific information needs to be reported, focusing merely on the act of notifying itself. The decision-support framework proposes the creation of a knowledge base where such templates could be stored and easily accessed as needed. In cybersecurity exercises, organizations might repurpose existing templates from other domains for these notifications. This might depend on the organization's size since larger organizations have better resources.

Furthermore, the decision-support framework emphasizes the changes in incident information, suggesting that the status of an incident may evolve and thus should be regularly updated. This requires a mechanism for receiving continuous updates to adjust the response strategy. However, in most cybersecurity exercises, notifications are typically issued once sufficient information about the incident has been gathered, potentially overlooking the importance of ongoing updates.

4.5 Summary of results

The data gathered considered primarily the first two research questions: **Do organizations practices align with the decision-support framework in reporting cyber incidents to authorities? How do these practices fail or succeed?** Figure 3 illustrates the challenges and success factors in practices. The third research question is further explored in the Discussion Chapter.

Step one of the decision-support framework involves confirming the incident, assessing its impact, and forming the IRT. Exercises adhere to the organization's protocols for confirming the incident, escalating it, and forming the IRT, but the specifics may vary based on the organization's own processes or the incident nature. The interviewers highlighted that pre-defined roles and responsibilities are essential to include in the organization's documentation, as their absence can prevent the formation of the IRT. The interviewees noted that the lack of documentation and processes are not the only issues with forming the IRT; participants' experience can also impact this process. This can lead to participants not understanding who should be involved in the IRT at that stage. While the decision-support framework suggests including a legal team member in the IRT, this often does not happen in practice. On the other hand, the decision-support framework does not mention including business side representatives, but they are present in exercises.

The decision-support frameworks step two involves filling in the 'Incident Specifics Questionnaire' to assess the details of the incident. It emphasizes that the questions depend on the organization in question. In exercises, the documentation is often inadequate, or unused which can be due to participants forgetting its existence. Typically, information is gathered through discussion within the group and relevant stakeholders.

The information gathering can be complicated by unclear roles and responsibilities, priorities, and communication challenges. These issues can lead participants to steer the conversations towards their own goals instead of focusing on the primary objective of restoring operations. To combat the issues of communication and unclear roles, the factor of experience comes into play. The more experienced the incident manager, the better they can direct the conversation and guide the participants towards common goals. This is further enhanced when participants also have experience, as it reduces the need for the incident manager to handle the whole situation alone.

The prioritization in exercises, as mentioned above, often focuses on restoring operations. Notifying the incident is often assigned a lower priority as the immediate goal is to restore operations. Making notifications is also not seen as benefiting the company in any way, thus it is given less priority.

The third step of the decision-support framework involves conducting the disclosure by having the notification template ready, having a disclosure strategy, and receiving updates of information relating to the incident. The data suggests that organizations often do not have templates ready for notification. Some organizations might repurpose other templates for this purpose. Often, larger organizations with more resources are better prepared with templates. There might

also be issues with the templates not being up to date. This is further complicated by experience; participants often do not know what information must be notified.

Typically in exercises, the notification to authorities is not considered beyond the fact that it has to be made. Often, when the notification is made, there is a considerable amount of information available about the incident. The status of the update is also not considered, as it is assumed that one notification is sufficient.

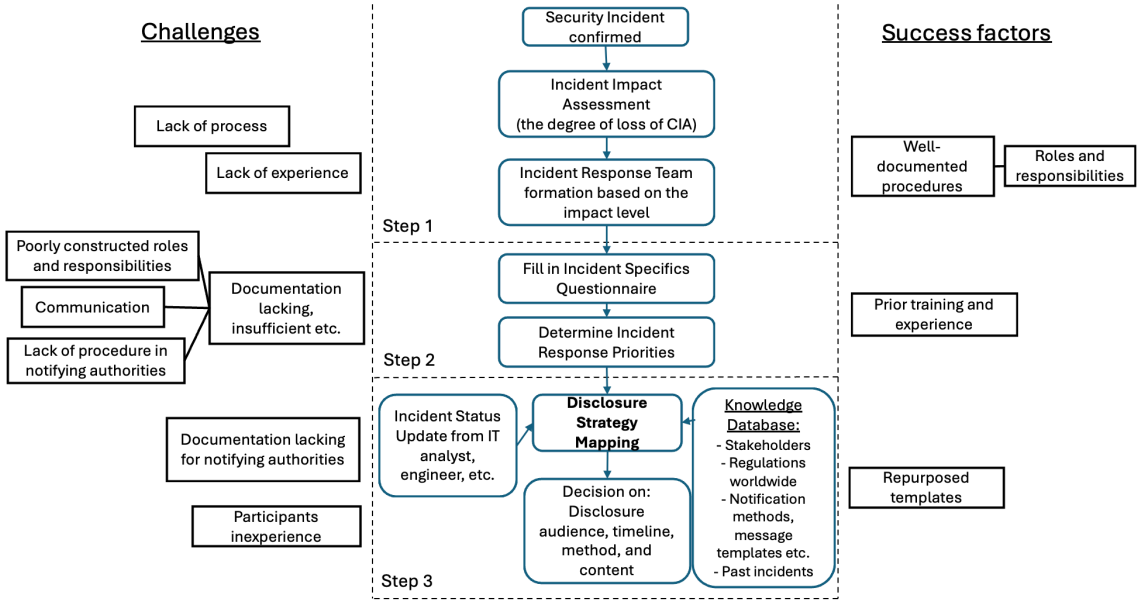

FIGURE 3 Challenges and success factors with practices and the decision-support framework modified from Kulikova et al. 2012

In essence, organizational practices partially align with Kulikova et al. (2012) decision-support framework, but there are notable differences. Practices often follow step one of the framework. However, as the framework indicates, there are differences based on the organization's processes and the nature of the incident.

In contrast, step two and step three are where discrepancies are observed. Organizations often lack proper documentation, or participants fail to utilize it to determine the specifics of the incident. Prioritization is also overlooked, as the primary goal is typically to restore operations. Step three reveals gaps in preparedness: many organizations do not have ready-made templates for notifications, or the templates they use are outdated or not intended for notifying authorities. Notifications are made once sufficient information about the incident is available, leading to a perception that further status updates are unnecessary. The success factors and challenges revolve around two primary areas: documentation and processes, and training or experience. The more effectively these elements are managed, the better organized and more efficient the operations of the IRT will be.

5 Discussion

Effective security measures are essential for managing incidents and reporting them to authorities. Initially, organizations should implement security measures such as risk assessments, regular audits, employee training, and strong cybersecurity policies. These steps are aimed at preventing incidents and reducing vulnerabilities. However, when an incident does occur, having a clear incident management process is crucial. This process includes quickly identifying and assessing the incident's impact, then moving rapidly to contain and mitigate the damage. The IRT, with clear roles and responsibilities, takes the lead in managing the situation. Good communication within the team and with external stakeholders is key to a coordinated response. Finally, reporting the incident to authorities is a critical step, especially with new legislations that require timely and specific disclosures. Organizations need to have set protocols to gather the necessary information and communicate it to the authorities efficiently, ensuring they meet legal requirements. The implementation of these new legislations will enable national authorities and the EU to collect more data on current cyberattacks, their impact, and the broader threat landscape. This information will enable organizations to enhance their risk assessments and possibly their incident management.

With the recent legislation, NIS2, CER and DORA, new obligations on reporting incidents to authorities is more essential than before. This thesis aimed at finding out whether the organizations practices align with Kulikova et al. (2012) decision-support framework, how the practices fail or succeed and whether the legislations warrant adaptions to the decision-support framework. The data collected in this thesis suggests that the decision-support framework could serve as a foundation for incident reporting to authorities. However, the specifics may vary based on each organization's unique processes and circumstances. The decision-support framework's first step involves an initial impact assessment, followed by escalating the incident management process, which ultimately leads to forming the IRT. According to research organizations should have a well-defined process for escalation that includes notifying the authorities (Cichonski et al., 2012; Grey et al., 2020). Earlier research states that clearly outlining roles and responsibilities for those involved in incident management is crucial (Aoyama et al., 2017; Bartnes et al., 2016; Ilkka et al., 2017; Khurana et al., 2009; Staddon & Easterday, 2019).

While many organizations have incident management procedures documented, participants often lack clarity on identifying incidents or understanding who should be included in the IRT. The Kulikova et al. (2012) decision-support framework's initial impact assessment relies on the CIA model. Organizations should swiftly measure the incident's impact to convene the relevant stakeholders as the IRT (Kulikova et al., 2012), but this often doesn’t happen in practice. Participants may sense that the incident has substantial impact but lack certainty about its severity. This leads to a simplified understanding of the situation. Thus, the decision-support framework creates a too simplistic picture of the situation. Though the initial IRT is formed, additional stakeholders might still be needed once more information is available.

Even the initial incident management team should be diverse. Research suggests it should comprise relevant stakeholders from across the organization to ensure effective incident management (Bartnes et al., 2016; Staddon & Easterday, 2019). The decision-support by Kulikova et al. (2012) framework touches on roles very lightly. It mentions that the IRT should be cross-functional and include at least someone from the incident response management team, privacy office, senior management, legal, and communications. The members and their responsibilities should be defined in more detail. Clearly defined roles and responsibilities guide the IRT's actions. It is crucial to involve relevant stakeholders or at least have a knowledgeable person leading the response, like an incident manager familiar with who to contact in different situations (Hove, et al., 2014; Luttgens et al., 2014). Clear roles also help participants and the incident manager identify necessary information for mandatory reporting.

Communication, both within the team and with external stakeholders, should follow a clear path to ensure appropriate messaging (Ilkka et al., 2017). Poor communication can adversely affect decision-making (Aoyama et al., 2015). The data gathered suggests that the decision on whether to report the incident needs input from legal. Many organizations do not include a member of the legal team in their IRT, but this should be considered again, since the legislations requires an incident to be reported. Although, it might not require a person from the legal team to be in the IRT but there needs to be a clear communication path to consult with the legal team.

Clear roles also prevent IRT members from pursuing personal goals during an incident response, emphasizing prioritization. The Kulikova et al. (2012) decision-support framework not only concerns notifying authorities but also other disclosures. However, considering the legal obligations of NIS2, CER and DORA, the prioritization step in the decision-support framework is not valid when considering reporting incidents to authorities. The second step should be based solely on the impact assessment and recognizing whether the incident is significant, i.e. the law mandates the notification, and if it considered a major ICT incident, significant disruption or a significant incident, the organization is required by law to make the notification. Most organizations prioritize restoring operations, often placing lower importance on notifications. With mandatory notification, organizations must shift focus based on impact assessment to comply with legal requirements. The IRT must have clear guidelines on reporting, with policies covering legal standards or official guidelines from authorities.

The third step of the decision-support framework by Kulikova et al. (2012) points to a key issue: knowing what information to report is often overlooked. Data collection may be hindered by outsourced IT or the lack of templates, with participants not understanding what data is necessary. Organizations must document what to report and when. This is linked to the impact assessment step. They should have detailed guidelines that align with official regulations once they are published.

The decision-support framework also emphasizes the incidents status changes and adjusting the disclosure strategy accordingly. NIS2 and DORA, require an intermediate report if there is a relevant status update or the National CSIRT requires it. Clear responsibilities must be established for providing this

information, along with a transparent communication pathway with relevant stakeholders.

Additionally, technical preparation presents another challenge, especially as new legislation mandates organizations to report specific details, such as the root cause of the incident. Consequently, every part of the service chain must be able to provide necessary information promptly and accurately. This ensures that organizations are not only compliant with new regulations but also prepared to handle the complexities of incident reporting.

Research shows that training and experience are crucial for the incident reporting process, as many organizations struggle due to a lack of awareness or recognition of existing processes (Hove, et al., 2014; Kapoor et al., 2018a; Line et al., 2014). Experience also addresses communication, roles, and responsibilities. With experience the participants are aware of the whole incident management process. This can guarantee that the members of the IRT know who should be contacted or present, which information they need for the notification, and when each notification must be sent. Participants highlighted that real-life incidents and training significantly enhance their response capabilities. Cybersecurity exercises, in particular, were cited as a valuable training form (Jones, 2020; National Institute of Standards and Technology, 2020a; Schreider, 2019).

The decision-makers in the IRT must be knowledgeable about legal requirements. Several studies underscore the absence of individuals familiar with incident management processes (Kapoor et al., 2018a; Line et al., 2014; Nyman et al., 2019). If smaller organizations are lacking dedicated legal expertise, the entire IRT should be aware of their obligations. The Kulikova et al. (2012) decision-support frameworks suggests a knowledge base for incident disclosures, but in the heat of a crisis, participants often feel a sense of urgency and might not have the time or patience to search for templates or documents. This issue can be mitigated by relying on knowledgeable individuals who can either recall the necessary information or direct others to where templates and documents are located to facilitate the notification process.

While the decision-support framework by Kulikova et al. (2012) provides guidance for post-incident learning through reports, this aspect was not included in the gathered data as it was beyond the scope of the thesis. Nevertheless, the framework encourages organizations to adapt their post-incident disclosure strategies based on these insights. However, it doesn't fully consider the value of IRT members' actions and input throughout the process. This comes down to the reality of the incident. Documents and processes can be very high quality, but they will not work if the people following them are not aware of them or follow them in a real crisis. The effectiveness of documents and processes depends on team members being both aware of and capable of following them during a real crisis. The data indicates that learning should encompass the entire incident management process, not just disclosure strategies, to ensure that incident notification is effective and comprehensive.

In conclusion, NIS2, CER and DORA legislations make timely and accurate incident reporting to authorities more crucial than ever. This thesis's findings reveal that while the Kulikova et al. (2012) decision-support framework provides a structured approach, its effectiveness is dependent on each organization's unique

processes and context. The decision-support framework encompasses steps from initial impact assessment to the formation of the IRT, with a focus on escalation procedures that include mandatory notifications to the authorities. Yet, many organizations struggle with practical application, often lacking clarity in defining roles, responsibilities, and understanding the severity of incidents.

This study has shown that effective incident management requires not only a theoretical framework but also practical readiness, such as having knowledgeable personnel, clear communication channels, and appropriate technical preparation to meet legal standards. Organizations must prioritize training and experience to enhance their incident management capabilities, ensuring that the IRT members are proficient and prepared to handle the complexities of incident reporting. Ultimately, while the decision-support framework by Kulikova et al. (2012) serves as a foundational guide, the true test of its efficacy depends on those who implement it during real-life crises, underscoring the importance of comprehensive training and a thorough understanding of legal and operational requirements for successful incident disclosure and management.

5.1 Limitations and implications for future research and practice

The thesis offers important insights into reporting incidents to authorities and the implications of recent legislation such as NIS2, CER, and DORA. However, there are limitations to consider. Firstly, the data was primarily gathered from cybersecurity exercises, which, while designed to mimic real-life scenarios, do not fully replicate the complexities of actual cyber incidents. This difference suggests that while the exercises provide a framework for understanding incident management, they may not completely capture the nuances of real-life events. Additionally, it is important to note that the study was based on interviews with a relatively small number of participants, specifically seven cybersecurity experts. Future research could use a larger sample size and delve into incident management in actual situations, and possibly explore the variance between simulated exercises and genuine cyber incidents, potentially yielding more comprehensive insights.

Secondly, although the current legislation is in force, specific guidelines from the authorities are still unpublished. This gap may lead to nuances between existing legislation and future guidelines. Future studies should also monitor these developments to evaluate their impact on the effectiveness of incident reporting and management practices.

Furthermore, the topic of incident reporting to authorities has gained even greater significance in the field of cybersecurity with the introduction of new legislation. The data that the EU will collect from these cyber incidents will enhance the understanding of the current threat landscape and the overall state of cybersecurity within the EU. Future research could investigate whether there are benefits to individual organizations from reporting incidents to authorities or what are the broader benefits to the EU.

This study highlights two main areas with significant implications for practice. First, it is crucial for critical entities and other organizations within the scope of these legislations to develop an incident management process or guidelines that incorporate the aspect of incident notification. This approach ensures that reporting procedures are integrated seamlessly into broader incident management strategies.

Second, the study underscores the importance of training and thereby enhances the validity of incorporating detailed incident reporting training within cybersecurity exercises. By doing so, organizations can strengthen their preparedness and ensure that their teams are well-equipped to handle and report incidents effectively and in accordance with legislative requirements.

6 Conclusion

The EU aims to strengthen the overall cybersecurity of Member States by introducing legislation that mandates various cybersecurity measures for organizations, including NIS2, CER, and DORA. One key requirement of these measures is the reporting of incidents to authorities. Through these notifications, the EU can collect more data on the cybersecurity landscape, such as threats, impacts, and adversaries. However, as the EU introduces these new reporting requirements, there are no guidelines for applying the changes brought about by the legislation. Existing frameworks and guidelines that organizations can use in reporting incidents to authorities may not fully meet the new legislative requirements, have not been tested in practice, or are too concise compared to the detailed obligations of the legislation.

Therefore, this thesis was conducted to determine whether the decision-support framework by Kulikova et al. (2012) for disclosing security incidents aligns with practice, the pitfalls and success factors, and how the new legislations might change the decision-support framework. The research questions were: **Do organizations practices align with the decision-support framework in reporting cyber incidents to authorities? How do these practices fail or succeed? Do the legislations, NIS2, CER, and DORA, warrant adaptations to the decision-support framework in reporting incidents to authorities?**

To understand whether the Kulikova et al. (2012) decision-support framework in question would be effective and to comprehend the effects of the legislation, a literature review was first conducted into existing research on reporting incidents to authorities and the legislations. After gaining an understanding of the current phenomena, data was gathered from interviews with cybersecurity experts who have observed cybersecurity exercises. The exercises simulate real-life cyber incidents to review, test, or validate the incident management process or documents. The data was then analyzed by conducting deductive coding.

The results indicated that the decision-support framework by Kulikova et al. (2012) can serve as a baseline, but the specifics may vary by the incident in question and the organization's own processes. The most crucial elements are clear roles and responsibilities, a diverse team, clear communication paths, and knowledgeable individuals. The importance of knowledgeable individuals is also related to another key finding: the importance of training and experience is highlighted. The actions of the incident management team depend heavily on their prior training and experience and can affect the whole incident management process. Thus, as the legislation introduces more comprehensive requirements for organizations, it is essential that the individuals in the core incident group are well-prepared not only with overall incident management but also with a thorough understanding of the incident reporting requirements.

This thesis provides valuable insights for both research and practice. However, there are some limitations to consider. The primary limitations are that the data was collected from only seven individuals, and it was not derived from real-life incidents. Additionally, specific guidelines from national authorities have not yet been published, which may influence reporting practices. Future research

should explore data from a larger sample size and from real-life cyber incidents. In practice, the results highlight that incident management should implement the new obligations into the process through documentation and processes and ensure that individuals involved in this process are trained.

REFERENCES

Aaltola, K., & Taitto, P. (2019). Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training. *Information & Security*, *43*(1), 123–133. https://doi.org/10.11610/isij.4311

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Anderson, R. (2020). *Security Engineering* (Vol. 3). Wiley. https://www.cl.cam.ac.uk/~rja14/Papers/SEv3-ch2-7sep.pdf

Andreasson, A., & Fallen, N. (2018). External Cybersecurity Incident Reporting for Resilience. In J. Zdravkovic, J. Grabis, S. Nurcan, & J. Stirna (Eds.), *Perspectives in Business Informatics Research* (pp. 3–17). Springer International Publishing. https://doi.org/10.1007/978-3-319-99951-7_1

Angafor, G., Yevseyeva, I., & He, Y. (2020a). Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis. *Joint Conference on Serious Games 2020*. https://doi.org/10.1007/978-3-030-61814-8_10

Angafor, G., Yevseyeva, I., & He, Y. (2020b). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *SECURITY AND PRIVACY*, *3*(6), e126. https://doi.org/10.1002/spy2.126

Angafor, G., Yevseyeva, I., & Maglaras, L. (2023). Scenario-based incident response training: Lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, *31*(4), 404–426. https://doi.org/10.1108/ICS-05-2022-0085

Anson, S. (2020). *Applied Incident Response*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=6017672

Aoyama, T., Nakano, T., Koshijima, I., Hashimoto, Y., & Watanabe, K. (2017). On the Complexity of Cybersecurity Exercises Proportional to Preparedness. *Journal of Disaster Research*, *12*(5), 1081–1090. https://doi.org/10.20965/jdr.2017.p1081

Aoyama, T., Naruoka, H., Koshijima, I., & Watanabe, K. (2015). How Management Goes Wrong? – The Human Factor Lessons Learned from a Cyber Incident Handling Exercise. *Procedia Manufacturing*, *3*, 1082–1087. https://doi.org/10.1016/j.promfg.2015.07.178

Bartnes Line, M., Anne Tøndel, I., & Jaatun, M. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations.

International Journal of Critical Infrastructure Protection, *12*, 12–26. https://doi.org/10.1016/j.ijcip.2015.12.003

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, 32–45. https://doi.org/10.1016/j.cose.2016.05.004

Benfield, K. (2023, September 26). Keeper Security Releases Cybersecurity Disasters Survey: Incident Reporting & Disclosure. *PR Newswire*. https://www.proquest.com/docview/2868559513/citation/BF401C182EDC402BPQ/1

Bingham, A. J. (2023). From Data Management to Actionable Findings: A Five-Phase Process of Qualitative Data Analysis. *International Journal of Qualitative Methods*, *22*, 16094069231183620. https://doi.org/10.1177/16094069231183620

Brajdic, I., Kovacevic, I., & Gros, S. (2021). *Review of National and International Cybersecurity Exercises conducted in 2019*. Academic Conferences Limited.

Brewster, E., Griffiths, R., Lawes, A., & Sansbury, J. (2012). *IT Service Management: A Guide for ITIL Foundation Exam Candidates*. BCS, The Chartered Institute for IT.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review*, *4*(1), 79–90. https://doi.org/10.1365/s43439-022-00076-5

Council Directive 2022/2555 issued on the 14th of December 2022, Network and Information Security 2

Council Directive 2022/2557 issued on the 14th of December 2022, Resilience of Critical Entities

Council Regulation 2022/2554 issued on the 14th of December 2022, Digital Operational Resilience for Financial Sector

Cusick, J., & Ma, G. (2010). Creating an ITIL Inspired Incident Management Approach: Roots, Responses, and Results. *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. https://doi.org/10.1109/NOMSW.2010.5486589

DarkReading. (n.d.). *Sandworm Cyberattackers Down Ukrainian Power Grid During Missile Strikes*. Retrieved January 21, 2024, from https://www.darkreading.com/ics-ot-security/sandworm-cyberattackers-ukrainian-power-grid-missile-strikes

Dewar, R. S. (2018). Cybersecurity and Cyberdefense Exercises. In *CSS Cyberdefense Reports* [Report]. ETH Zurich. https://doi.org/10.3929/ethz-b-000314593

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, EP, CONSIL, 194 OJ L (2016). http://data.europa.eu/eli/dir/2016/1148/oj/eng

Eiopa. (n.d.). *Digital Operational Resilience Act (DORA) – European Union*. Retrieved January 16, 2024, from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

ENISA. (2023). *Incident reporting*. CIRAS. https://ciras.enisa.europa.eu/ciras-consolidated-reporting

Eriksson, P., & Koistinen, K. (2014). *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus. https://helda.helsinki.fi/items/db985ead-f6d1-4537-a432-4267f321a5c5

Eriksson, P., & Kovalainen, A. (2008). *Qualitative Methods in Business Research*. SAGE Publications Ltd. https://doi.org/10.4135/9780857028044

European Banking Authority. (2021). *Revised Guidelines on major incident reporting under PSD2 | European Banking Authority*. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20major%20incident%20reporting%20under%20PSD2%20EBA-GL-2021-03/1014562/Final%20revised%20Guidelines%20on%20major%20incident%20reporting%20under%20PSD2.pdf

European Commission. (n.d.). *Critical infrastructure resilience – European Commission*. Retrieved January 16, 2024, from https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en

European Commission. (2023a, June 29). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

European Commission. (2023b, December 18). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Parliament. (2021a, April 22). *Shaping the digital transformation: EU strategy explained*. Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained

European Parliament. (2021b, October 12). *Cybersecurity: Why reducing the cost of cyberattacks matters*. Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters

European Union. (2022a). *European Union directives | EUR-Lex*. https://eur-lex.europa.eu/EN/legal-content/summary/european-union-directives.html

European Union. (2022b). *European Union regulations | EUR-Lex*. https://eur-lex.europa.eu/EN/legal-content/summary/european-union-regulations.html

Europen Parliament. (2022, November 10). *Fighting cybercrime: New EU cybersecurity laws explained*. Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained

Evesti, A., Kanstren, T., & Frantti, T. (2017). Cybersecurity situational awareness taxonomy. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. https://doi.org/10.1109/CyberSA.2017.8073386

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access*, *10*, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Freeze, D. (2023, October 12). Cybercrime To Cost The World $9.5 trillion USD annually in 2024. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Furtună, A., Patriciu, V.-V., & Bica, I. (2010). A structured approach for implementing cyber security exercises. *2010 8th International Conference on Communications*, 415–418. https://doi.org/10.1109/ICCOMM.2010.5509123

Georg-Schaffner, L., & Prinz, E. (2022). Corporate management boards' information security orientation: An analysis of cybersecurity incidents in DAX 30 companies. *Journal of Management and Governance*, *26*(4), 1375–1408. https://doi.org/10.1007/s10997-021-09588-4

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). *Guide to test, training, and exercise programs for IT plans and capabilities* (NIST SP 800-84; 0 ed., p. NIST SP 800-84). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-84

Grey, O., & Brown, R. (2020). GDPR Compliance: Incident Response and Breach Notification Challenges. In *Cyber Security Practitioner's Guide* (pp. 275–302). https://doi.org/10.1142/9789811204463_0008

Gurnani, R., Pandey, K., & Rai, S. K. (2014). A scalable model for implementing Cyber Security Exercises. *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, 680–684. https://doi.org/10.1109/IndiaCom.2014.6828048

Hautamaki, J., Karjalainen, M., Hakkinen, P., & Hamalainen, T. (2019). CYBER SECURITY EXERCISE – LITERATURE REVIEW TO PEDAGOGICAL METHODOLOGY. *13th International Technology, Education and Development Conference*, 3893–3898. https://doi.org/10.21125/inted.2019.0985

Hirsjärvi, S., & Hurme, H. (2009). *Tutkimushaastattelu – Teemahaastattelun teoria ja käytäntö*. Gaudeamus Helsinki University Press.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2009). *Tutki ja kirjoita* (Vol. 15). Kariston Kirjapaino Oy.

Hove, C., Tårnes, M., Line, M. B., & Bernsmed, K. (2014). Information Security Incident Management: Identified Practice in Large Organizations. *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, 27–46. https://doi.org/10.1109/IMF.2014.9

Hove, C., Tarnes, M., Line, M. B., & Bernsmed, K. (2014). Information Security Incident Management: Identified Practice in Large Organizations. *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, 27–46. https://doi.org/10.1109/IMF.2014.9

Ilkka, J., Sahlman, A., Mäntylä, H., Hartikainen, J., Janhunen, K., Grönroos, K., Raappana, M., Kinnunen, P., Heikkinen, P., Niinikorpi, S., Lehtinen, T., Törmälä, J., & Pajunen, K. (2017, February 14). *Tietoturvapoikkeamatilanteiden hallinta* [Sarjajulkaisu]. Valtiovarainministeriö. https://julkaisut.valtioneuvosto.fi/handle/10024/79258

Institute for Security and Technology, & Cyber Threat Alliance. (2023). *Cyber Incident Reporting Framework: Global Edition*. Institute for Security and Technology, Cyber Threat Alliance. https://www.cyberthreatalliance.org/wp-content/uploads/2023/04/Cyber-Incident-Reporting-Framework-Global-Edition.pdf

John R. Vacca. (2013). *Computer and Information Security Handbook: Vol. 2nd ed*. Morgan Kaufmann. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=485997&site=ehost-live

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 ed., p. NIST SP 800-30r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Jones, E. (2020). The GDPR Two Years on. *Antitrust*, *35*, 51.

Juhila, K. (n.d.). *Koodaaminen*. Tietoarkisto. Retrieved May 1, 2024, from https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/koodaaminen/

Kapoor, K., Renaud, K., & Archibald, J. (2018a). Preparing for GDPR: 2018 AISB Convention: Symposium on Digital Behaviour Intervention for Cyber Security. *Symposium on Digital Behaviour Interventions for Cyber-Security*, 13–20.

Kapoor, K., Renaud, K., & Archibald, J. (2018b). Preparing for GDPR: Helping EU SMEs to Manage Data Breaches. *Symposium on Digital Behaviour Interventions for Cyber-Security*.

Karjalainen, M., & Kokkonen, T. (2020). Review of pedagogical principles of cyber security exercises. *Advances in Science, Technology and Engineering Systems Journal*, *5*, 592–600.

Karyda, M., & Mitrou, L. (2016). Data Breach Notification: Issues and Challenges for Security Management. *MCIS 2016*. https://aisel.aisnet.org/mcis2016/60/

Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., & Butler, R. (2009). Palantir: A framework for collaborative incident response and investigation. *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, 38–51. https://doi.org/10.1145/1527017.1527023

Kick, J. (2014). *Cyber Exercise Playbook*. https://www.mitre.org/news-insights/publication/cyber-exercise-playbook

Kulikova, O., Heil, R., Van Den Berg, J., & Pieters, W. (2012). Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information. *2012 International Conference on Cyber Security*, 103–112. https://doi.org/10.1109/CyberSecurity.2012.20

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2014). Information Security Incident Management: Planning for Failure. *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, 47–61. https://doi.org/10.1109/IMF.2014.10

Linneberg, M., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal*. https://doi.org/10.1108/QRJ-12-2018-0012

Luiijf, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, *35*, 100471. https://doi.org/10.1016/j.ijcip.2021.100471

Luttgens, J., Pepe, M., & Mandia, K. (2014). *Incident response and computer forensics* (Vol. 3rd). McGraw Hill.

Maniati, A., & Tringali, S. (2019). *EBF position on Cyber incident reporting*. https://www.ebf.eu/innovation-cybersecurity/ebf-position-on-cyber-incident-reporting/

Mäses, S., Maennel, K., Toussaint, M., & Rosa, V. (2021). Success Factors for Designing a Cybersecurity Exercise on the Example of Incident Response. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 259–268. https://doi.org/10.1109/EuroSPW54576.2021.00033

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Myers, M. (2009). *Qualitative Research in Business & Management* (Vol. 3rd). SAGE.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2020a). *NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0* (NIST CSWP 01162020; p. NIST CSWP 01162020). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01162020

National Institute of Standards and Technology. (2020b). *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Nyman, M., & Große, C. (2019). Are You Ready When It Counts? IT Consulting Firm's Information Security Incident Management. *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 26–37. https://doi.org/10.5220/0007247500260037

Ogee, A., Gavrila, R., Trimintzios, P., Stravolopoulos, V., & Zacharis, A. (2015). *The 2015 Report on National and International Cyber Security Exercises*. ENISA. https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

Ouzounis, E., Trimintzios, P., & Saragiotis, P. (2009). *National Exercise – Good Practice Guide* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

Pallagi, A., Peto, R., & Hronyecz, E. (2023). Increasing the Resilience of Critical Infrastructures with Defense Zone System. *2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, 000549–000554. https://doi.org/10.1109/SISY60376.2023.10417949

Pöyhönen, J., Nuojua, V., Lehto, M., & Rajamäki, J. (2019). *Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations* [Publication]. 19416; Procon. http://www.theseus.fi/handle/10024/263082

Pursiainen, C., & Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: What does it mean? *Sustainable and Resilient Infrastructure*, *8*(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562

Saaranen-Kauppinen, A., & Puusniekka, A. (n.d.). *KvaliMOTV - 5.5 Tapaustutkimus*. KvaliMOTV. Retrieved April 29, 2024, from https://www.fsd.tuni.fi/menetelmaopetus/kvali/L5_5.html

Sarajärvi, A., & Tuomi, J. (2017). *Laadullinen tutkimus ja sisällönanalyysi* (Vol. 1). Tammi. https://www.ellibslibrary.com/book/9789520400118/laadullinen-tutkimus-ja-sisallonanalyysi-uudistettu-laitos

Schmitz-Berndt, S. (2023a). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1), tyad009. https://doi.org/10.1093/cybsec/tyad009

Schmitz-Berndt, S. (2023b). Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes. In C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, & M. G. Jaatun (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (pp. 343–351). Springer Nature. https://doi.org/10.1007/978-981-19-6414-5_19

Schmitz-Berndt, S., & Anheier, F. (2021). European Union · Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group

Publication 04/20 in Context. *European Data Protection Law Review*, *7*(1), 101–107. https://doi.org/10.21552/edpl/2021/1/13

Schmitz-Berndt, S., & Chiara, P. G. (2022). One step ahead: Mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*, *3*(2), 289–311. https://doi.org/10.1365/s43439-022-00058-7

Schreider, T. (2019). *Building an Effective Cybersecurity Program, 2nd Edition*. Rothstein Associates, Incorporated. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=5965808

Seng, N. (2023). Cybersecurity incident reporting laws in the Asia Pacific. *International Cybersecurity Law Review*, *4*(3), 325–346. https://doi.org/10.1365/s43439-023-00088-9

Singh, C. (2023). European cyber security law in 2023: A review of the advances in the Network and Information Security 2 Directive 2022/2555. *Cyber Security: A Peer-Reviewed Journal*. https://hstalks.com/article/8051/european-cyber-security-law-in-2023-a-review-of-th/

Staddon, J., & Easterday, N. (2019). "It's a generally exhausting field" A Large-Scale Study of Security Incident Management Workflows and Pain Points. *2019 17th International Conference on Privacy, Security and Trust (PST)*, 1–12. https://doi.org/10.1109/PST47121.2019.8949012

Tirtea, R. (2017). *ENISA overview of cybersecurity and related terminology*.

Traficom. (2019). *Kyberharjoitusohje*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

Traficom. (2023, October 20). *Tietomurtoaalto leviää organisaatiosta toiseen – katkaise tietojenkalastelu*. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoaalto-leviaa-organisaatiosta-toiseen-katkaise-tietojenkalastelu

Tsvetanov, T., & Slaria, S. (2021). The effect of the Colonial Pipeline shutdown on gasoline prices. *Economics Letters*, *209*, 110122. https://doi.org/10.1016/j.econlet.2021.110122

Tuomala, V., Vaahtera, J., & Mäkinen, M. (2021). *Kriisiviestintä kyberkriisissä. Kyberkriiseihin valmistautuminen ja kriisiviestinnän harjoittelu pk-yrityksissä* [Publication]. Kaakkois-Suomen ammattikorkeakoulu. http://www.theseus.fi/handle/10024/494993

Valtioneuvosto. (2022). *Ministry sets up a project to improve resilience of critical infrastructure and to identify entities critical to the functioning of society*. Valtioneuvosto. https://valtioneuvosto.fi/en/-/1410869/ministry-sets-up-a-project-to-improve-resilience-of-critical-infrastructure-and-to-identify-entities-critical-to-the-functioning-of-society-

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890. https://doi.org/10.1016/j.clsr.2023.105890

Wanecki, P., Jašek, R., & Drofova, I. (2023). The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model. *2023*

International Conference on Information and Digital Technologies (IDT), 149–154. https://doi.org/10.1109/IDT59031.2023.10194454

Wolff, J. (2014). Models for Cybersecurity Incident Information Sharing and Reporting Policies. *The 43rd Research Conference on Communication, Information and Internet Policy Paper*. https://doi.org/10.2139/ssrn.2587398

APPENDIX 1. INTERVIEW INVITATION

Hei!

Olen työstämässä pro gradu -tutkielmaani Jyväskylän yliopiston Kyberturvallisuuden maisteriohjelmassa. Graduni keskittyy kyberpoikkeamien ilmoittamiseen viranomaisille ja tätä tarkastellaan NIS2, CER ja DORA-lainsäädäntöjen kontekstissa.
Tarkoituksenani on haastatella henkilöitä, jotka ovat toimineet kyberharjoituksissa havainnoitsijoina, jonka takia olet valikoitunut haastateltavaksi. Haastattelun kautta saadaan tietoa, miten kyberharjoitusten ympäristössä toimitaan merkittävien poikkeamien (eng. significant/major incident) ilmoittamisen suhteen. Haastatteluissa ei pyydetä jakamaan tietoa yksittäisten organisaatioiden toimintatavoista, vaan kuvaamaan kyberharjoitustilanteita yleisellä tasolla.
Sinun ei tarvitse valmistautua haastatteluun millään tavalla. Haastattelu kestää noin tunnin ja se nauhoitetaan. Nauhoitus litteroidaan, jonka jälkeen äänitiedosto poistetaan. Litteroitu aineisto anonymisoidaan tutkielmaa varten, eli yksittäistä haastateltavaa ei voi tunnistaa tutkielmasta, eikä [yritys X] nimeä mainita tutkielmassa.

Hyväksymällä kalenterikutsun ilmaiset suostumuksesi osallistua haastatteluun.
Mikäli sinulla herää aiheesta kysyttävää, voit ottaa minuun yhteyttä.

In English:
I am working on my thesis in the Master's program in Cyber Security at the University of Jyväskylä. My thesis focuses on cyber incident reporting to authorities, and this is examined in the context of NIS2, CER and DORA legislation.
My intention is to interview individuals who have acted as observers in cyber exercises, which is why you have been selected as an interviewee. The interview will provide insight into how the reporting of significant/major incidents is handled in the cyber exercise environment. The interviews will not ask you to share information about the practices of individual organizations, but to describe cyber incident situations in general.
You do not need to prepare for the interview in any way. The interview will last approximately one hour and will be recorded. The recording will be transcribed, after which the audio file will be deleted. The transcribed data will be anonymized for the purposes of the thesis, i.e. the individual interviewee will not be identified in the thesis and [company X] name will not be mentioned in the thesis.

By accepting the calendar invitation, you express your consent to participate in the interview.
If you have any questions on the subject, please feel free to contact me.

APPENDIX 2. INTERVIEW QUESTIONS

Basics

1. How many cyber exercises have you observed, approximately? What kind of exercises have they been?
2. Is incident reporting to authorities been practiced in cyber exercises? If yes, how is it incorporated into the exercise?
3. Can you say if the new legislation (NIS2, CER, and DORA) will change cybersecurity exercises? How?

Step one questions

4. What are the key actions cyber exercise participants take when starting the incident management process regarding significant incidents?
5. How do organizations confirm the incident before starting the incident management process?
6. (When there is a significant incident,) What actions have organizations taken before forming the incident response team in response to a sig-nificant incident?
7. Who are the key personnel in the Incident Response Team in response to a significant incident?
8. What have been the reasons they have not formed the IRT, even if they should have? Or they have formed the IRT too early?
9. What can go wrong in forming an incident response team in the event of a significant incident? What are some success factors in forming an incident response team in the event of a significant incident?

Step two questions

10. What kind of understanding of the incident does the IRT team have when they are first formed? What factors contribute to the accuracy or the inaccuracy of that understanding?
11. How does the IRT figure out if they need to make an external notifica-tion to the authorities?

Support questions:

i. What factors do they consider when assessing if they need to make an external notification?
ii. Does everyone have to agree on the matters concerning the incident for them to make the notification?
iii. Does the IRT consult some external parties (who are not in the incident response team), either outside or inside the organization, before deciding to notify authorities?
iv. Does the IRT decide someone to be responsible for the no-tification? If yes, who might it be on the team? If not, how is the notification handled?

12. Have participants prioritized other issues being more important than notifying authorities? What, for example?

13. What kind of information do the participants have before notifying the authorities? When would they have enough, and when would it be too little?

Step three questions

14. Does the IRT have templates for notifying authorities of incidents? If yes, what qualities do these templates have? If there are no templates, how do participants know who, when, and how to contact?
15. What factors might influence notifying authorities of the incident? What are some challenges? What about success factors?

What if information has to be updated to authorities, is it part of the exercise to create a plan for this? What might this plan entail? What can be some bottlenecks in ensuring the information to authorities is updated?

In finnish:

Ensimmäisen vaiheen kysymykset

1. Mitkä ovat keskeiset toimenpiteet, joita kyberharjoituksen osallistujat tekevät, kun he aloittavat tietoturvapoikkeaman hallinnan prosessin (eng. Incident management process) merkittävien poikkeamien osalta?
2. Miten organisaatiot vahvistavat poikkeaman ennen kuin aloittavat tietoturvapoikkeaman hallinnan prosessin?
3. (Kun kyseessä on merkittävä poikkeama,) Mitä toimenpiteitä organisaatiot ovat tehneet ennen kuin muodostavat Incident Response Teamin?
4. Ketkä ovat organisaation keskeiset henkilöt IRT-tiimissä, kun kyseessä on merkittävä poikkeama?
5. Mitkä ovat olleet syyt siihen, miksi organisaatiot eivät ole muodostaneet IRT:tä, vaikka olisi pitänyt? Tai ne ovat muodostaneet IRT:n liian aikaisin?
6. Mikä voi mennä pieleen incident response teamin muodostamisessa, kun sattuu merkittävä poikkeama? Mitkä ovat onnistumisen avaintekijät IRT-tiimin muodostamisessa, kun sattuu merkittävä poikkeama?

Vaiheen kaksi kysymykset

7. Millainen käsitys poikkeamasta IRT:llä on, kun se muodostetaan? Mitkä tekijät vaikuttavat tuon käsityksen tarkkuuteen tai epätarkkuuteen?
8. Miten IRT selvittää, onko heidän ilmoitettava poikkeamasta viranomaisille?
    a. Tukikysymykset:

   i. Mitä tekijöitä he ottavat huomioon arvioidessaan, onko heidän ilmoitettava poikkeamasta viranomaisille?
   ii. Onko kaikkien IRT-jäsenien oltava samaa mieltä poikkeamaan liittyvistä asioista, jotta he voivat tehdä ilmoituksen?
   iii. Konsultoiko IRT joitain ulkopuolisia osapuolia (jotka eivät kuulu IRT:hen) joko organisaation ulkopuolelta tai organisaation sisältä ennen kuin se päättää ilmoittaa poikkeamasta viranomaisille?
   iv. Valitseeko IRT jonkun, joka on vastuussa ilmoittamisen tekemisestä? Jos kyllä, kuka ryhmän jäsenistä se voisi olla? Jos ei, miten ilmoitus hoidetaan?
9. Ovatko osallistujat priorisoineet muita asioita tärkeämmiksi kuin poikkeamasta ilmoittamisen viranomaisille? Mitä esimerkiksi?
10. Mitä tietoa IRT:llä on ennen kuin he ilmoittavat poikkeamasta viranomaisille? Milloin heillä on tarpeeksi? Entä milloin liian vähän?

Vaiheen kolme kysymykset

11. Onko IRT:llä malleja (eng. template), joiden avulla poikkeamien ilmoittamisesta viranomaisille? Jos kyllä, millaisia ominaisuuksia näillä malleilla on? Jos malleja ei ole, miten osallistujat tietävät, keneen, milloin ja miten ottavat yhteyttä?
12. Mitkä tekijät voivat vaikuttaa ilmoituksen tekemiseen? Mitkä ovat joitakin haasteita? Entä onnistumisen avaintekijöitä?
13. Entä jos poikkeaman tietoja on päivitettävä viranomaisille, kuuluuko tämän suunnitelman laatiminen osaksi harjoitusta? Mitä tämä suunnitelma voisi sisältää? Mitkä voivat olla joitakin pullonkauloja varmistaessa, että tietoa päivitetään viranomaisille?

APPENDIX 3. USE OF ARTIFICIAL INTELLIGENCE TOOLS

The author utilized Artificial Intelligence (AI) tools to enhance the research process. These tools were used to translate the interview questions, and invitations into English, occasionally to identify more appropriate synonyms for certain words and translate the abstract to Finnish. The translations were conducted using ChatGPT and DeepL. Additionally, in some cases the author translated the interview quotes with DeepL. Following the initial translations, the author reviewed and revised them to correct any mistakes and ensure the terminology was consistent with the vocabulary used in the thesis. For synonym selection, ChatGPT was the primary tool used but on some occasions the author used DeepL to find synonyms from Finnish to English.