# Incident Information Sharing in the Danish Critical Infrastructure

**– Proposal of a Conceptual Centralised Framework –**

Master Thesis

Ievgeniia Moturi, Livia Dzupinova, Michael Christensen

Aalborg University
Electronics systems

**AALBORG UNIVERSITY**

STUDENT REPORT

**Electronic systems**
Aalborg University
A.C. Meyers Vænge 15
DK - 2450 København SV
http://www.aau.dk

**Title:**
Incident Information Sharing in the Danish Critical Infrastructure: Proposal of a Conceptual Centralised Framework

**Theme:**
Incident information sharing

**Project Period:**
Spring Semester 2022

**Project Group:**
Fri-70141-7

**Participant(s):**
Ievgeniia Moturi
Livia Dzupinova
Michael Christensen

**Supervisor(s):**
Emmanouil Vasilomanolakis

**Copies:** 1

**Page Numbers:** 210

**Date of Completion:**
May 31, 2022

**Abstract:**

This report addresses different aspects of incident information sharing, focusing on the Danish critical infrastructure. Firstly, we consider general challenges in the related work linked to information sharing and combine them with stakeholders' real-life opinions gained by conducting semi-structured interviews. The results were the primary source for the requirements, based on which we created a set of framework guidelines for an information-sharing platform. The report's outcome is a conceptual proposal for a centralised sector and cross-sector information sharing solution where the idea of sharing groups provides users anonymity and freedom for custom sharing besides the obligatory sharing.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

*"Power, today, comes from sharing information, not withholding it"*
**-Keith Ferranzzi**

Sharing cyber security incidents amongst other entities is crucial for an incident management process. A piece of timely shared information can mitigate the consequences of an attack and possibly prevent similar instances among counterparts.

The amount of cyber attacks rises daily. Check Point, a major cyber security company, observed an overall increase of 50% in cyber attacks per week in 2021 [1]. This trend translates into an increase in incidents that companies have to handle. Concerning recent events, such as the attack on Vestas [2] and ongoing attacks on the Ukrainian power grid [3, 4], it is apparent that malicious actors are targeting critical infrastructure. Therefore, information sharing is essential in strengthening the nations' cyber defence to protect organisations.

## 1.1 Background

Incident management is used to mitigate and handle cyber attacks and can help companies prepare for an attack. It is challenging to establish incident management within an enterprise, as it requires financial resources and a knowledgeable overview of enterprise assets and potential vulnerabilities. Additionally, there is no 'one size fits all' solution. The International Organisation of Standards (ISO) and National Institute of Standards and Technology (NIST) offer standards and guides for incident management. ISO mentions incident management in multiple standards; however, ISO 27035 aims specifically for incident management [5], and NIST provides the *Computer Security Incident Handling Guide* [6].

These standards can provide guidance for incident management, improve preparedness and handle critical events, even though it is not mandatory. In addition,

both of them have similar phases of an incident and suggestions on how to handle them (see Table 1.1).

| | **ISO27035** | **NIST** |
|---|---|---|
| 1 | Plan and Prepare | Preparation |
| 2 | Detection and Reporting | Detection and Analysis |
| 3 | Assessment and Decision | Containment, Eradication, and Recovery |
| 4 | Responses | |
| 5 | Lessons Learnt | Post-Incident Activity |

**Table 1.1:** The phases that ISO 27035 and NIST Incident Management standard mention

These phases include anything from Risk Management, Logging and Monitoring, Awareness and information sharing (IS) after or during the incident.

The information sharing is based on information gathered from incidents, either from logs in applications, operating systems or other security systems or reports from employees. Logging is a software feature that can generate automated alerts for the security team, customised after the setup. On the other hand, getting employees to report incidents requires awareness of what to report and how the procedure is shaped for reporting incidents [7]. Awareness in this context includes indicators of what to look for, how to react in case of an incident, and whom to contact. However, as the paper by **Maria Bada et al.** suggests, this is challenging due to the psychology of people [8]. The authors discuss challenges of how an individual can find security an obstacle for their work, leading them to ignore security warnings rather than reporting them, as well as not understanding the consequences of ignoring the alerts.

An awareness program is vital for education and gathering information, which can help prevent an issue from escalating. While the information gathered from the system is crucial, users can also help, as they may notice phishing emails missed by an antivirus or a firewall or other security issues. Automated security solutions for detecting malicious or abnormal activities can be signature-based or anomaly-based. However, the user may notice malicious activity that the software does not, as they know how the system usually interacts.

Information sharing can include multiple elements, such as types of attacks and Indicators of Compromise (IoC). In addition to NIST and ISO, the European Union has created a Directive on security of Network and Information Systems (NIS) [9]. NIS also mentions information sharing concerning cyber security incidents. While NIST and ISO aim for organisations of every size and nature, the NIS Directive focuses on critical infrastructure. The NIS Directive encourages information sharing regarding cyber security incidents to improve security and prevent additional attacks. The information sharing is subject to interpretation in terms

of methods in each member country, leading to differences in interpretation and a lack of uniformity regarding requirements and implementation.

## 1.2 Motivation

The primary motivation for this project is to explore information sharing as an element of incident management. It is partly due to the interest of the group and the need for information sharing and its benefits across industries [10]. The area of interest includes awareness, as having proper reporting guidelines in an organisation can help gather information for the security team. In 2020 out of over 400 cyber incidents handled by the Centre for Cyber Security (CFCS) in Denmark, more than half were phishing or phishing-like [11]. Therefore, we also want to emphasise awareness as a factor positively influencing company preparedness and reaction [12, 13]. Knowing what and who attacked an organisation is vital for other organisations to prevent similar attacks. Equally important is employee training and staying alert for any irregularities, suspicious or potentially malicious activity to detect or prevent incidents [14]. Therefore the concept of awareness and its challenges will be addressed in this report.

We aim to address and analyse current efforts for information sharing, potential challenges and room for improvement. Once the current efforts have been identified, we would like to contribute with a conceptual framework compliant with current regulations and based on real-life experience. The ultimate goal is to create a simplified way to report and share information about cyber security incidents without compromising privacy.

## 1.3 Information Sharing in Denmark and the EU

This section describes information sharing in Denmark and has comparisons to other approaches in other EU countries. It is split into two parts, Cyber Security Incident Response Team (CSIRT) and Computer emergency response team, used across the EU, and Decentralised Cyber Information Security (DCIS), more specific to Denmark.

### 1.3.1 CSIRT and CERT

The Network and Information Systems Directive [9] set a foundation for incident reporting and information sharing when released in 2016 and updated in 2018. By requiring members of the EU to create Computer Security Incident Response Teams (CSIRTs) and authorities on a national level concerning Operators of Essential Services (OES) within a limited time, many uncertainties have been raised within this area. In addition, a plethora of solutions for specific cases, states and

organisations make centralised information sharing difficult. Just in Denmark, ENISA recognises 12 distinct CSIRTs, which can be seen in Table 1.2, and in the EU, there are over 600 others [15].

| OES | Team | Constituacy | CSIRT Network member | FIRST member |
|---|---|---|---|---|
| Digital infrastructure | TDC SOC | ISP Customer Base | No | Yes |
| Energy | Orsted SAC | Commercial Organisation | No | Yes |
| | EnergyCERT | Non-Commercial Organisation | No | No |
| Financial | JN DATA CDC | Financial | No | No |
| | NetsCERT | Financial | No | No |
| National level | CFCS | Government, National | Yes | Yes |
| | DKCERT | National research and education network (NREN) | No | Yes |
| Sea transport | SWAT | Commercial Organisation | No | No |
| No | CSIS.dk | Commercial Organisation | No | No |
| | Secunia Research | Commercial Organisation | No | Yes |
| | KMD-CERT | ISP Customer Base | No | Yes |
| | Ezenta | Service Provider, Customer Base | No | No |

**Table 1.2:** Overview of CSIRTs in Denmark according to ENISA [15]

Even though most CSIRTs in Denmark are created for individual companies, some fulfil services of so-called SOCs (Security Operations Center), centralised management and support every security aspect of company operations. Except for the Centre for Cyber Security (CFCS), none of the organisations depicted in Table 1.2 is a member of the CSIRTs Network [16], and half are under the global association of CSIRTs - FIRST [17], meaning there are not many indicators of sharing between individual CSIRTs. Some of the teams on the list have the suffix 'CERT' in the title, meaning Computer Emergency Response Team, which acts as a trademark assigned after being approved by CERT-CC.

The key difference between CSIRT and CERT is that Governments or companies establish CERTs to advise about incidents and knowledge of information sharing with other CERTs and help handle incidents, while CSIRTs are, in most cases participating in international cooperation and established to support OES. National CERTs handle incidents of companies that do not have designated or contracted CERTs/CSIRTs. For example, DKCERT [18] is publishing a yearly trend report on current cyber threats to inform about current risks and potential attacks. The cooperation of CSIRTs can be arranged as either centralised, sectorial or mixed [19] (see Figure 1.1).

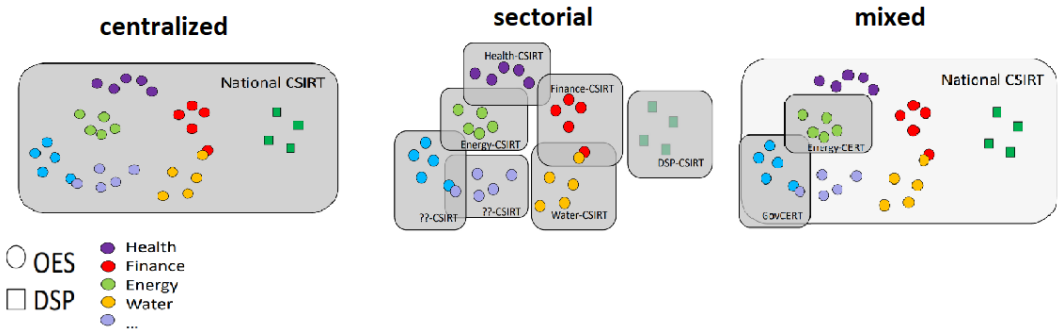


**Figure 1.1:** CSIRTs cooperation models [19]

The sectorial information sharing can be included in Information Sharing and Analysis Center (ISAC). Its primary purpose is to be able to share information between private and public sectors, within the same sector and across other countries. To this day, the EU formed ISACs for the financial sector, energy sector, aviation sector and most recently, the railway sector, of which Denmark is also a member [20]. To take an example on the national level, Finland has a centralised information sharing between the sectors. The National Cyber Security Centre Finland (NCSCFI) administers an ISAC type of sharing system where each sector ISAC shares to one place [21]. It is worth mentioning that this setup includes more than NIS defined as critical infrastructures such as media and water management, to name a few (see Figure E.1).

### 1.3.2 DCIS

Apart from CSIRTs/CERTs, some of the other critical sectors in Denmark (health [22], finance [23] and telecommunications [24]) have established sector-specific Decentralised Cyber Information Security (DCIS) units as an intermediary agent between a company and the CFCS. For 2022-2024 Denmark set a budget of 270 million DKK [25] to support strengthening Danish cyber and information security [11], including, among others, efforts to have a dedicated DCIS for all sectors within the critical infrastructure. As indicated in a study by Hansen [26], the DCIS establishment limits the information sharing within sectors, its direct collaboration with authorities and further sharing. Furthermore, such an establishment does not provide transparency or data utilisation outside state threat intelligence. Lastly, not all sectors have their own DCIS, as there is no mention of energy and transport sector DCISs.

At the time of writing, it was only found that the railway subsector actively participates in the information sharing within ISAC for Denmark. When we look at sectors within Denmark, we can see prevailing efforts in the Financial, Energy, Sea

transport and Digital infrastructure sectors, as seen in Table 1.2. However, all in all, we did not find any cross-sectorial inter-border solution for information sharing (for example, in Austria [19] or aforementioned Finland) apart from National CERTs. Lastly, we did not find that individual sector DCISs share information with each other.

### 1.3.3 Problem Delimitation

Since information sharing according to the NIS Directive is up to each member state of the European Union, there is no unified way or procedure to do so. This project focus on the challenges of information sharing concerning cyber security incidents and develops a framework for an information sharing solution. Furthermore, the focus will be on critical infrastructure due to its importance to society and regulations, which requires these organisations to have special security measures. According to the Danish national strategy for cyber- and information security [11], critical infrastructure sectors in Denmark are considered to be finance, sea transport, energy, health, telecommunications and transport. The upcoming new NIS Directive (NIS2), among other sectors, also includes the water and space sectors [27]. However, because the NIS2 Directive is yet to be finalised in 2022, we only consider the sectors from the original NIS Directive defined in Denmark. Therefore, we focus on the Danish critical infrastructure to further limit the project's scope. The project will also investigate awareness elements in gathering information for cyber security information sharing.

#### Problem Statement

As described in Section 1.3, information sharing (IS) in Denmark is often restrained within each sector, and in that way, the comprehensive information and knowledge dissemination are inherently limited. Thus, we wonder whether a more centralised approach could benefit information sharing. To quote the American cybersecurity agency CISA: *"The more you share, the more everyone becomes informed, and the more we all prevent further damage from vicious cyber-attacks together!"*. In addition to this, it is interesting to determine whether the stakeholders would be interested and willing to expand their information sharing domain. This led to the problem statement with subquestions as follows:

***How can a national information sharing platform for critical infrastructure in Denmark be designed?***

1. How can the platform users be authenticated and managed?
2. What is the motivation for information sharing?

3. How does awareness influence information sharing?
4. What type of information should be processed?
5. How do we secure data handled by an IS platform?
6. What requirements and features are relevant for the platform?

The problem formulation and its subquestions will be addressed throughout the report. The chapters are organised as follows:

**Chapter 2** will look into the methods used throughout the report. **Chapter 4** and **Chapter 3** looks into the awareness and information sharing state of the art and the identity and access management elements in the background, respectively. **Chapter 5** describes the stakeholders and outcomes of the interviews. **Chapter 6** will gather the requirements obtained in the previous chapters and creates a final list. **Chapter 7** will consider legal perspective and analyse the sharing technologies required to create a solution. **Chapter 8** will take the requirements and finalise a list of functionalities combined into a conceptual design for the framework. **Chapter 9** and will discuss the project limitations and **Chapter 10** concludes the outcome of this project.

# Chapter 2

# Methodology

This chapter presents and explains methods, method choice, their usability and the benefits of the methods applied in this project. It is composed of **Section 2.1**, where we reason for the choice of our custom process model. **Section 2.2** introduces the methods involved in gathering and generating system requirements, and lastly, **Section 2.3** describes the approach used for the second round of user involvement.

## 2.1 Process model

While creating our custom process model, we got inspired by the process model in the related work PROTECTIVE [28]. In this project, the requirement gathering phases are performed in parallel. We have decided to create our process model based on two factors.

Firstly, none of the traditional models like Waterfall or the Incremental model for software development was chosen, as they do not involve stakeholders. As we needed an agile process where we could revisit and rephrase requirements as we proceeded with new phases, the Waterfall model [29, 30, 31] was not applicable with its no recursive approach. Secondly, we divided the gathering process equally into three individual stages.

Since the goal of this project is the system design and not the implementation, an incremental model [29], which focuses on the incremental deployments, was deemed as overreaching and thus unfit for us. Although, we did utilise the iterative element in our requirement generation and design phase. As for Scrum and other agile models [30], the importance of precise planning and the need for a structural meeting is beneficial. However, we did not plan to develop anything tangible and instead focused on analysing the aspects of the solution and finding the right design and collection of the features. We did not use this model either. Although, we have utilised the planning routine and continuous status meetings.

Despite identifying practical elements from other models, none matched our

project workflow completely. Therefore, we have designed a process model (Figure 2.1) composed of the background of Identity and access management, State of the art, and interviews in Stakeholder involvement as parallel phases to gather a list of initial requirements. The next step is to analyse different technical and legal areas relevant to the system. Some of the functional requirements were included in the second round of Stakeholder involvement to inquire about the users' opinions and incorporate them into the design. The design for the information sharing platform is created at last, based on all the knowledge acquired until this phase.

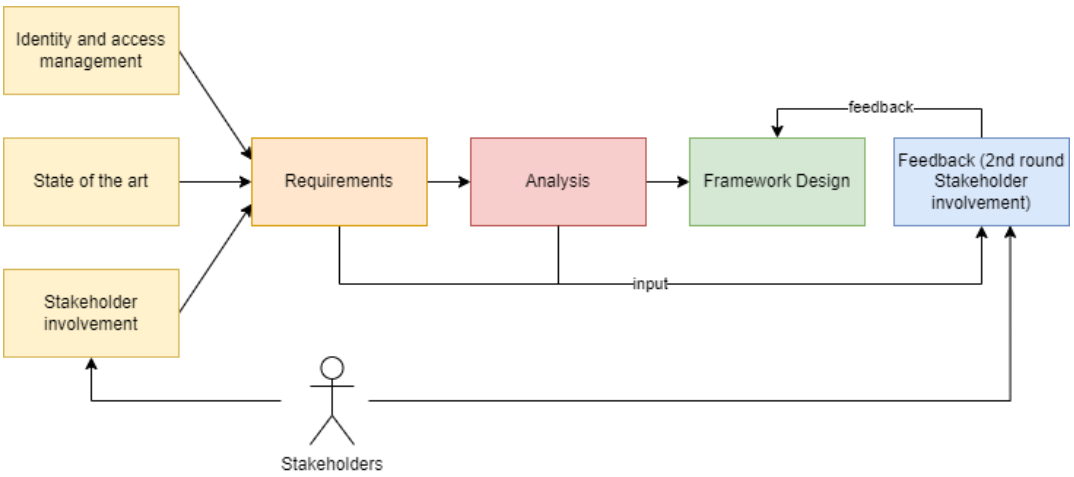


**Figure 2.1:** Project process model

## 2.2 Requirement engineering

Requirement engineering comprises two phases: Requirement gathering and Requirement implementation [32]. Due to the nature of the project being theoretical, we will focus solely on the Requirement gathering phase.

In the following sections, we argue for selecting methods for gathering information about information sharing. The most important findings were used to elicit requirements and guide our design choices for the ideal information sharing system. **Rehman et al. [32]** advise using more than one method in this process. For this reason, we utilised several methods and both first-hand and second-hand sources in the project.

### 2.2.1 Literature review

In order to present factual and academic knowledge in this report, we utilised thesis literature review [33] as the dominant method to gather sources of related work. The baseline condition was that source needed to be public or available under a

student licence. The majority of **Chapter 4** consists of the results of our literature review. Search engines like Google Scholar, AAU library, as well as regular Google search were used to find relevant titles and works done in the thesis area. Using keywords search like "*awareness*", "*awareness training*", "*information sharing*", "*information sharing systems*", "*cyber threat intelligence sharing*", "*cyber incident sharing*", "*challenges in information sharing*", and "*motivation for information sharing*" we have narrowed down related work based on a relevance to the topics discussed in **Chapter 4**, a publisher, the number of citations and the overall findings of the research.

### 2.2.2 Survey research: Questionnaire

Survey research is a method for collecting data for further analysis [34]. A questionnaire is a tool for collecting data, which, if using the correct formulations, could lead to the desired answer for the research.

Designing the questions is as important as defining the correct target group to answer. As for the different approaches to questionnaires, there are two distinct types: self-administered and researcher administered. In the first case, the respondent is not directly interacting with the researcher. In this case, the questionnaire can be delivered online (e.g. via email) or in a paper version via post. The major advantages of the self-administered questionnaire are cost and time effectiveness for the researchers, an opportunity for the respondent to answer the questions at a comfortable pace, easiness of sampling small and large groups, and the possibility of making a survey anonymous. However, self-administered questionnaires have some disadvantages: non-completed surveys and biased responses from volunteers, among others.

When it comes to the researcher-administered questionnaires, the researcher is present at the response time. This method allows getting more complete answers as a participant may be requested to elaborate the response by clarifying ambiguous formulations. There is a higher probability of completing the questionnaire, and it helps the researcher make sure that the respondent is a representative of the target group (Section 5.1.2). On the negative side, researcher-administered questionnaires are time-consuming. The qualitative responses collected from the open questions may pose an obstacle in later data analysis. Another difficulty is social desirability bias [35], which indicates that people tend to respond in a more socially acceptable way. It means that respondents may answer even in an untruthful way to perceive a norm in a given society.

In this project, questionnaires were self-administered as the structure of the questions, yes/no answers aimed to eliminate bias in the responses. Another reason for choosing the self-administered questionnaire type was the planning of the interviews and the overall business of the stakeholders, where they could submit

their answers prior to the scheduled interview at a convenient time.

### 2.2.3 Interviews

To gather first-hand information from potential system stakeholders, which is highly valuable in the requirement elicitation process [36], we chose the interview method. To analyse the gathered information, the semi-structured interview is preferred, as this method provides a structural and homogeneous approach to questioning the subject resulting in comparable outcomes while being versatile at the same time.

The semi-structured interviews are based on a common understanding of the question by subject rather than specific phrasing [37]. The advantage of that is the ability for the interviewer to ask a probe (rephrased question or supplementary question) to make the interviewee understand the question's meaning. The compatibility of semi-structured interviews in mixed-method data processing is also deemed beneficial as it allows us to analyse data from both qualitative and quantitative perspectives [37].

#### Pilot interviews

**Chenail [38]** has proved that pilot studies are essential to improve and test the prepared questions and interview procedures. By performing a test interview, one can gain helpful feedback to understand weak points in the interviews and even remove and change focus on a few elements.

#### Sampling and Recruitment

According to our scope explained in Section 1.3.3, our target group are companies classified as OES in Denmark. In order to recruit the most fitting respondents, we decided to conduct Purposive Sampling to select candidates for questionnaires and interviews.

Purposive Sampling is about selecting participants based on their relevancy and knowledge about the researched topic, in our case, experience with information sharing and critical infrastructure management [39]. Purposive Sampling, in comparison to Random Sampling, results in a more fitting sample and, in that way, guarantees that each interviewed person has the required skill to answer the questions, thus improving the outcome information quality [40].

To improve recruitment efficiency, we utilised the element of Convenience sampling [40] by reaching out to potential participants through an acquaintance or someone we know beforehand to forward the interview request. This factor might possess the bias for the motivation of participants to contribute as an outcome of favour. However, we assume that the information acquired in the interview can be

narrowed to the bias of a respondent's role in a company rather than the incentive to participate. We utilise email, Linkedin, and personal contact to gather contact information in a few cases.

### 2.2.4 Scenarios and Use cases

Use cases in software development are essentially the user's (actor's) actions with the given system. They define what functional requirements need to be implemented. In addition, each use case can be turned into a test case, which simplifies the testing of requirements and system validation [41].

In order to gather as well as understand which use cases are relevant for our system, we utilised scenarios in the process. Scenarios are useful as they give an easy to read, high-level description of a use case and a situation where it is performed. In addition, research concludes that scenarios positively affect the final requirement quality [42]. Creating scenarios for all types of users, can ensure that different user perspectives and system functions will not be easily overlooked. We decided on a narrative type of scenario, which in contrast to the step-by-step scenario type, broadens situational context and still offers logical flow.

### 2.2.5 MoSCoW method

An inevitable part of the requirement engineering process is requirement prioritisation. It can be done by utilising techniques from ranking and analytical hierarchy to the different sorting schemes. We strive to find the method which would be time-convenient and harmonising with our process model. Analytical Hierarchy Process (AHP) constitutes comparing pairs and assigning a scale to create a hierarchy, which gives a very detailed overview of connections and the importance of one requirement in relation to another. On the other hand, it is rather time consuming and impractical for agile requirement creation. Each time a requirement has been added, removed or modified would impact the whole hierarchical organisation of the requirements and need to be redone. Therefore, even though this method is highly recommended by **Khan et al. [43]**, we looked for methods where results are easily adjustable, thus fitting in our requirement re-visitation model.

Another research recommended method is the MoSCoW method [44]. Unlike AHP, this method does not provide detailed analysis. Instead, it classifies requirements into four categories: *Must, Should, Could and Won't*, further elaborated in Figure 2.2, specifying their importance to the products initial and latest release stages.

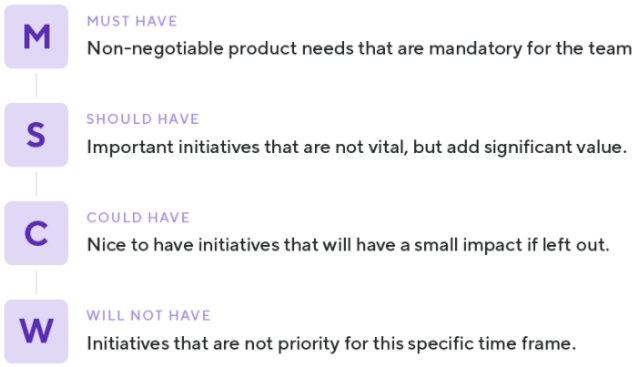


**Figure 2.2:** MoSCoW categories explained [45]

In addition, by dividing requirements like so, one may realise that certain requirements from the *Could* and *Won't* pile might be redundant for the system. This method, however, poses some challenges. For example, prioritisation within the group is not advised, and it is up to the engineers to prioritise the implementation of each modal verb group. Overall, the MoSCoW method is relatively easy to perform, uncomplicated to understand and performs well when it comes to the time required and late requirement changes, contrary to other more complex methods [44, 46]. Thus, it was prioritised for this project over the other requirement prioritisation methods.

## 2.3 Second round of user involvement

The second round of user involvement is to validate the relevance of a portion of the functional choices of our proposal. As we were solely interested in users' feedback on what the system does, disregarding system layout, we omitted the system interface from testing altogether. In that regard, methods like Wireframing would not work. Instead, we decided to conduct a validation session based on Scenario-based testing [47] with users where a simplified version of system scenarios would be introduced to provide context.

The user would be guided through the list of tasks and asked to justify the presented system function's choice to fulfil each task. In this way, we can get feedback on the functional requirements which involve user actions. Based on the user's comments, we can understand whether the function is relevant, sufficient, or needs to be modified or removed from the framework proposal.

# Chapter 3

# Identity and Access management Background

This chapter provides the background of the identity and access management system. An overview of this topic helps future planning for the framework design and provides the foundation for user management processes. Section 3.1 focuses on authentication and identity management as an essential element of the system. Section 3.2 describes identity management solutions, while Section 3.3 dives into phases of the access control mechanisms and presents various protocols potentially utilisable for the information sharing platform.

## 3.1 Identity and Access management

Identity and access control management is defined here as *"the control of access to system resources after a user's account credentials and identity have been authenticated and access to the system has been granted"* [48]. The process is divided into the three phases identification, authentication and authorisation. The identification and authentication represent the identity management phase, and authorisation deals with access management in the identity and access management solutions. Figure 3.1 displays the access control mechanisms involved in managing the identity during a user's access to the desired resource. The following sections discusses the three stages of the identity and access management to determine the most fitting solution for an information sharing platform.

### 3.1.1 Identification

Identification is a step in the identity management phase, during which a user presents a set of claims about themselves or other digital subjects [50]. The goal of identification is to identify the user in a requested system or application uniquely

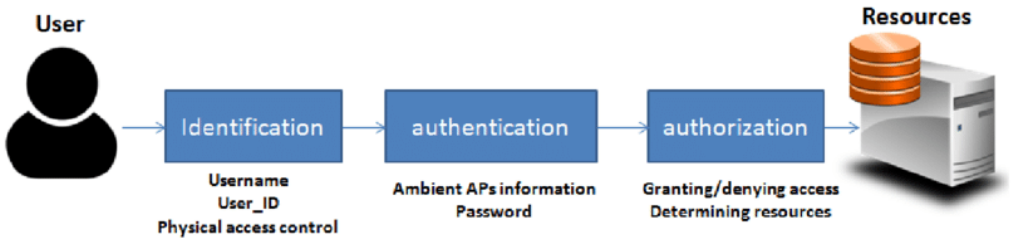


**Figure 3.1:** Access control mechanisms [49]

by providing one or more pieces of evidence of the user's identity. Generally, it is done in one or a combination of the three ways: by providing something that a user knows (e.g. password), something that a user has (e.g. cryptography keys, hardware token, phone etc.) or proving who they are (biometric authentication). Identification lays the foundation for an entity's authentication process, which can be done in multiple ways discussed in the following section.

### 3.1.2 Authentication

Authentication is an operation that determines if someone requesting access to a particular resource is whom they claim they are. Digital authentication happens via authentication protocol and aims to preserve the privacy of the credentials presented in the authentication dialogue. It is the second step in the user access processes after identification.

Even though authentication mechanisms strive to preserve privacy, transferring user credentials in the authentication process poses the risk of leaking user information, thus compromising the user's privacy and the requested resource. The National Institute of Standards and Technology (NIST) provides guidelines on how to minimise the risk of disclosing the user identity via so-called assurance levels [51]. Assurance levels represent guidelines for organisations on how to separate identity assurance into separated components of the authentication. NIST distinguishes three levels of assurance: Identity Assurance Level (IAL), Authenticator Assurance Level (AAL) and Federation Assurance Level (FAL). For the systems that facilitate the non-federated environments, the two first assurance levels could be chosen: IAL, which concerns the identity proofing process, or AAL, which refers to the authentication process. If the environment supports the federated architecture of identities. Depending on the future design of the envisioned system, the NIST Assurance levels can serve as a guideline for the required implementation and technical consideration for the identity handling and authentication processes.

In this section, we present user-authentication strategies. First, we discuss the

existing schemes, and then we assess their suitability and components for information sharing for critical infrastructure scenarios.

### Password authentication

One of the oldest authentication methods is a password-based authentication proposed by Lamport in 1981 [52]. This method has proven effective for both users and systems: it is relatively easy to remember shared secrets with the IT system. From the system perspective, it is cost and resource-effective [53]. Although, for the information sharing platform, password-based authentication should be fast and a secure way to authenticate an entity, it is necessary to follow a list of requirements to make it more secure [54]. It may be possible only to use password authentication for the information sharing scenario. However, the password's strength should correlate with the security requirements, e.g. having an adequate password length, the system checking the newly created password against the list of the top 10000 breached passwords [55], etc.

### Hardware based authentication

Hardware based authentication represents a method where a user presents a physical possession that plays a part in the authentication process. This method is widely used in securing physical access in combination with password authentication. In the software domain, hardware authentication suggests possession of a cryptographic device (e.g. a token) that is used to gain access to the desired resource.

### Biometrics authentication

The biometric factor is a method that allows verification and authentication of an individual based on the presented physiological or behavioural characteristics [56]. This authentication method regularly combines one or two other authentication factors, where read biometric characteristics are associated with a username stored in a database. It is a secure way to authenticate users; however, this comes with a cost. Biometric authentication requires installed specialised hardware on each endpoint. Depending on the method used, it can be a fingerprint, retinal, iris scanner, i.a. Another concern is the sensitivity level, which decides what percentage of exact match a recorded sample compares to the presented one at the time of authentication [57].

Biometric authentication is used in, for example, FIDO2: WebAuthn CTAP, where during the registration and authentication phases, biometric information is never leaving a user's device, eliminating the risk of phishing and password theft [58].

#### Multifactor authentication

Multifactor authentication represents a combination of methods where a combination of two or more authentication methods is used [59]. Compared to a single-factor authentication, an additional factor adds a barrier to a potential attacker, i.a., even though the attacker learns a user's password, they lack an additional possession or inherence factor to finish authentication.

None of the authentication schemes discussed above is ' bulletproof' and can be compromised [60], [61]. However, an additional level of security makes it much more difficult to gain unauthorised access to the malicious actors.

Selecting a suitable authentication scheme is essential for the following identity and access management step, namely authorisation.

### 3.1.3 Authorisation

The rights of what a user can or cannot do with a particular requested resource and revocation of access or usage rights are defined by the process called **authorisation** [62]. This procedure ensures that the requesting party exercises only authorised rights. This process is known as policy enforcement. At the authorisation, there must be methods that determine those rights, defined in the policy definition. There must be some rights that the user will obtain using an access control model in most environments. Various organisations depending on their business needs and goals, implement different access control models.

#### Access control schemes

There exist several types of access control: Discretionary Access Control (DAC), Mandatory access control (MAC), Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

DAC is a commonly used access control model [63] since it is implemented on most operating systems used today. E.g. when a user creates a spreadsheet, they become an owner of the document. The owner in this scenario can control who has access and what type of access they have. In addition, the document owner can modify or revoke access at any point in time, which both can be a strength and a weakness.

On the one hand, the owner has all the flexibility to grant access, allow object modification or revoke all rights from a user. On the other hand, user administration and flexibility also bring weakness to access control security. As a user is prone to mistakes (e.g., assigning more rights than necessary or forgetting to revoke the access rights), this access control model is considered weak.

MAC is the strictest access control model based on the hierarchical approach to control access to files/resources. The operating system will limit how much access

a client will have to a particular object. For example, governments and military offices often use MAC. It uses "security labels" (or "clearance levels") to allocate resource objects on the requested system, meaning that every object a user may access needs a security label to be assigned to it, e.g., "public", "confidential", "secret", etc. The users are provided with certain rights depending on the objects and users' security levels. The administrator of the system decides what specific access a user may have. A user cannot change the rights assigned under the Mandatory Access Control model.

RBAC is an access control model where based on a particular role assigned to a single user (e.g., a "director" role, "manager" role, "administrator" role etc.), they can access or perform actions on particular system objects. The negative side of RBAC is referred to as a role explosion describing a situation when depending on the system and application, a user (within an organisation) can occupy different positions. For example, an employee can be an application owner and thus have administrative rights in the HR system but only have access as a "reader" to an IT application. To administer the granular access rights, the admins should create various roles for users and continuously monitor their access levels. Reviewing is both a time consuming and complex process, especially when it comes to a large organisation. One of the solutions to facilitate RBAC is to limit the amount of time a user has a particular role. The access level can be extended or revoked close to the expiration time.

Attribute-based access control ABAC is the most complex access control model compared to those mentioned above. It allows for creating a very sophisticated and complex relationship between the requested service, the data used by the service, and the user who requests the service. ABAC allows to determine precisely what type of access a user might have; therefore, it is often referred to as "Next Generation Access Control" [64], [65]. ABAC may consider a combination of factors to assign users certain access rights, e.g. IP address, time of the day, geographical location etc.

| Factors | DAC | MAC | RBAC | ABAC |
|---|---|---|---|---|
| **Access Control to Information** | Through owner of data | Through fixed rules | Through roles | Through attributes |
| **Access Control Based on** | Discretion of owner of data | Classification of users and data | Classification of roles | Evaluation of attributes |
| **Flexibility for Accessing Information** | High | Low | High | Very high |
| **Access Revocation Complexity** | Very complex | Very easy | Very easy | Very easy |

**Figure 3.2:** Comparison between DAC MAC RBAC and ABAC [66]

Figure 3.2 provides an overview of the above presented access control schemes. Based on the flexibility and access revocation complexity, the ABAC seems the

most flexible in granting and revoking access.

## 3.2 Identity management solutions

When it comes to identifying entities on the information sharing platform, one of the fundamental concepts is the identity of an entity requesting access to a resource or performing an action of the platform. Identity management concerns managing the information about the identity of users and regulation of their access level to the requested resources [67]. In the given scenario, a company that shares the information about a breach is still represented by a single individual. Therefore, it is up to each user of the platform to present a set of credentials and identify themselves as a trusted party on the platform. While trust would be discussed in Chapter 7, the focus lies on identifying a potential player in the information sharing platform, i.e. how to identify entities from multiple sectors before authenticating them to the platform, as well as how to manage identity in a secure way.

Kim Cameron defines *digital identity* as a set of claims made by one digital subject about itself or another digital subject. In the proposed seven laws of digital identity [50], Cameron addresses the underlying problem of interconnected systems on the Internet, the problem of not knowing who is connecting to what. The laws highlight the importance of privacy for the subject and data minimisation when it comes to proof of one's identity and limiting the number of parties who can access the information provided by the claimant. These qualities are highly valued when sharing information about possible attacks with multiple businesses, including competitors.

When it comes to business-to-business communication, we are talking about two solutions. First, a single employee's identity can be managed centrally via a trusted third party by creating an inter-organisation identity management system or by each organisation, creating and maintaining their connection to the system. The centralised system will authenticate and authorise users with a custom credential set defined by each organisation. The central services ensure that all users have the same unified set of credentials, ensuring consistency throughout the platform. This setup simplifies orchestrating management and maintenance operations of the platform by providing a centralised point of control on the one hand. On the other hand, this is also a single point of failure, whereby taking down this central point will disable access for all the entities.

### 3.2.1 Single sign-on and single sign-off

Single sign-on and single sign-off (SSO) enable users to navigate between multiple systems and applications without manually managing passwords and credentials for each one of them [68]. There are variations in the authentication flow depending

on the system requirements, but the generalised case is presented in Figure 3.3. It depicts the authentication flow in the SSO scenario and has the following steps:

- A user intends to login to a platform and visits the desired web address;
- The browser "visits" the Identity Provider (IdP), and the IdP performs authentication;
- After the user has been authenticated, the IdP agrees to share the user information with the relying party with the help of an authorisation code;
- The relying party can now use the authorisation code to retrieve necessary tokens from the token endpoint (provided by the IdP);
- In many cases, to avoid re-authentication, the relying party sets persistent cookies on the user side.

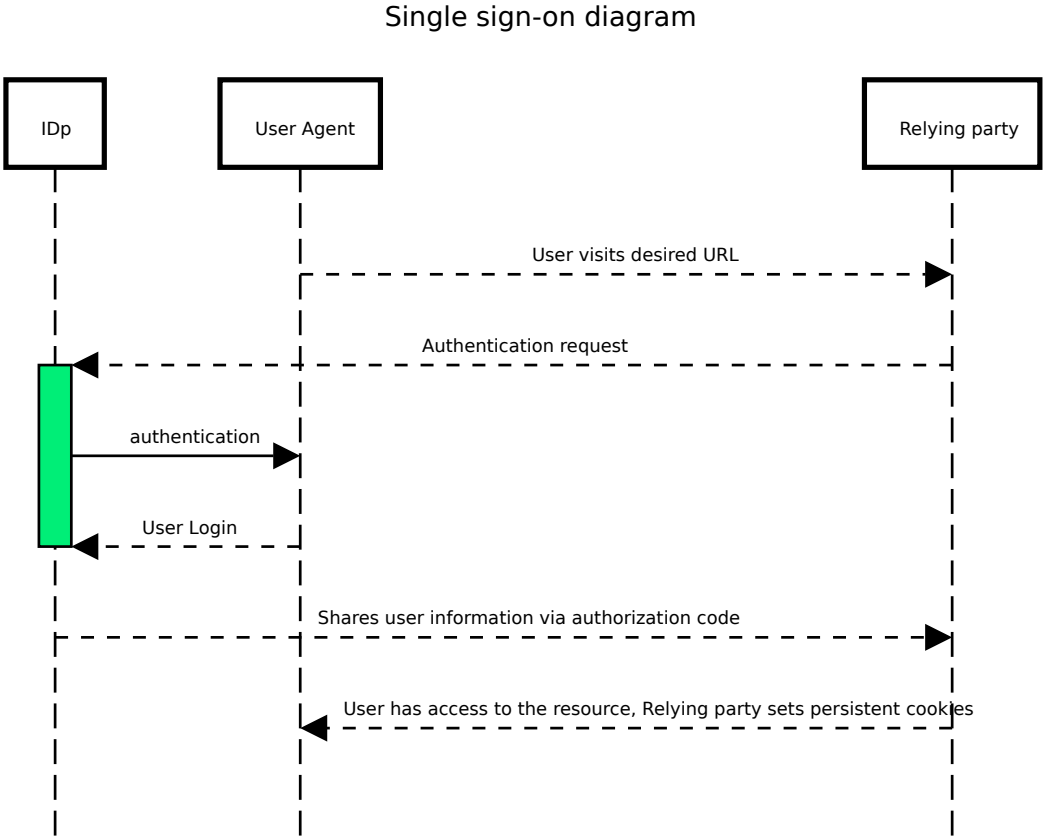


**Figure 3.3:** Single sign on

Looking at the flow, the positive factors of SSO can be counted as ease of use for the end-user, integrated experience, and no additional credential maintenance.

However, when it comes to the negative side of SSO, the following should be considered: sharing organisational credentials pose a severe security risk in case of data leakage, and there exists multiple vulnerabilities in Identity and access management protocols implementations [69], [70], and the most severe one is the inability to recover from an IdP compromise.

SSO solutions require maintaining all the actor's credentials by a single party (IdP). This makes it a very attractive aim for the attackers as compromise will inevitably compromise all entities and stakeholders involved. The recent Okta hack can serve as an example of such a compromise [71].

### 3.2.2 Federated identity

Federated identity aims to solve the challenge of identity and access management solutions in cross-organisational collaboration. Even though the federation might look for the end user just like SSO, there is a distinctive difference in processing authentication. The problem of the users of an organisation "A" needing to access resources of an organisation "B" (vendors, suppliers, customers etc.) could be solved by managing external accounts manually. This would mean maintaining a database with all the access rights for a single resource and extending access rights whenever they are expiring. This approach is resource-heavy and is neither user-friendly nor secure due to human error. Another solution to inter-business communication is federated identity management. The federated identity model setup does not require a homogeneous setup from the involved parties. During the establishment process, all the cooperating parties determine who, how and in what configuration they will operate [72].

Figure 3.4 demonstrates schematically federated identity architecture, components involved, and a typical information flow in the federated model during authentication. The Service Provider (SP) authorises a user to access the requested resource. Authorisation happens after exchanging credentials with the IdP utilising a security token. IdPs can be independent or grouped with SPs. In this case, IdPs and SPs are connected by mutual trust and exchange user information concerning privacy preservation. Black dotted lines represent authentication requests, whereas amber dotted lines indicate authorisation responses.

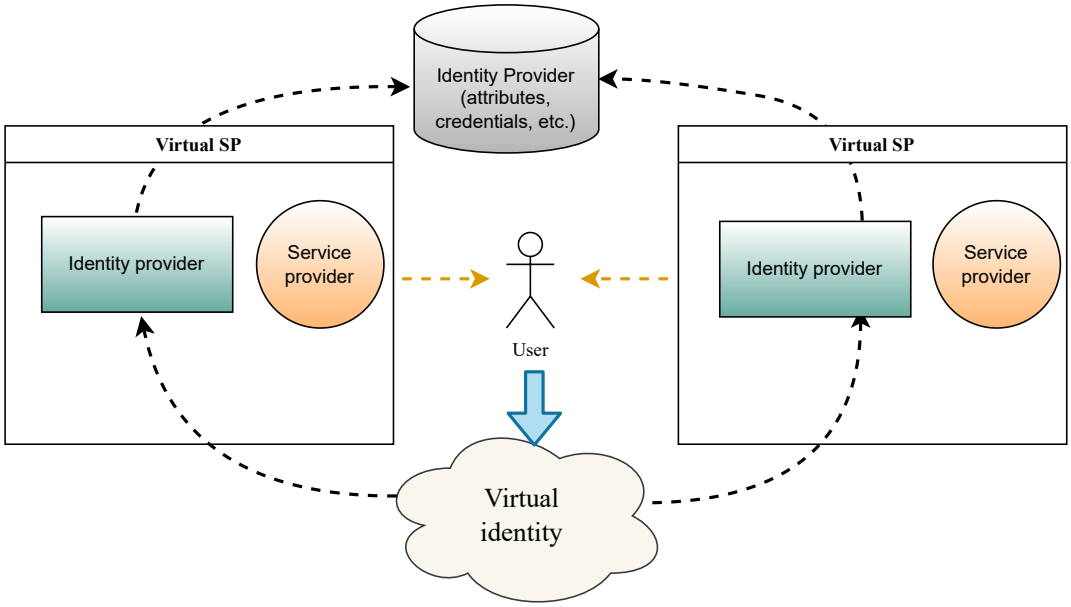


**Figure 3.4:** Federated identity architecture [73]

Even though the primary goal of the federated identity model is to ensure that SSO is enabled between multiple autonomous business entities. It also allows users to prove their identities based on a subset of claims, i.e., providing a partial identity.

There currently exist many solutions to federated identity management. However, some predominant solutions are SAML and OIDC [74]. Security Assertion Markup Language (SAML), which is commonly used in business-to-business collaboration identifies two roles: IdP and SP. OpenID Connect (OIDC), is another standard, which is a popular choice for Internet-based services and refers to OpenID Providers (OP) and Relying Parties (RP) [75]. We will discuss these and the other standards for identity federation in detail in the following section.

The range of access and uniformity of the platforms of the parties enrolled on an information sharing platform are the two main aspects to consider when it comes to the choice of the identity management solution. For the information sharing scenario, one of the key requirements is to preserve the privacy of the communicating parties. The federation model can serve as a good solution to this requirement, as it allows for a combination of IdP setups. In addition, grouped IdPs used in the same critical infrastructure sector can ensure more trust between the parties. In contrast, an independent IdP could serve as a central unit that would identify, authenticate and authorise parties, sharing the information between the sectors.

## 3.3 Identity management protocols

In this section, we describe various identity management protocols. They play an essential role in governing information sharing solutions as they contribute to the security and usability of the platform by managing the identities of all the platform actors. The identity management protocols aim to facilitate the authentication and authorisation of users. It is achieved with the help of a few separate entities within the protocol, and the steps vary based on the protocol implementation, purpose and place of usage. User identity is established with the help of an IdP, which is enabled to send user credentials to the service provider, where authentication and authorisation happen before assigning the requesting entity a certain level of access.

Figure 3.5 demonstrates one of the possible classifications of the identity management protocols, which is dividing the list into web-based and their counterparts as well as some hybrid solutions. This section aims to find the most suitable protocols for the information sharing use case. Majorly basing our classification on usability on the web, we search for the best fit for the information sharing use case. The necessity to look through many solutions is justified by the fact that the final product should be versatile. The platform should also authenticate and authorise users based on various credentials depending on the level of access each entity requirements.

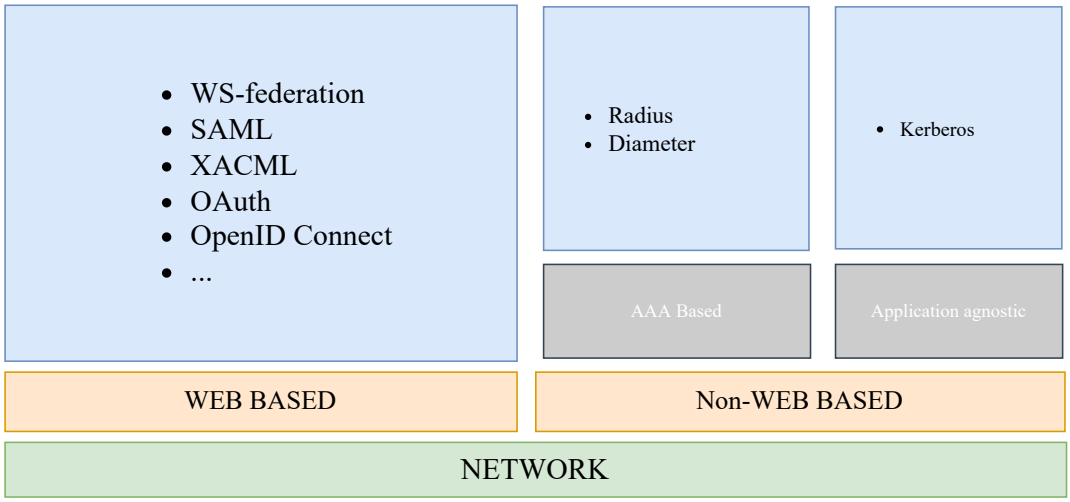


**Figure 3.5:** Identity Management Protocols [73]

### WS-federation

Web Services federation [76] is a protocol used for facilitating user access to different security domains and networks, with a precondition of an established trust

relationship between the parties. WS-federation is a part of an umbrella framework called WS-Security (Web-based security). Used solely in Windows-based solutions, WS-federation establishes security requirements for communication between multiple entities based on each participant's security policies.

The parties involved in the communication flow of the protocol are IdP, Security Token Service (STS) and the Resource Provider. The flow can be divided into several logical steps: a user requests a desired resource administered by the Resource Provider; the Resource provider receives the request together with the query for policies; then IdP issues an identity security token, which the client can use; This token is presented to STS to obtain access to the desired resource. However, the implementation and steps can vary depending on the level of trust established between the entities [77], e.g. the number of claims presented, demonstration of an authorised use of security token, digital signature etc.

### SAML

Security Assertion Markup Language is an open standard managed by the Organisation for the Advancement of Structured Information Standards. It is used for federated identity systems, offering the user a single sign-on experience. A user only has to sign in one place but can access multiple domains. This is done by signing in to an IdP, which can pass authentication tokens, responsible among other properties for session management, to other service providers, which trust the IdP. It also allows the service providers to operate their services without performing authentication of users themselves [78][79].

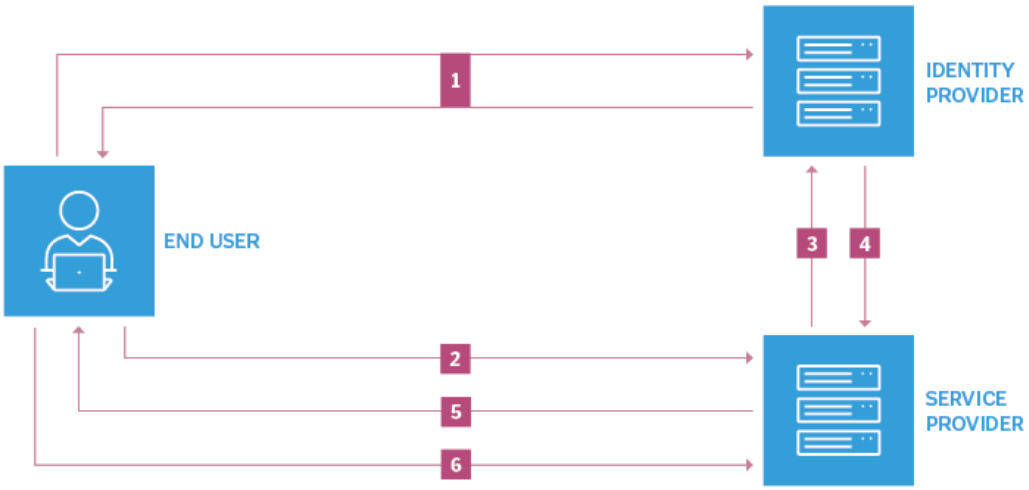


**Figure 3.6:** SAML protocol messaging for SSO login [79]

Figure 3.6 shows the six steps which are used in the SAML protocol.
**Step 1** shows the user logging into the single sign-on domain via the IdP.
**Steps 2, 3 and 4** show the user attempting to initiate a connection with the service provider. The service provider then queries the IdP, and the IdP authenticates the user to the service provider.
**Step 5 and 6** shows the service provider validating the users' identity, initiating the authentication session and the user accessing the service provider's resources.

### XACML

XACML is an abbreviation which stands for "eXtensible Access Control Markup Language" and represents an XML based language for defining access control policies [80]. It allows declaring fine-tuned, attribute-based access control policy languages that determine who is allowed to do what in an organisation. It also includes request/response mechanisms that contain queries about access levels. Another component of XACML is reference architecture. It represents an arrangement standard for necessary software modules within the XACML infrastructure to ensure the most efficient enforcement of defined policies.

### OAuth 2.0

OAuth is an identity management protocol used to authorise users and applications to various platforms and websites [81]. It provides secure delegated access and allows the third party to gain access to the resource without sharing the credentials with the help of a token that defines the level of access by the scope parameter. However, OAuth works only with known clients and requires additional mechanisms to authenticate unregistered or unknown clients securely.

There exist several roles in the OAuth 2.0 authorisation dialogue [82]:

- **Resource owner** end user who can grant access to the requested resource.
- **Resource server** hosting the protected resource server.
- **Client** the application that requests the protected resource. In the case of machine-to-machine communication, the client and the resource owner is the same entity.
- **Authorisation server** the server that issues authorisation tokens

OAuth 2.0 provides multiple authorisations flows, which represent different ways of retrieving authorisation tokens [83]. Factors that can influence the choice of the flow include mentioned above client, and the resource owner is essentially the same entity if the client is a web application hosted on a server, how trusted the client is with the user credentials, or if the client is a mobile application or a single page web application.

### OpenID Connect

OpenID Connect is an additional identity layer for OAuth 2 and handles the user's authentication [84]. OpenID Connect does not require users to share credentials to get authorised to a server. Instead, in the authentication phase, a client would authenticate to an IdP, using obtained credentials to authenticate the user in other accessed platforms.

One of the most valuable features OpenID Connect brings to authentication is a set of scopes for the user's identity [85]. Scopes represent a set of credentials that are returned as a user attribute set defined for each particular scope. This facilitates the administering of connections to various platforms and enables interoperability.

Figure 3.7 represents the typical authentication flow of the OpenID Connect protocol. It starts with the User-Agent requesting a resource on the OpenID Connect Relying Party. The Relying Party contacts the IdP with the authentication request. The IdP provides a form for the user to authenticate, where the user inputs credentials. After the authentication, the IdP shared necessary user information with the Relying Party to complete the access.

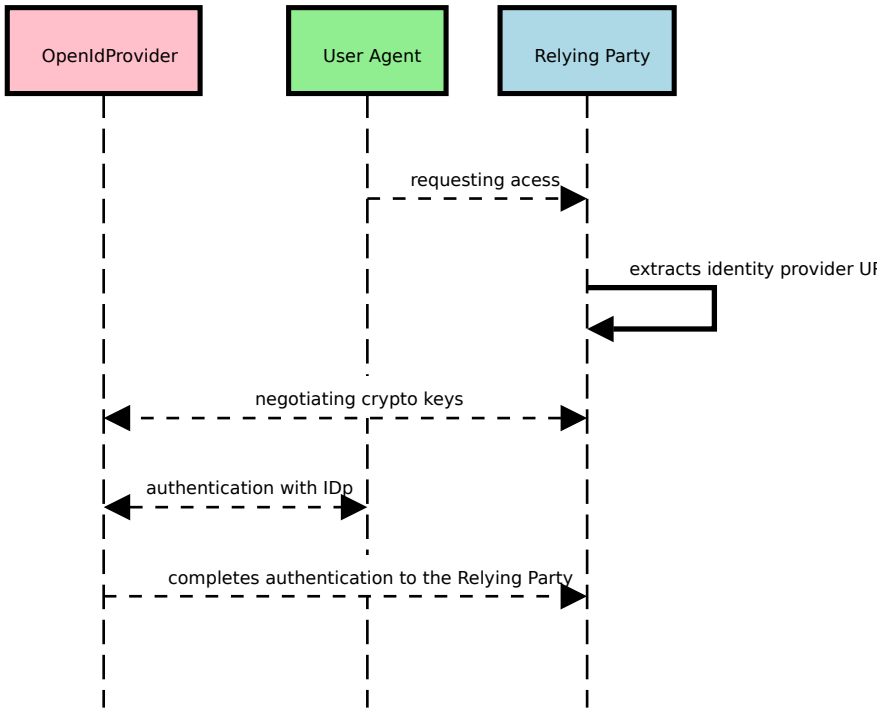


**Figure 3.7:** OpenID Connect authentication flow

Implementing OpenID Connect together with OAuth 2 completes the Identity and Access management of a user.

### RADIUS and Diameter

Remote Authentication Dial-In User Service (RADIUS) and Diameter are examples of Authentication, Authorisation, and Accounting, so-called AAA framework. They were developed for remote access via a network with the help of authentication, giving an authenticated entity rights through authorisation and keeping track of the performed actions using accounting.

RADIUS [86] is a protocol that enables Network Access Server (NAS) to communicate with the centralised server for user authentication, authorisation and further accounting phases. In RADIUS, a connection point between the user and AAA servers can be NAS or WAS (Wireless access point). The latter is used for users connected to a wireless access point supported by AAA RADIUS. The protocol was initially used to enable dial-up and terminal server access. However, constantly growing demands, driven by the growing complexity of networks and a growing number of applications, led to a new development in the AAA framework. One of such new protocols RADIUS has evolved into is Diameter.

Diameter [87] is a next-generation AAA protocol, which brings several improvements to the existing RADIUS implementation: it is a peer-to-peer protocol that allows anyone to start a conversation, whereas RADIUS is a strict client-server. In addition, authentication in both RADIUS and Diameter supports access rules and authentication restrictions. Diameter also supports periodic reauthentication and reauthorisation on-demand.

### Kerberos

Kerberos is a network access protocol which works based on tickets and is used for secure communication over an insecure network [88]. Built on the symmetric key cryptography with the central element - a trusted third party that handles ticket management and authenticates servers to users and vice versa.

To prevent loss of confidentiality and tampering with the data sent between parties involved in an authentication dialogue, Kerberos provides a cryptographic encryption type. It establishes a shared secret between the parties. Focusing on encryption, Kerberos provides a variety of algorithms to protect communicating parties [89].

Kerberos protocol is used to authenticate principals or participants of the authentication dialogue. A principle can be a client, a server, an application or any other network entity willing to communicate securely with another party on the network. In an inter-organisational scenario, Kerberos requires a particular setup called CrossRealm Kerberos Authentication Operation [90]. However, the solution is prompt to issues since lack of scalability brings issues like downtime and vulnerabilities in the possible implementation: man-in-the-middle vulnerability, authentication chain unreliability, and exposure to DoS attacks, among others.

The benefit of using Kerberos in the information sharing scenario lies in being application-agnostic. It means that the protocol can provide an authentication layer to the applications and entities that do not implement it on their own. Another solution for Kerberos used for both web and non-web applications is the feature of sending the assertions of one type through the protocols of another type, with the condition that the receiver can receive and decode them. This requires a hybrid setup, and Federated Kerberos (FedKeb) can provide support in the administration of such a setup.

#### LDAP

The Lightweight Directory Access Protocol is a lightweight version of the Directory Access Protocol which runs over the TCP/IP stack. It is a part of the X.500 standard, which is a standard for hierarchical directory services in networks [91]. LDAP have fewer features than DAP; however also requires fewer resources and offers fast read times, scalability and ease of work. Unlike other Internet protocols, it provides an API that simplifies writing Internet-based applications using directory services [92]. It is well-defined and has documentation, namely RFC4511 [93], which enables developers to encode requests and responses to use LDAP. The connection is persistent compared to other HTTP-based protocols, often short-lived, allowing the connection to be hours, days or longer.

It is possible to implement LDAP in different ways depending on the need for the application. However, every schema must include attribute syntax defining: the type of data represented, matching rules defining the comparisons that can be performed on the data, attribute types defining the named units of the information stored and object classes which define the named collections of attributes [94]. In addition, the schemes offer additional elements which can be used.

#### SCIM

System for Cross-domain Identity Management [95] is an open standard like SAML, but focus on identity provisioning and management for cloud-based environments. This allows a company to create a new user in their cloud environment and SCIM can then provision the user to other cloud applications like mail, communication and file sharing platforms that are used within the company.

## 3.4 Requirements from Identity and Access Management

The need for an Identity and Access Management (IAM) deployment comes from various sources (compliance policies, risk management etc.) Nevertheless, the successful implementation of solutions for managing users depends on the correctly

formulated requirements of the system. Table 3.1 represents a summary of the requirements collected from the digital identity management stages discussed in Section 3.1 and features of identity management protocols analysed in Section 3.2 and Section 3.3. The indexation of each requirement in the table below is 'IAM' plus a numerical value, as it concerns Identity and Access Management and provides more clarity to the reader.

| Index | Name | Category | Dependency | Reference | Reason |
|---|---|---|---|---|---|
| IAM1 | Provisioning | F | | 3.1.1 | Digital identity defines what role and access rights a user will get during the following stages of using the requested resource |
| IAM2 | Authentication | F | IAM1 | 3.1.3 | Set of claims presented defines if the user/entity is who they claim they are |
| IAM3 | Authorisation | F | IAM1 | 3.1.3 | System has to grant access rights to the user based on the assigned permissions |
| IAM4 | Role management | F | IAM1 | 3.1.3 | To ensure that only the user has correctly assigned permissions to use a resource or access the file |
| IAM5 | Session management | F | IAM2, IAM3 | 3.1.3 & 3.3 | To manage interaction between the user and the system in a secure way |
| IAM6 | Privacy for identities | NF | IAM1 | 3.2 | Implementation pf principle of least privilege principles of data limitation |
| IAM7 | Multifactor authentication | F | IAM1, IAM2 IAM4, IAM5 | 3.2 & 3.1.3 | Introducing additional factor of authentication to enhance security of the platform |
| IAM8 | Attribute management | F | IAM2, IAM4 | 3.1.3 | Assigning roles and privileges to correlating entities based on the set of presented attributes. Ensuring freshness of user's role and ensuring policy enforcement on those attributes and roles |
| IAM9 | Single sign-on, single sign-off | F | | 3.2.1 | User can securely authenticate by providing only one set of credentials |
| IAM10 | Support identity federation | NF | IAM1, IAM10 | 3.2.2 | Enabling user-friendly and secure operation for multiple entities |
| IAM11 | Anonymous access | NF | | 3.2 | A user should be able to get access to the system without being registered and logged in |
| IAM12 | Access logging and monitoring | F | | 3.3 | To have an overview of who is accessing and performing actions on the platform |

**Table 3.1:** Potential system requirements based on Section 3.1

## 3.5 Summary

A robust identity and access management solution with strong authentication and authorisation processes must be in place, considering the sensitive data the plat-

form will contain. Accessibility remains a top priority for identifying and authenticating entities. Therefore, information sharing solutions should authenticate based on a multifactor authentication scheme, which implies processing various authentication factors.

In regards to authorisation scheme, we consider ABAC authorisation to be the one offering both flexibility and generality.

The main goal of Section 3.3 was to find one or more protocols that would fit the information sharing platform use case. From the presented protocols, we can conclude that considering the number of players sharing the information, there may not be one protocol that all entities will unanimously use. Therefore, at this stage of the project, the most suitable solution is for the system to support multiple protocols of various levels of user federation and sign-on requirements.

Identity and Access Management is an essential part of any platform or system. It refers to both technical (architecture, protocols, security) aspects and non-technical (usability, user experience).

# Chapter 4

# State of the art

This chapter provides an overview of current solutions and challenges related to information sharing. Using literature review Section 2.2.1), we gathered related literature on information sharing and awareness. Altogether, we deemed relevant six papers from the **IEEE** public library, three **Science Direct** publications, two publications from **ACM**, one from **Taylor and Francis** Library, two journal articles and two university reports. Awareness and its importance in information sharing are presented in Section 4.1. Additionally, the motivation for IS and problems that emerged around it is explained in (Section 4.2). Lastly, we conclude with a requirements list generated based on the prior sections.

## 4.1 Awareness

The following section will look into the importance of awareness in terms of cyber security: different kinds of awareness for information gathering, some of the current solutions and challenges.

### 4.1.1 What is cyber security awareness?

Cyber security awareness has multiple elements, including awareness for employees, the security department and the internal network [96, 97]. The internal traffic awareness spans knowing what happens in a system at a given time. The logging system's activity provides an overview of every action taken by users and what network traffic flows in the internal systems and incoming and outgoing traffic. By logging and supervising every step from the machine used, the routers and switches, the firewalls, intrusion detection systems to intrusion prevention systems and more, user actions and traffic can be monitored. These logs can be analysed by various security products and can also be sent to a Security Information and Event Management (SIEM) system. SIEM systems can gather logs from various sources

and include customised alerts that can trigger the security team rather than reacting to every security warning from every security product. Such security products are often based on signature-based solutions, meaning they require that the threat or something similar has been seen before. Otherwise, the threat may evade detection and prevention. Anomaly-based detection methods are also introduced into the field and base their detection on the activities performed to determine if they are expected or not.

Being able to detect threats with technical solutions is beneficial and has improved. Security features are built into operating systems and software, which means these are better protected against cyber threats. The increased security in the applications leads attackers to shift their focus to the people using these applications, and thus awareness for the employees is required [98]. Proper awareness allows the person operating the systems to understand and report potential security risks. It can prevent employees from, for example, opening malicious links and using malicious USB devices. However, this awareness method has its challenges, and the remainder of this section will focus on awareness for an individual rather than technical aspects.

### 4.1.2 Challenges

Awareness training for employees is crucial to sharing information within an organisation. However, while important, cyber security awareness has proven challenging to accomplish. According to a survey conducted by SANS, a U.S. based cyber security company, lack of time was the biggest challenge for companies, together with lack of personnel, as shown in Figure 4.1 [99].


**Figure 4.1:** Results from SANS survey about challenges with awareness programs and training [99]

While Figure 4.1 shows many challenges regarding time, budget and bureau-

cracy, the inability to engage employees also poses a challenge for the awareness personnel. This challenge plays a crucial factor in how the employees or participants in the awareness training program perceive and absorb the knowledge gained. The methodology used to deliver the training content is vital for the effect this may have. A paper by **Abawajy [100]** discusses different delivery methods which can be used for awareness training. The consensus is that the delivery method should appeal to participants with varying knowledge, from general users to super users. Some participants may use email and generic applications as they may be working in production. In contrast, information technology users often use Internet and different applications in their daily work.

In addition to the varying base knowledge, awareness training should also engage the participant to activate them and show real-world scenarios using games, web-based applications, or real simulations. An example of this can be phishing attacks being sent and the employee having to determine and react to whether the email is phishing or not. A study by **Kumaraguru et al. [101]** shows that simulation-based training followed by follow-up notifications improved the participants' ability to detect phishing mail better than using conventional delivery methods like pamphlets or other paper-based delivery.

### 4.1.3 Current solutions

There exist different products that conduct cyber security awareness training. Solutions like ProofPoint [102], Microsoft cyber security awareness training for Office 365 [103], PhishGuru [104], to mention a few. **Stephen Hart et al. [96]** introduce the concept of learning cyber security awareness via a simple board game, customised based on the organisational work condition, for both students with cyber security background but without experience and staff lacking technical background. The difference this solution proposes in comparison to other awareness programs is the possibility for the users to try and understand the defender perspective, the 'blue team' and the 'red team' adversary perspective. In addition, it is possible to customise the board game environment based on the organisation's own and it that way make it more familiar to the employees. Using current solutions for awareness training rather than creating custom solutions for each company can aid in the lack of time and lack of personnel. These solutions have to be set up, which requires personnel's time. However, it can lower the effort required as they are designed for these scenarios.

These solutions offer various options, from phishing simulations to video material that participants can watch. The videos and simulations prepare the participants on how to act in case of a cyber attack. One example is the ability to report phishing emails directly in the email application Outlook, which can be used as the awareness training to give practical experience.

### 4.1.4 Awareness for information sharing

The aforementioned awareness solutions enable the user to better react to security threats and thus report these to the security department. Having the knowledge that users inform allows the security department to set up security measures that may prevent such threats in the future.

As mentioned in Section 4.1.2, some of the challenges that awareness personnel encounter include a lack of time and money. These factors encourage the problem delimitation of this project, mentioned in Section 1.3.3. Enabling information sharing across companies and sectors allows for a broader knowledge base as it does not depend on one company but multiple. While some sectors have central organisations to share and discuss cyber security incidents Section 1.3, it is hard to find evidence that it is shared across sectors.

## 4.2 Information sharing

In this section, we unfold the essence of information sharing. We review why it is not easy to implement IS and what current efforts have been done in this area. The latter will focus on IS platforms, their functionalities and security measures, thus potential requirements for our system.

### 4.2.1 Challenges

In order to design the right technical solution, one needs to understand why information sharing is a challenging topic and what are the motives to share. **Koepke [105]** analyses which incentives motivate companies to share cyber threat-related information and which obstacles make information sharing unattractive to organisations. Eight of each are identified in the study; however, the majority have both a positive and a negative context, depending on the situation. For example, legal motivation and protection are deemed as encouraging, where fear of breaking the law or legal agreements by improper disclosure is considered a barrier. Other deficits described in the paper are lack of trust between firms, inability to efficiently process shared information and lack of technical compatibility. Interestingly, similar challenges have been identified in older research by **Mallinder et al. [106]** and NIST Guide for information sharing [107]. This shows that despite time progression, some problems are yet to be solved. As an outcome, **Koepke's** study resolves on legal protections and gaining awareness as the most significant incentives for sharing information.

**Rizov [108]** presents some of the overall benefits of collaborative threat and information sharing between organisations under the concept of *'one organisation's detection becomes another's prevention'*. In addition, the study touches upon the most

useful information to share and potential difficulties present in establishing and using such a platform (see overview in Table 4.1).

| **Inter-organisational Information sharing** | | |
|---|---|---|
| **Benefits** | **Challenges** | **What to share** |
| increased awareness | establishing trust | IOCs (suspicious IP, DNS, file names, sizes, hash values) |
| better understanding of threats | interoperability, lack of normalization | security alerts |
| gaining collective knowledge | protection of sensitive unclassified data | configurations |
| collective imunity | protection of classified data | TI reports (actors, etc.) |
| building defense agility | feeling in control of one's data | procedures, strategies, best practice |

**Table 4.1: Rizov [108]**: insights to collective information sharing

**Skopik et al. [109]** review different areas related to information sharing. The research looks at legal obligations and the different platforms which only provide partial solutions to the problem. Nevertheless, relevant facts from the paper are useful for our research, demonstrating considerations for not only punctuality but also the efficient framework and five-dimensional conceptualization for information sharing systems, we have interpreted it to apply to our report, see Figure 4.2.


**Figure 4.2:** Information sharing dimensions inspired by [109]

### 4.2.2 Current solutions

This section navigates through related literature and research done around information sharing platforms. Moreover, we explore the capabilities of the **MISP** platform in particular. Lastly, we look at the information exchange protocol **TAXII** and a framework designed not only for information exchange but also to improve situational awareness in organisations **PROTECTIVE**. To understand the usability and common functionalities of each, we will look at these implementations and compare them across different parameters in Section 4.2.2.

#### Related work solutions

- **The collaborative group-centric information sharing framework** (CGCF) was firstly introduced in 2012 by **Zhao et al. [110]**It is based on the group-centric access model [111], where each group falls under a well-defined authorization policy and groups are independent and isolated, meaning they can not influence each other's privileges in any matter. We deemed this research relevant as it proposes a similar architectural structure to the one we aim to achieve in this project (see Figure 4.3). Moreover, there have been several additional efforts and improvements to the research, as presented further. The authors state system shortcomings clearly. One of them is the requirement for system administrators to assign which sector groups should be allowed access to incident information. The disadvantage of this approach is the lack of automation in the critical timeframe of incident reporting. For access levels research proposed the Chinese Wall policy [112]. However, this

approach still requires additional handlers to avoid conflicting access policy situations. **Zhao et al. [110]** express the importance of privacy but do not state any particular mechanism in the design that, for example, results in missing authentication features. In 2014 **Zhao et al. [113]** published a complementary requirement list to this framework, clarifying information sharing flows and scenarios featuring, among others, awareness (Figure E.2).

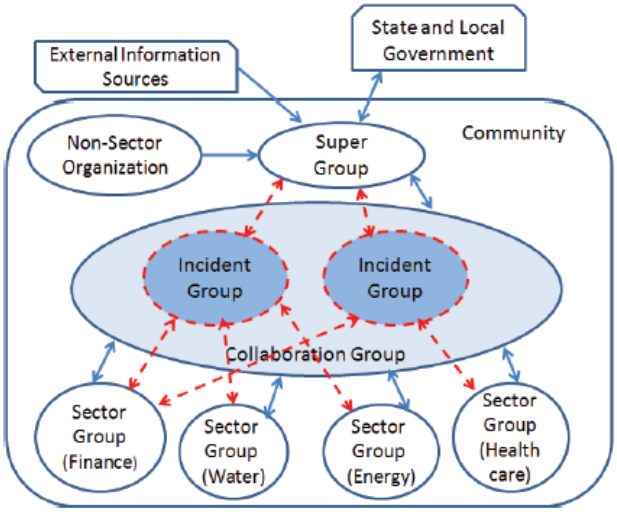


**Figure 4.3:** Architecture of collaborative incident information sharing system [110]

In 2017 **Zhao et al. [114]** revisited this project once more, not to present technical improvements to the framework (which are lacking see Tables 4.2 and 4.3), but to update the proposed architecture (Figure 4.3) by extending it with information exchange with Emergency Operation Centers (EOC) intermediated through Fusion centre (Figure E.3). The contribution from the paper is a thorough analysis of maturity levels of IS dependencies like management, technology and policy. The paper describes different use of the system in scenarios, the evolution of information sharing engagement maturity model Figure E.4, policies accompanying IS on each maturity level, steps and procedures which will serve as inspiration for our proposal.

- **Cybersecurity Information Exchange (CYBEX)** is an attribute based information sharing system proposed by **Vakilinia et al. [115]**. Traffic Light Protocol (TLP) is deemed inadequate in this work as it does not perform well when involving semi-trusted sharing servers. Instead, research suggests using CP-ABE (Ciphertext Policy Attribute based Encryption) to authorise access to confidential or sensitive information. In other words, only the users with adequate access attributes will be able to decrypt the information. The attributes are organised as a tree structure. The solution is built based on

CYBEX framework, and the Structured Threat Information Expression (STIX) language is further explained in Section 7.5.2. For user registration, the proposed work suggests, as a good fit in terms of efficiency, the Elliptic Curve Digital Signature Algorithm (ECDSA) digital signature scheme.

- **Sholihah et al. [116]** writes about development of an **Information Sharing and Analysis Center (ISAC)** system based on Design Research Methodology [117] and several testing approaches, including Prototype testing. The outcome is a web-based platform utilising MISP for handling threat information and visual representation of data input. The system was essentially built, fulfilling five functional and two nonfunctional requirements. It needs to be said, the requirements in this research are very general, and if one would like to reproduce the process, it would need more than those requirements to achieve a fully functional system. On the other hand, this lack is complemented by a series of well-described diagrams showcasing the use cases and architecture of the system. The highlight of the paper is security testing performed on the final product, where the system persisted brute-force attempts thanks to 2F authentication but was not invulnerable to XSRF (Cross-Site Request Forgery) and XSS (Cross-Site Scripting). Positively, **Sholihah et al. [116]** state possible mitigations to both.

- **Sadique et al. [118]** created a **CYBEX-P** privacy-enhanced cyber security information sharing platform employing multiple data and user protection mechanisms. The collected data is stored in either cache and encrypted with public key cryptography or in the archive and encrypted using symmetric encryption. To anonymise data, CYBEX-P utilises a technique called Blind processing (Figure E.5), where cyber threat reports are produced, removing any indicators concerning the source of processed information (see Figure 4.4). The study by **Sadique et al. [119]** shows the advantages of CYBEX-P specific graph-based cyber threat language TAHOE developed to translate data into the normalised format, support privacy and speed of data analysis.

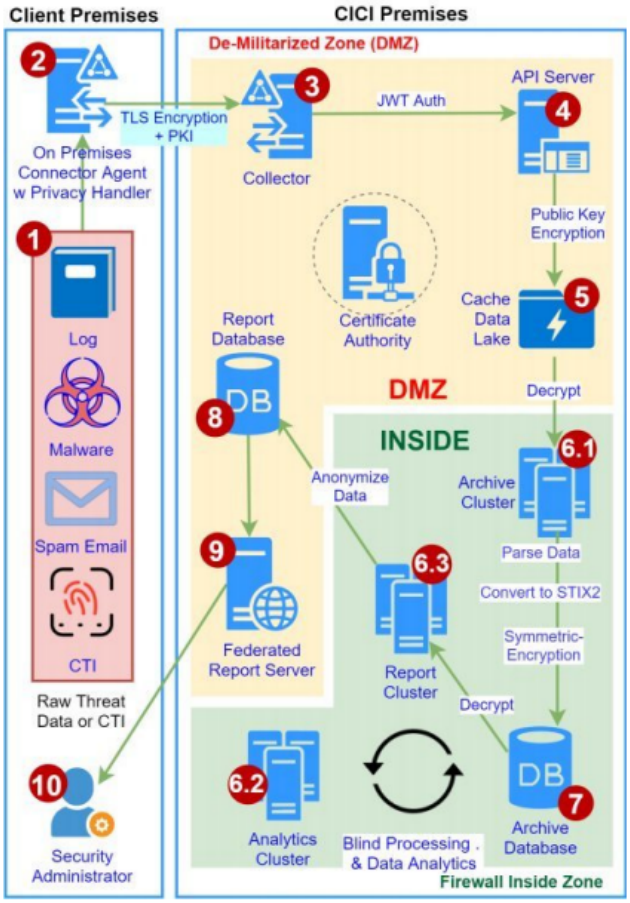


**Figure 4.4:** Architecture diagram of CYBEX-P [118]

- **PRACIS** is an information sharing scheme focusing on the privacy of information transferred designed by **Fuentes et al. [120]**. It is built onto the STIX standardised language and uses encryption mechanisms like homomorphic encryption[121] and format-preserving encryption[122] to protect against linking incident and entity publishing it. This precaution is implemented based on the assumption that any server within the information sharing network connected to PRACIS can be potentially compromised but attacked would not be able to leverage privacy-critical information. The proposed scheme performs well when it comes to the speed of creating, verifying, processing and decryption information taking just milliseconds. The information exchange is based on the publisher-subscriber model, and verification of the information is done via HMAC.

**Other solutions**

- **MISP**, an opensource software created and maintained by CIRCL is currently used by a variety of different organisations, among others, NATO and the EU [123]. MISP enhances malware detection software by utilising knowledge collected via sharing threat information such as IoCs, attack vectors, etc. To protect information disclosure MISP [123, 124] offers different access levels defining end-user(s)/group(s) to whom information becomes accessible. Information sharing can be restricted between parties by assigning one of four possible set-ups: 1) intra-organisation or CERT only sharing, 2-3) within one or more group(s) sharing, where the group is a list of communities, industrial sectors or network of connected CERTs, and 4) sharing to all communities. In addition, it leverages the TLP, which classifies information on four levels, from strictly restricted content to public content, as follows: RED - Personal for Named Recipients Only; AMBER - Limited Distribution; GREEN - Community-Wide; WHITE - Unlimited [125]. Users can access data via API, which can be exported in a variety of formats from MISP XML to STIX, JSON and even IDS-specific formats like Suricata or Snort [123].

- **TAXII** is protocol-based application for the collection and sharing of CTI. It implements DNS for server identification and HTTPS for secure information transfer, supporting different formats, including STIX. As for sharing models, it is possible to establish a peer-to-peer connection, publisher and subscriber, and hub-spoke connections [126]. Despite securing information transfer TAXII on its own does not handle attribute based access level controls.

- **PROTECTIVE** is designed for NREN to exchange threat information with external CSIRTs and fulfil the functions of the Security Situational Awareness Manager. It presents a series of requirements in its documentation based on a similar methodology to this project. Therefore, we deemed it relevant to include it in the state of the art section despite not being in the thesis literature review. The fact that over 4 million euro was dedicated by the EU project Horizon 2020 [127] to research and create such a framework just emphasises the European efforts and demand for better information sharing solutions. PROTECTIVE documentation [28] lists relevant concerns and observations for the system design. To name a few, information types compatibility, legal requirements to secure compliance with NDAs and GDPR. In addition, awareness as an important factor in better threat intelligence is underlined. Concerns about sharing malware data containing illegal material are also raised in the document [28]. The features included in PROTECTIVE are mostly about alert handling and utilisation, supporting automation of rule-based ticket creation, data management and reporting (see more in

Table 4.3). Figure 4.5 depicts data handling operations involved in an information sharing flow. Data anonymisation and categorisation according to rules and TLP user authentication are present as part of the process.

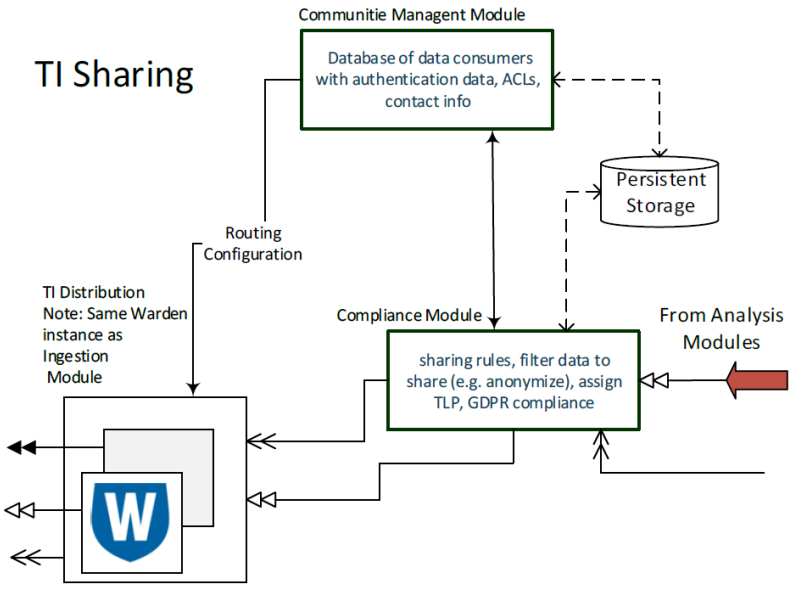


**Figure 4.5:** PROTECTIVE sharing information flow [28]

### Summary

In **Section 4.2.2**, we have presented 8 different frameworks, all connected by the main functionality, sharing incident and threat-related information implemented in one way or the other. We will look at common dimensions of the systems based on the sources presented for each. Table 4.2 compares different systems based on the format of the information, access control mechanism, data classification schemes and data encryption methods. Out of all data formats, STIX is by far the most populated. Only two systems offer more than one data exchange format or language by default. When it comes to access controls, Attribute based seems to be a common approach to several solutions, while the rest either implements something else or does not mention access control at all. Data classification can be done in many ways but based on our selection of systems, the division between sensitiveness and disclosure levels (TLP) prevails. Lastly, all but one system provides encryption to protect information shared.

| IS system title | Dimensions | | | |
|---|---|---|---|---|
| | **Language/ data formats** | **Access control** | **Data classification** | **Data encryption** |
| **CGCF** | N/A | g-SIS, The Chinese Wall policy | sensitive/public, threat alert/levels | N/A |
| **CYBEX** | STIX | CP-ABE, Access Tree | TLP, sensitive/ non-sensitive | Yes |
| **ISAC** | N/A, plans to use STIX in future | N/A | threat level, vulnerability level, warning level | HTTPS |
| **MISP** | STIX, JSON, MISP XML/ JSON, others | Trust-groups, Attribute level distribution | TLP, tags | PGP encryption |
| **TAXII** | STIX | No | N/A | TLS, HTTPS |
| **CYBEX-P** | TAHOE, TDQL | Attribute based access control | public/private data attributes | TLS |
| **PRACIS** | STIX | N/A, subscriber mechanism instead | sensitivity levels | Format-preserving encryption |
| **PROTECTIVE** | IDEA | Yes | sensitive/ non-sensitive | TLS |

**Table 4.2:** IS systems compared on data manipulation and access solutions

In Table 4.3, we can see a feature list of each IS system. Needless to say that features are tightly connected to the specific purpose of the system meaning whether it is focused on analysis or pure data transition. Another factor influencing the feature list is the type and nature of the information exchanged and processed. Amongst the most populated can be seen TI data and IoCs. The leftmost column describes the security mechanism established to protect that information with the system. All but one, CGCF provides several security mechanisms from anonymisation and encryption to authentication.

| IS system title | Dimensions | | |
|---|---|---|---|
| | **Security mechanism** | **What can be shared** | **Features** |
| **CGCF** | N/A | warnings, alerts, threats, incidents, vulnerabilities, response activities, response capabilities, awareness, mitigation strategies | connect with group, add/remove/update objects, join/leave group, import/export information |
| **CYBEX** | ECDSA digital signatures, key distribution center | CTI, system configurations, zero-day vulnerabilities, users' private information, blacklisted IPs | registration, sharing, access, |
| **ISAC** | 2F authentication, OTP, HOTP | incidents, threats, vulnerabilities, warning indicators, cyber security training | display attack/threat list, complain form, admin data update, login, 2F authentication |
| **MISP** | integrated encryption, signing of the notifications via PGP and/or S/MIME | IoCs, malware samples, attack/attackers characteristics | data import/export/ storage/sharing/ correlation/filtering |
| **TAXII** | HTTPS, server authentication and certificate verification (PXIX) | CTI data, CTI objects | host/share/request information |
| **CYBEX-P** | symmetric encryption(AES256), key management system, PKI | spam emails, raw threat data, phishing URLs, SSH logins attempt, firewall logs, | store/share/collect/analyse data, login, alert/report, register, visualize incidents, phishing URL detection |
| **PRACIS** | homomorphic encryption, message verification | incidents, Courses-of-Action, IoCs, | message forwarding, data aggregation, STIX message generation, data subscription |
| **PROTECTIVE** | anonymisation, authentication, GDPR and compliance modul, authorization | alerts, TI, URLs, risk awareness, information from monitoring systems, IP addresses, MD5 hashes | data collection/sharing/filtering, trust related analysis, object linking, alert prioritisation/ normalisation/aggregation |

**Table 4.3:** IS systems comparison across security, information shared and features

### 4.2.3 Requirements from Information sharing related work

The following list of requirements Table 4.4 was created based on the collected knowledge discussed in Section 4.2. The functionality traits of IS systems inspired a majority of the functional requirements. At the same time, the necessity of trust and security is discussed in the challenges bound to information sharing projected in non-functional requirements. The result is 21 potential requirements for an information sharing platform where half are dependent on at least one other requirement (Dependency' column). The ' Reference' column presents the link between the requirement and its initial source, while the 'Reason' column contains the reasoning for the requirement. Index and Name can be found in the same named columns. The index *IS*, is derived from the Information Sharing section. The column 'Category' assigns whether the requirements fall under functional (F) or non-functional (NF).

| Index | Name | Category | Dependency | Reference | Reason |
|---|---|---|---|---|---|
| IS1 | Legal agreement | NF | | [28, 105] | To limit data dissemination |
| IS2 | Establish trust | NF | IS1 | [28, 105] | Trust can increase sharing |
| IS3 | Data usability | NF | IS4 | [28, 105] | Parties are able to further utilise their data (in firewall settings, procedures, etc.) |
| IS4 | Information in unified format | F | | [28, 105, 108, 118] | To support compatibility of data utilisation for different parties |
| IS5 | Protect sensitive data | NF | IS13, IS18 | [108] | To avoid leaking data that could corrupt party's reputation |
| IS6 | Sharing IoCs | F | IS12, IS21 | [108] | System needs to be able to handle log formats and other formats IoCs can be represented in |
| IS7 | Sharing additional data | F | IS12, IS21 | [108] | System needs provide option to share data like: Procedures, best practices, Security alerts, CTI reports |
| IS8 | Control of the data | F | IS11 | [108] | Provider needs to be able to edit/delete data shared |
| IS9 | Sharing groups | F | IS10, IS12 | [110, 123] | Sharing parties can access data shared from their own group |
| IS10 | Selective choice of data receiver | F | | [110] | Provider can define the receiver of the shared data |
| IS11 | Access authorization | F | IS12 | [110, 115] | In order to access confidential data sharing party needs to be authorised |
| IS12 | Sharing party registration | F | | [115] | Sharing parties need to register in the system |
| IS13 | Information encryption | F | | [115, 118, 120] | To protect data from being abused encrypt it, to protect against incident linking |
| IS14 | Use MISP for data handling | F | | [116] | To process threat data integrate MISP |
| IS15 | Secure system against CV | NF | IS5, IS11 | [116] | To make system resilient to common vulnerabilities like (XSS, MITM, etc) |
| IS16 | Store data | F | | [118] | Provide persistent storage |
| IS17 | Secure data storage | NF | IS16 | [118] | To prevent abuse of store data, data leakage |
| IS18 | Anonymise data | NF | | [28, 118] | To remove sensitive data, to protect against linking incident |
| IS19 | Verify data integrity | F | | [118] | To ensure that data was not tempered with |
| IS20 | GDPR compliance | NF | | [28] | To ensure legal requirements applicable to system by GDPR |
| IS21 | Data transfer | F | IS13 | [110, 118, 126] | System needs to be able to send data from provider to receiver |

**Table 4.4:** Potential system requirements based on Section 4.2

# Chapter 5

# Stakeholder involvement

This chapter introduces stakeholder involvement to create a framework for information sharing in the Danish critical infrastructure. In addition to exploring the stakeholders, this section will also include questionnaires and interviews conducted.

## 5.1 Stakeholder analysis

Including potential stakeholders in the system's design is an important component of requirement engineering (see Section 2.2). In order to identify the target group for questionnaires and interviews, we needed to determine, firstly, the stakeholder domain (Section 5.1.1) of where such a stakeholder can be found and, consequently, who such a stakeholder can be (Section 5.1.2).

### 5.1.1 Stakeholder domain

The stakeholder domain can be drafted based on the project scope (Section 1.3.3). For the stakeholder domain, several areas can be considered, including critical infrastructure in Denmark, Incident reporting in Denmark, and Incident handling and management in Denmark (see Figure 5.1). The organisation might not necessarily have headquarters in Denmark, but as long as it operates in the critical infrastructure in Denmark, it is considered a stakeholder in this research. Similarly, not all companies belonging to one of the sectors are under the same regulations as essential operators but still fall under critical infrastructure. Nevertheless, to follow the scope, we interviewed both groups. For the authorities, the only criterion was for them to be involved in the information sharing process or regulate it. That would also include information sharing hubs like DCIS or CERTs/CSIRTs, but to simplify, we refer to them as the 'authority group'. Our only criterion for IT security companies was that they work with information sharing or are involved in

procedures prior to information sharing. Public, investors and vendors were considered out of scope. Hence, the focus was on the critical infrastructure, security providers who may be in charge of incident management, and the authorities.

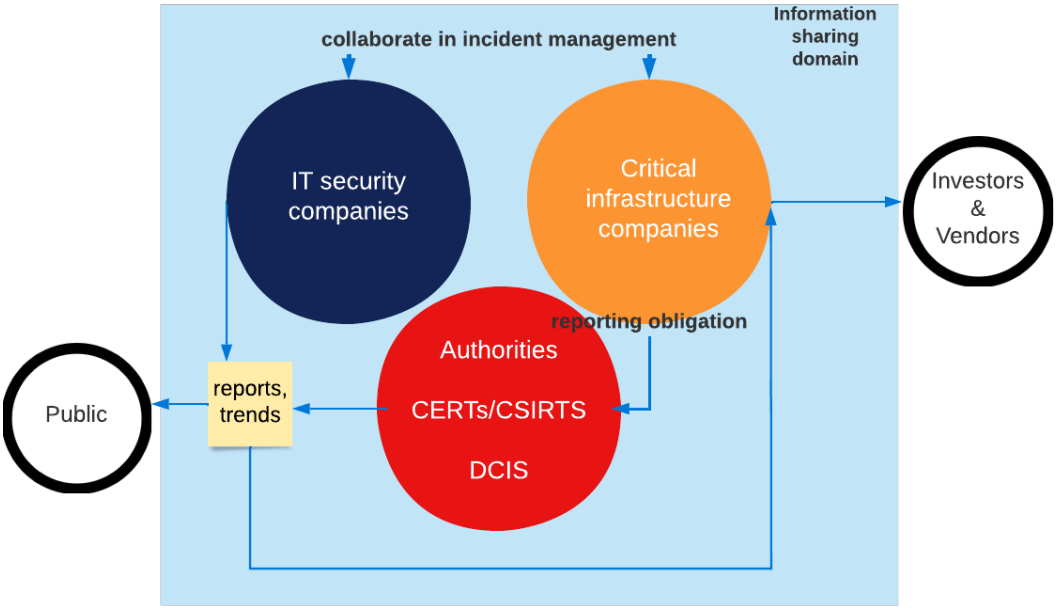


**Figure 5.1:** Stakeholders of information sharing in Denmark

### 5.1.2 Target group

As indicated in the previous section we identified three distinct groups in our stakeholder domain: critical infrastructure, authorities and IT security companies. For each of the three stakeholder groups (Figure 5.1), we recruited only people who worked in incident management, information sharing or IT or equally relevant departments. As the recruitment in most cases happened through referrals (see Section 2.2.3), we can not directly control the person's position, but we could define the preferred area.

## 5.2 Questionnaires

The incentive behind the questionnaire is, as described in Section 2.2.2, to collect quantitative information, help us understand the current situation and support or contradict some of our assumptions (Section 1.3). We have asked five questions (see the complete questionnaire form in Appendix A). All questions were multiple-choice, mostly Yes/No-questions, designed to avoid ambiguity.

Narrowing the questionnaire down to five questions in easy to answer form was a deliberate choice to reduce our target group's burden of responding [128]. In addition, events happening at the time of research, namely the war in Ukraine, which globally impacted many organisations, was a concern. Finally, since most of our target group are critically important employees in leading positions, it was essential to minimise the time required from respondents to participate.

Another element taken into consideration was privacy. Both companies and employees may want to stay anonymous and do not want to answer sensitive questions. Therefore, the questions were made rather broad not to require any participants to go into detail and avoid disclosing sensitive data.

Moreover, by contacting potential respondents to gain answers to the questionnaire, we have created a natural opportunity for us to ask about potential interest in the interview. Finally, with the questionnaire requiring low effort to complete, we hoped to give an impression that an interview would also require similarly low effort if they decided to participate.

### 5.2.1 Questionnaire questions and Results

All in all, 14 respondents representing critical infrastructure stakeholder group answered the questionnaire. In the **first question** we asked about how many incidents an organisation has experienced in the past 12 months. The reasoning behind this question was to understand how often an organisation happens to be in a situation where it might consider sharing information.

The options for the **question 1** were: *"No incidents"*, *"1-10"*, *"11-50"*, *"51-100"*, *"more"* or *"I am not allowed to answer"*. The latter option was offered for all five questions of the questionnaire to respect the potential non-disclosure policy an organisation might have. Figure 5.2 shows the results of **question 1**, where approximately 30% of the respondents experienced 1-10 incidents. Another third was not allowed to answer this question. Curiously, about 14% answered that they had no incidents at all, raising the question of how they define an incident. The rest experienced more than 11 incidents in the past 12 months.

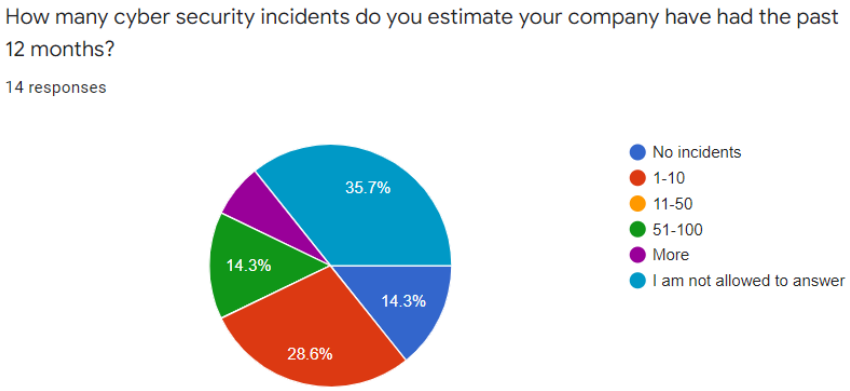


**Figure 5.2:** Questionnaire question 1 results

**Question 2** and **3** was about sharing incidents of different size: minor, middle, and major cyber incidents. 11 out of the 14 respondents stated that they share major size incidents, whereas only 5 out of the 14 respondents share minor and middle-size incidents with external entities, as seen in Figure 5.3 and Figure 5.4.

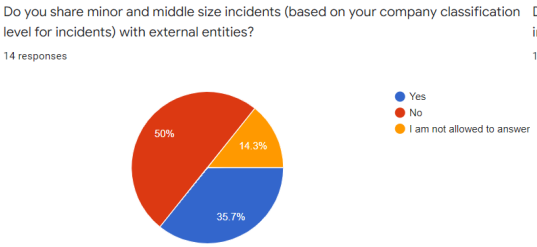


**Figure 5.3:** Questionnaire question 2 results

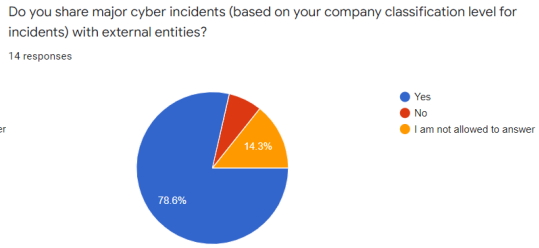


**Figure 5.4:** Questionnaire question 3 results

However, this question raised concerns among the respondents about how the different degrees of incidents, namely minor, middle and major, were defined. The original version of the question did not include "based on your company classification level for incidents". Nevertheless, this text was added for the respondents to give context for the incident classification. This fact does make it harder to compare as the degree of an incident most likely changes from organisation to organisation [129][130]. However, it also gives the answers a better indication of when they report as if we defined the degree, which could change their view on their incident levels.

These results indicate that companies share information about incidents, but the severity of the incident impacts sharing.

The **fourth question** , *"Do you have interest in other entities within the critical infrastructure sharing information regarding cyber security incidents with your company?"* was asked to measure the organisation's interest in incident information from other

organisations within critical infrastructure and was unanimously answered positively as *"Yes"* (Figure 5.5).

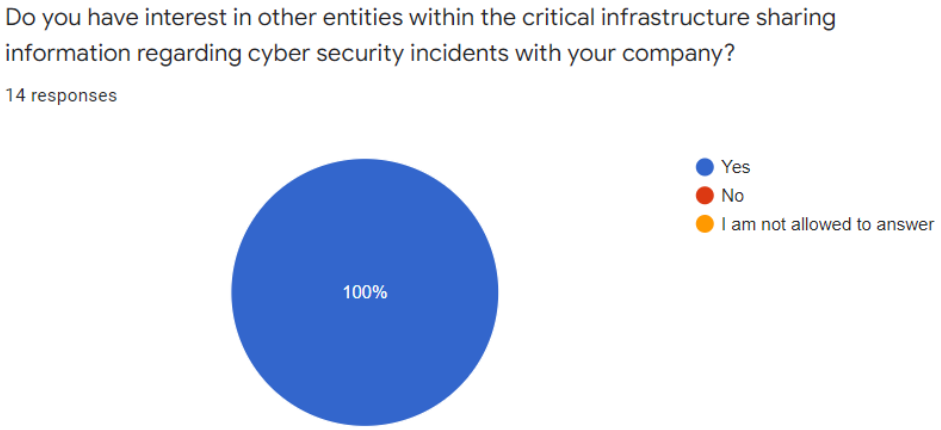


**Figure 5.5:** Questionnaire question 4 results

While most respondents are interested in sharing, many incidents are not shared with other organisations.

The same answer option was again unanimously chosen on the **last question**, number five, where we asked whether they have established procedures regarding internal incident reporting (Figure 5.6). This question was asked mainly as a precondition for us being able to ask interview questions (Interview for critical infrastructure question 5), where we further ask about the procedures.


**Figure 5.6:** Questionnaire question 5 results

## 5.3 Interviews

As presented in Section 2.2.3, we chose semi-structured interviews as the primary stakeholder involvement method. A short list of 6-7 questions with probes was designed carefully to be open but clear. As with the questions in the questionnaire, privacy had to be taken into consideration to avoid sensitive data and the risk for participants not to answer a question. The questions differ only in minor details for each of our target groups. The critical infrastructure group of respondents was the first to be interviewed and provided insights into alterations of the other two group's interview questions mentioned in Section 5.3.2. The interviews were created to last around 15 minutes, but the interview time naturally differed based on the respondent and interviewer (see the setup in Table 5.1). For each interview, only one of the researchers was conducting it at the time. That was to optimise the overall time required to conduct interviews and provide a more natural dialogue like environment for the respondent.

#### Pilot interviews

The pilot interviews were conducted before we interviewed our selected respondents. In addition, we asked the pilots to provide us a feedback for the questionnaire questions. The pilots were conveniently chosen for their work experience and availability, Pilot 1 being an Enterprise Architect and Pilot 2 being a Network Administrator. Pilot 1 commented on the subjectivity of the questions, which we objectified by, for example, replacing 'you' for 'your company'. Initially, questionnaires, did not include definitions for terms like incidents. Both Pilot 1 and Pilot 2 raised concerns for common understanding; therefore, further descriptions of those terms have been added. We settled on two pilots, as after the third one, we have not experienced a need for further modifications to both interviews and questionnaires. Thus, the third interview was treated as one of the regular interviews.

#### Interview setup

As Table 5.1 shows, we conducted most of the interviews via Teams and not physical meetings. The online setup allowed flexibility in choosing the time and place, as the respondents are located in different parts of Denmark or abroad. Additionally, the day and time were marked as this could potentially impact the answers. While it may not affect having an interview at a given time during the day, it could give biases, for example, mental fatigue [131].

The first element in every interview was to ask the respondent for consent to record the interview; however, not all respondents consented. Instead of transcribing, the interviewee took notes based on what was said. This may introduce bias, as the results of the interview depend on the interviewee and their memory and

| ID | Setup | Place | Day and time | Recorded | Sent questions | Duration |
|---|---|---|---|---|---|---|
| CI1 | Physical | Coffee shop | Fri afternoon | Yes | No | 9 min |
| CI2 | Online | Teams | Fri morning | Yes | No | 17 min |
| CI3 | Online | Teams | Thu morning | Yes | No | 17 min |
| CI4 | Online | Teams | Thu morning | Yes | No | 10 min |
| CI5 | Online | Teams | Fri morning | Yes | No | 12 min |
| CI6 | Online | Teams | Mon afternoon | Yes | No | 10 min |
| CI7 | Online | Teams | Mon afternoon | No | No | 12 min |
| CI8 | Online | Teams | Tue afternoon | Yes | No | 9 min |
| CI9 | Online | Teams | Tue afternoon | Tech. issues | No | 10 min |
| CI10 | Online | Teams | Thu afternoon | Yes | Yes | 31 min |
| CI11 | Online | Teams | Mon morning | Yes | No | 16 min |
| CI12 | Online | Teams | Fri morning | Yes | No | 15 min |
| A1 | Online | LinkedIn | Thu morning | Yes | No | 10 min |
| A2 | Online | Teams | Wed afternoon | Yes | No | 21 min |
| A3 | Online | Teams | Mon afternoon | Yes | No | 30 min |
| A4 | Online | Teams | Fri afternoon | Yes | No | 21 min |
| A5 | Online | Teams | Thu afternoon | Yes | No | 26 min |
| A6 | Online | Teams | Fri afternoon | No | No | 30 min |
| A7 | Online | Teams | Thu afternoon | Yes | No | 11 min |
| A8 | Online | Teams | Thu morning | No | No | 25 min |
| E1 | Online | Phone call | Wed afternoon | Yes | No | 43 min |

**Table 5.1:** Interview setup overview

notes from the interview rather than the transcription. In one case, due to technical issues, the interview was recorded with poor sound quality, and thus, it was based on notes made by the interviewing researcher. At last, one interview transcription (CI10) was omitted due to a request from the respondent.

Due to the disclosure concerns of some organisations, two respondents requested the questions in advance. While this did give preparation time for the interviewee and cause a potential bias, it did allow the interviewee to participate in the interview.

### 5.3.1 Critical infrastructure group

The following parts about respondents are the elements that the researchers have extracted from the respondents' answers. Transcriptions for those answers that were successfully recorded can be found in Appendix C. All transcriptions were subjected to anonymisation as this was necessary to ensure the anonymity of the respondents and avoid NDAs. Anonymisation can include names, sectors, companies and product names being left out or altered, tense being changed, or small bits excluded. While this does obscure the transcriptions, it was necessary for the report.

### Interview questions for critical infrastructure

The interview for the critical infrastructure had six questions and can also be found in Appendix B.1.
**Question 1:** *"Can you tell me what is your role in regards to incident management and information sharing?"*. This question is meant to clarify the position, experience and exposure of the interviewees to the problem and compare the differences in their replies. For example, a student helper might answer differently than a CISO.
**Question 2:** *"In your experience in your current company, what are the positive and negative elements about information sharing?"*. The answers gave insights into how the respondent saw information sharing and potentially harmful elements, which would have to be addressed for a framework that allows sharing. The question included "experience" and "current company" to ensure that it was based on the respondent's current company rather than previous cases. The "experience" suggested that it was based on incidents that had occurred rather than plans or ideas.
**Question 3:** *"Can you describe the process of information sharing in your company using a few steps?"*. Knowing how companies deal with information sharing can impact how the framework should be set up as different information may be shared in multiple phases of an incident.
**Question 4:** *"What information do you share (internally or externally)?"*. This question gives suggestions as to what is important for the users of a framework for information sharing. This question also included whom this information is shared with, as this suggests who may need access to the shared information.
**Question 5:** *"Do you have procedures where the employees can report incidents/suspicious activities?"*. Having procedures for reporting is essential to detect attacks as the user is often the first that can react to an incident.
**Question 6:** *"Could you describe the ideal information sharing system for your company?"*. This is an open question regarding the framework this report will work on creating. Allowing respondents to answer what they want and consider necessary and nice to have elements is important to create a framework they can use.

### Respondent CI1 (Network Administrator)

The respondent administers the enterprise's networks and participates in incident handling.

**Interview outcome:**

- An entity represents a centralised system with no access gradation to the sector-specific systems (changes are seen immediately after executing all users)
- There is no continuous awareness training regarding incident management (the respondent has mentioned that a phishing awareness campaign was held

in October with phishing emails and small awareness material on how to spot a fraudulent email)

- The entity has dedicated in-house IT staff that handles network and minor incidents; however, the major cyber incidents are handled by the outsourced team
- In the information sharing, the valuable parts are what attack the entity is experiencing and where it originates from
- The information sharing platform should bring transparency and awareness to the entities
- The authorities should handle the information sharing platform

**Respondent CI2 (CISO)**

The person is a CISO of the company, among others, in charge of the awareness program and coordinating internal and external incident management and information sharing.

**Interview outcome**

- Trust is important
- We have a continuous and constantly updating awareness training program
- We have an external security company we share incident information and, in the GDPR case, also with Datatilsynet
- We do not engage in collaborative information sharing
- Several sources of information are preferred over a single source
- We have a news feed to keep us up to date about trends
- Sharing security procedures and setup is extremely important for us

**Respondent CI3 (Chief Security Officer)**

The respondent is a Chief Security Officer in Nordics in his company and is responsible for incident management and information sharing in his organisation.

**Interview outcome**

- Sharing of information is determined a lot by the size of the incident
- Stakeholders have a certain influence on what and how it is being shared

- The information that is being shared varies depending on whom it is shared with: authorities require information if the business operations were affected, whereas the technical community seeks the technical information
- The value in information sharing is present only when the information is unique and contextualised; all the generic cases can be Googled
- Awareness program is well established, and objectively efficient
- Incident reporting happens via a dedicated portal as well as by directly contacting the security team
- Ideal information sharing platform should contain relevant and reliable information. The sharing should happen with the privacy-preserving mechanisms
- Participants in the information sharing platform should have a great level of trust, possibly verified by the trusted third party
- Using TLP can be useful

**Respondent CI4 (Head of support and IT)**

The respondent is the head of support and IT for parts of the operation in the company.

**Interview outcome**

- Severity of an incident determines how it will be shared
- Sharing information can cause problems with clients and shareholders
- Obliged to share with authorities
- Information sharing with external parties is not regular
- Awareness and awareness training is in place, and procedures are in place for reporting
- Sharing information cannot expose infrastructure, e.g. names, domains etc.
- Only stakeholders should know shared information to start with

**Respondent CI5 (Systems Security Architect)**

The respondent is a security systems architect and does not have any direct involvement with information sharing but focuses on the security of products.

**Interview outcome**

- Different protocols depending on the severity of the event
- Required to share with authorities (GDPR reasons)
- Positive to share as to further security, but can hurt stock values
- Well defined reporting opportunities
- Anonymity is important in terms of sharing information
- Not sure anonymity can be achieved for this scenario
- Nice to know information when sharing:
  - IoCs
  - threat actor
  - type of attack
  - specific vulnerability, etc.
- For a utopian solution, sharing across all sectors would work, but it depends if it can be achieved

**Respondent CI6 (Chief of Security)**

The respondent is the chief of security and takes part in sharing information with other security leaders in the industry.

**Interview outcome**

- Sharing information can aid in being smarter about security
- IoCs are interesting for security
- MISP is a commonly used platform for such sharing
- Have personnel taking care of awareness and training
- Trust is important, however hard to obtain as it is not technical trust but trust amongst peers

**Respondent CI7 (CISO)**

The person is a CISO of the company, managing Information security and Incident handling.

**Interview outcome**

- It is important to share information to learn about others and compare if we do everything correctly, but we do not have any agreements for sharing information with other companies.
- We share information with the authorities for our sector and Datatilsynet, where we have to report incidents and any GDPR related breaches.
- The general concern about sharing comes from information being sensitive. Sharing too much about it can reflect on negative a reputation.
- Hoping NIS2 brings more information sharing requirements for us and in general.
- We use our incident data to improve our systems and procedures constantly.
- We collaborate with a security company to handle critical events.
- We have procedures for reporting, sharing information and awareness also training.
- The ideal system would include NDA. It would also require more openness to share, anonymisation and creating a network of trust.

**Respondent CI8 (Director of Cyber Defence Center)**

This respondent is the director of the company's internal cyber defence centre, responsible for operational security, information sharing and some incident handling.

**Interview outcome**

- Sharing information can aid in being smarter about security
- IoCs are interesting for security
- MISP is a commonly used platform for such sharing
- Have personnel taking care of awareness and training
- Trust is important, however hard to obtain as it is not technical trust but trust amongst peers.

**Respondent CI9 (Senior Security Architect)**

The respondent is a senior security architect but does also know information sharing and incident management in their company.

**Interview outcome**

- Information should be accessible to other relevant parties
- Mainly positive to share information but also negative that others will put the blame
- MISP is relevant for this kind of sharing
- IoCs are highly relevant, both to share but also to receive, in order to secure systems
- Anonymity can be hard to achieve as it will be leaked if they are under attack, and if IoCs pop up at the same time, we can deduct who it is from
- Trust is hard but often comes from meeting people in real life
- The platform should ensure that the attackers do not enter and either follow along or enter wrongful information

**Respondent CI10 (CISO)**

This respondent is VP responsible for infrastructure and operations and acting CISO.

**Interview outcome**

- People want precise data early; however, this may not be possible as it may not be reliable intelligence
- People should know the content shared
- The information should not be leaked to the public unless explicitly mentioned
- Protection of Intellectual Property is important
- Nice to know information when sharing:
  - IoCs
  - hashes
  - IP addresses
  - TLP
- A lot of smaller cyber security incidents
- Need for proper tools for sharing, including watermarks and other ways to identify who owns it
- Awareness is a part of our culture and part of our onboarding process

- Detailed logging about who accesses what
- Journalists and others can request access to documents from governmental entities

**Respondent CI11 (CISO)**

This respondent is CISO and responsible for the security.

**Interview outcome**

- IT vendors are looped into the security
- Crisis response at a sector level
- Reports to authorities (including CFCS and CERT)
- Confidentiality is the primary problem for sharing
- Sharing is good, but confidential information is on a need to know basis
- Reporting happens during the incident and after
- Nice to know information when sharing:
  - IoCs
  - tactics
  - procedures, etc.
- Multilayer sharing, the primary group first and then later to all

**Respondent CI12 (CISO)**

This respondent is CISO and responsible for the security.

**Interview outcome**

- Not a lot of formal sharing; however, much informal sharing
- Sharing major incident information
- Many companies share rather late and not during the incident
- Security handbook, however, not a lot of training
- Anonymous sharing is important
- Companies should not sell the data on the platform; it is for internal use only

### 5.3.2 Authorities and IT security groups

As with the questions for the critical infrastructure companies, privacy, anonymity and time were thought into the questions for authorities and IT security companies. As mentioned in Section 5.3, the questions are not identical to those of the critical infrastructure companies, but they still have many questions in common. Both the interview questions for authorities and IT security companies consist of seven questions.

#### Interview questions for authorities and security companies

All interview questions for authorities and security companies Appendices B.2 and B.3 respectively.

**Question 1** is identical in all three interview questions, and question 6, regarding the ideal information sharing system, is question 7 in the Authority and IT security company interviews.

**Questions 2 and 3** for authorities are similar to questions 3 and 4 for security companies, which have question 2 to be *"Are any of your customers in terms of cyber security, in the critical infrastructure?"* for the reliability of the interview. The questions for 2 and 3 are *"In case of a cyber security incident, what information is important for you to be shared?"* and *"Where is the information about the incidents shared?"*. The answers showed what information the framework should include for sharing, if any such platforms or frameworks already exist and where to share it. A key element to the security company questions is that *"for the incidents within critical infrastructure companies"* have been added, as they may handle other companies than critical infrastructure.

**Questions 4 and 5** for authorities are *"What is the status of awareness from companies in terms of information sharing?"* and *"Are the company/(companies) prepared and do they know the legal requirements to disclose?"* as they may have knowledge of this due to their position as CERT, DCISs and more. This gives insight into companies' knowledge in the field of information sharing. This is also related to question six of security companies *"While talking to your customers, is awareness of preventing cyber attacks important and does this awareness include information sharing?"* which also talks about the awareness for companies and prevention and information sharing.

On the other hand, **question 5** for security companies is *"How do you establish and manage trust between the parties?"* which is also similar to question 6 of the authorities, being *"Do you collaborate with other entities? And how do you establish and manage trust?"*. As several critical infrastructure respondents have mentioned trust, it is crucial to understand how this is gained and maintained.

Similarly, as with the critical infrastructure interviews, the transcriptions have been anonymised, meaning some tenses, names, sectors and so on may have been altered.

Both security companies and authorities are represented as the index "A".

**Respondent A1 (Head of CERT)**

The respondent is the head of one of the CERTs that support critical infrastructure companies. The respondent has direct responsibility for information sharing with authorities and other companies.

**Interview outcome**

- Giving the information is as important as getting something out of information sharing
- Nice to know information when sharing:
  - IoCs
  - timestamps
  - data that helps to understand the threats
- Sharing the information with other counterparts, government authorities, and law enforcement are important.
- Awareness is rather good, but different entities have different appetites for information sharing
- Trust can be established based on the person to person relationships as well as the rules and a setup around an information sharing framework
- Ideal platform will benefit all its participants by providing transparency to all the participants.
- Providing KPIs to measure the efficiency of the framework

**Respondent A2 (Threat analytic)**

The respondent is a threat analytic in the CERT finding threats in the critical companies' infrastructures.

**Interview outcome**

- IoCs are important
- Can be used for prevention, protection and detection
- DCIS MISP in Denmark with a lot of sharing across sectors
- Chat forum for the members

- Maybe DCIS/CERT split due to different ministry responsibility
- Awareness level is very different depending on the company
- Motivation to not share is often due to psychology and fear of consequences
- DCIS/CERT checks if the reported information is legit or clear false positives
- If automatic reporting is utilised, false positives can become a problem
- Logging in Denmark is generally not sufficient

**Respondent A3 (Head of CERT)**

The respondent is the head of one of the CERTs that support critical infrastructure companies. The respondent has direct responsibility for information sharing with authorities and other companies.

**Interview outcome**

- DCIS/CERTS are owned by the members (critical infrastructure companies)
- DCIS/CERTS help drive and facilitate information sharing
- Creates threat assessment for the relevant sector
- Nice to know information when sharing:
  - IoCs
  - tactics, techniques
  - procedures, etc.
- Vendors are included in information sharing
- Trust is problematic in large groups because people cannot know everyone
- Larger groups can be split into smaller trusted sharing groups
- The Covid-19 pandemic has shown that trust can be obtained online too
- Trust is built and not instant

**Respondent A4 (Head of DCIS)**

The respondent is the head of one of the DCISs that supports critical infrastructure companies. The respondent has direct responsibility for information sharing with authorities and other companies.

**Interview outcome**

- DCIS does not help with an incident response but does support information sharing
- Does not share without permission from stakeholders
- Anonymises data before sharing
- Secure chat
- MISP and Mattermost
- Shared platform with threat intelligence, newsletter, awareness training, etc.
- GDPR can be a problem for sharing as it can protect some information
- Trust is important, but it is a long process
- Trust can be built through physical meetings
- Trust only lasts until someone breaks it
- Have a gatekeeper to authenticate and authorise

**Respondent A5 (Head of DCIS)**

The respondent is the head of one of the DCISs that supports critical infrastructure companies. The respondent has direct responsibility for information sharing with authorities and other companies.

**Interview outcome**

- Not everything can be shared
- Uses MISP
- Nice to know information when sharing:
  - IoC
  - TLP
- Awareness is about maturity

- Good relation and collaboration with other authorities
- Uses Mattermost
- International collaboration

**Respondent A6 (Head of DCIS)**

The respondent is the head of one of the DCISs that supports critical infrastructure companies. The respondent has direct responsibility for information sharing with authorities and other companies. An additional respondent took part in the interview.

**Interview outcome**

- DCIS does not handle information sharing
- System based on trust
- Sharing requires permission from the company
- Uses MISP (requires login), Mattermost, Slack and mail
- DCIS provides newsletter
- Some DCIS are public, and some are private
- Trust is a long process and can easily be broken
- Ideal sharing platform is a central place with a gatekeeper to manage who has access to the platform
- The sharing platform could also contain awareness training, exercises and more information
- International collaboration can make trust and authentication harder as it would require knowledge about other countries' company systems

**Respondent A7 (Security analyst)**

The respondent is a security analyst and is responsible for managing incident handling when such occurs.

**Interview outcome**

- Nice to know information when sharing:
  - Techniques
  - IoCs

- We do not share but do help the customers if they request this
- Trust is important and requires a human touch
- Awareness is important, but information sharing is not a big part of it
- Information sharing is lacking in general; the hackers are ahead while we keep the information to ourselves
- Sharing should be two way and not some who share a lot and some who do not share any
- It should be open to who is on the platform and who is shared with

**Respondent A8 (Security management and incident response boss)**

The respondent is the boss in the security management and incident response department and is responsible for managing incidents; however, does not directly share information.

**Interview outcome**

- Suppliers for critical infrastructure companies are sharing and being shared with too
- Nice to know information when sharing:
  - Threat actor, who committed the cyber attack
  - Techniques
  - Infrastructure used for the attack
  - IoC
  - Information should be updated as an IP can be bad one day but good the next and vice versa
- Some information can be public; however, the company should be anonymous
- Trust is both who is shared with, but also if it is good content that is shared
- The content shared should be reliable and anonymous
- Security teams are good at sharing but may not have the infrastructure to do it properly
- Some companies do not want to share due to intellectual property

### 5.3.3 Expert interviews

Throughout the interviews, it was uncovered that a Danish community MISP existed. This discovery resulted in an interview with the creator of this community MISP as it could be interesting for the project. Only a few initial questions were prepared, which can be found in Appendix B.4.

#### Respondent E1 (Head of Danish community MISP, Dennis Rand)

The respondent is the owner of his own consultancy company eCrimeLabs, and also the head of the Danish MISP community for more than five years, with the insides of working with MISP participants and managing the platform.

**Interview outcome**

- Using MISP as a sharing platform, works in all scenarios I have had
- Sharing IoC is useful
- Context is important when utilising data
- Still place to grow for organisations to understand and be part of the information sharing
- Even if one does not share, companies can still benefit from being a part of the community
- The technology is there; the issue is people
- Information can be helpful at the time of the attack but also in retrospect to check one's security
- It is hard to define what is a targeted attack and what is not; therefore, more information can be relevant
- We need to address what is making it hard for organisations to share information so we can make it easier for them
- Companies are checked against the CVR register and for when they were established
- Companies have to use their company email to register, so it does not come from a random Gmail
- The more members, the harder it is to ensure trust
- Sharing can happen within a trusted group or with everyone
- Time, relevance and fear are factors to prevent sharing

## 5.4 Summary

Throughout this chapter, we presented outcomes of 21 semi-structured interviews. We interviewed four different groups of respondents for various purposes. Critical infrastructure organisations and security companies may benefit from an information sharing platform that can be used to share cyber security incidents, as shown in the interviews. Authorities were also interviewed as they may either regulate, handle information sharing or are a part of the security solutions for the companies. Although authorities do utilise MISP for information sharing, as stated by multiple respondents, additional research can be beneficial for this solution.

Every sector mentioned in Section 1.3.3 is represented in the set of respondents. The respondents had different positions, including security architects, administrators and CISOs.

The questionnaire showed that cyber security incidents are relatively common. However, due to the difference in the definitions of an incident, these numbers may be hard to compare. One respondent mentioned no incidents in the past 12 months, which did raise confusion as to whether this is due to a difference in definition or strong security, leaving the attackers to focus on other targets or if the detection is lacking. This difference in definitions continued in the following questions about sharing. Most respondents stated that they do not share minor or middle sized incidents. However, the majority share critical or major incidents. Interpretation variances of a cyber incident and its size make it impossible to conclude whether the companies share and exactly when. One observation is whether a unified definition and degree of an incident are missing in the Danish critical infrastructure.

The interview questions focused on the respondent's current company, thus within the critical infrastructure, and on the organisation rather than the individual. While transcribing the interviews, we subjected responses to anonymisation, as stated in Section 5.3, to ensure that the reader could not identify the respondents and their companies. Additionally, the key elements from each interview were extracted and organised into bullet points in Section 5.3.1 and Section 5.3.2.

Throughout the interviews, we discovered a collaboration between authorities, where incident information is shared utilising MISP. Such collaboration was not discovered until the interviews with authorities, which suggests that additional sharing can be added, which multiple respondents also mentioned. As many also state, the art of sharing information about incidents is a process which is still ongoing in the Danish critical infrastructure, suggesting that research in the field is beneficial for all parties.

Awareness also differs depending on the interview, as most respondents in the critical infrastructure replied they have awareness training; however, according to authorities, it varies. It could be due to the sample group for the interview being

more prepared than others or that a company may feel more ready than others see it. An additional point is how aware companies are of sharing with others and the maturity of a companies information sharing and incident handling, as many do not share a lot as seen in the questionnaire; however, in the interviews, multiple respondents suggest that sharing is beneficial if done anonymously.

In addition to the MISP amongst authorities, a Danish community MISP allows companies to join a platform to share information. It is, however, essential to note that authentication of which parties can enter the MISPs is done manually, resulting in much work if many companies and organisations choose to join a platform.

Sharing on the platform should include the critical infrastructure companies, authorities, security companies and other vendors.

Most respondents replied that sharing is positive and beneficial for security. However, this was often followed by the lack of trust that many have. Trust was often referred to as trusting the people on the other side who would receive the information. Many stated that trust could be obtained by meeting physically multiple times, which, as stated by respondent Section 5.3.2, can be hard to manage if the group of people to trust grows too large.

Anonymity was also regularly mentioned as a key element for successful information sharing to ensure that other organisations cannot use the information against the sharer. It does make trust harder as organisations want to know whom they are sharing with, which means this has to be dealt with in such a platform. While it should not be known who shares, it should be known who is shared with. Another challenge to anonymity, trust and privacy is the Danish "Offentlighedsloven" [132], where individuals, such as journalists can gain access by requesting access to documents (Aktindsigt). Thus, if the platform is run by a governmental entity it is possible to extract the information from the platform, even if it is not compromised.

### 5.4.1 Requirements

The questionnaires and interviews lead to a set of requirements that can be used for the framework and are organised chronologically according to the order of the interviews. Some of the requirements are very similar or directly depend on each other, like S11 and S22. We decided to be very specific with requirements at this phase as we wanted to capture the essence of each interview and individual request. In the further requirement generalisation phase, we will filter and possibly merge a large portion of the following list (Table 5.2).

| Index | Requirement | Category | Reference | Dependency |
|---|---|---|---|---|
| S1 | Sharing the IoCs | F | CI3, CI5, CI6, E1 CI8-CI10, A2, A3, | |
| S2 | Sharing the IoAs | F | CI1, CI3, CI5, E1 | |
| S3 | Sharing attack type | F | CI1, CI5, E1 | |
| S4 | Novelty of data | NF | CI3 | |
| S5 | Assign reliability meter | F | CI2, CI3, CI9 | |
| S6 | Information context | NF | CI3, A1, E1 | |
| S7 | Assign attack severity | F | CI3,CI4, CI5 | |
| S8 | Data anonymity | NF | CI4, CI5, CI7, CI9, A4 | |
| S9 | Sharing vulnerabilities | F | CI5 | |
| S10 | Sharing threat actor | F | CI3, CI5 | |
| S11 | Access control | F | CI1, CI3, CI4, CI9, CI10 | S8 |
| S12 | Establishment of trust | NF | CI1-CI3, CI6-CI9, A1, A3, A4, E1 | |
| S13 | Sharing with external parties | F | CI1,CI2, CI4, CI7, A1, A3 | S27 |
| S14 | Sharing with authorities | F | CI1-CI5, CI7, CI9, CI11, A1 | S27 |
| S15 | Confidentiality disclosure clauses | NF | CI2, CI3, CI7, C11, A1, A4 | S12 |
| S16 | Authentication | F | CI1, A2, A4 | |
| S17 | Send notifications | F | CI2 | |
| S18 | Centralised topology | NF | CI1 | |
| S19 | Verifying users | NF | CI3, E1 | S16 |
| S20 | Using MISP | F | CI6, CI8, CI9, A2, A4 | |
| S21 | Using TLP | F | CI3, CI10 | S20, |
| S22 | Control of data | F | CI10 | S11, S21 |
| S23 | Provide transparency | NF | A1 | S29 |
| S24 | Measure efficiency of platform | NF | A1 | |
| S25 | Trusted groups | F | A1-A3, E1, | S12, S27 |
| S26 | Sharing with sector | F | C11, A2 | S27 |
| S27 | Sharing groups | F | C11 | |
| S28 | Log user activity | F | C10 | S23 |
| S29 | Instant messaging/forum | F | A2, A4 | |
| S30 | Sharing setup guides, news | F | CI2, A4 | |
| S31 | Sharing procedures, strategies | F | CI2, CI11, A3 | |
| S32 | Data analysis | F | CI7 | |
| S33 | Protect system from intruders | NF | CI9 | S8, S11, S16, S19 |
| S34 | Verify data | NF | A2 | S5 |
| S35 | Secure data | NF | A4 | S8 |
| S36 | Using Mattermost | F | A4 | S30 |
| S37 | GDPR compliance | NF | A4 | |
| S38 | Public access | F | A5 | |

**Table 5.2:** Requirements gathered from interviews

# Chapter 6

# Requirements

Requirements constitute the foundation of any IT product. Gathering the complete list of requirements benefits the engineering process in the initial stages of planning the product, allowing to see the full capabilities. Another benefit is in the final stages to see if all the requirements have been met. This chapter presents scenarios in Section 6.1.1, use cases based on the scenarios in Section 6.1.2 and the final list of prioritised requirements.

## 6.1 Requirement gathering

In addition to the requirements gathered throughout Chapters 3 and 5, this section will create scenarios and use cases to find potential additions to requirements (see Section 2.2.4).

### 6.1.1 Scenarios

Multiple scenarios are created for users interacting with the information sharing system and performing different actions (use cases) depending on the given situation. For the most part, these situations are inspired and based on stakeholder interviews Section 5.3. Even though each of the twelve scenarios depicts a unique situation, some user actions are introduced in multiple scenarios.
**Scenario 1:** Create a user account (registration)

An organisation falls under the category of a platform user profile and needs to **create a user account** in order to join. By clicking on a registration button, an *electronic form* is **displayed** and needs to be **filled out**. The form content is **reviewed by a system administrator manually**, and after everything is verified, the user is either approved or rejected for the platform. If approved, the user **chooses a login method**, enters credentials (fulfilling the security requirements) and registers as a system user.

**Scenario 2:** Login and join a sector group

A user wants to **join a sector group** which is a sharing group with organisations from the same sector. The user **signs in using credentials** generated in the registration phase and those are authenticated. When successfully logged in, the user can **see their home profile** and **logged activities**, meaning their own and others shared information. Using this account, the user can **create sub-accounts** for other employees within their organisation. A user can **share with the entire platform**. However, today a user wants to **become a member of a sector group**. The user **sends a request to join**, and the platform automatically checks whether or not the user account belongs to the requested sector (Note: this information is not visible in the platform, only on the backend). After verifying that a user belongs to a specific sector, the user becomes a member and successfully **joins the sector group**. Now, the user can **share within this group** as well. The only criterion to join a sector group on the platform is to be part of that sector.

**Scenario 3:** Share information (IoCs, ) within a trusted group

After incident analysis, an organisation concluded that a ransomware attack had hit it. Due to the nature of an attack targeting sensitive records, it appears relevant to other companies within the sector to be on alert. Therefore the organisation **shares the IoCs and IoAs from the incident in their sector group**.

**Scenario 4:** Reporting to the authority

Yesterday an organisation faced a database compromise of their employee records. Due to reporting obligation in case of a GDPR breach, the incident needs to be **shared with the appointed authorities**. The user **selects a receiver** from the list of authorities who are the only members not anonymised in the system and **fills in additional information**, among others, the timestamp of the incident detection (to ensure they are compliant within the period for reporting) and reports the incident.

**Scenario 5:** Share information with their security company

A user has outsourced a portion of their incident analysis to a security company. In order to understand an incident better, the user **fills out a report** form with the attack type and context of what happened and **shares it with their security company**. The system then **sends the information** to the recipient as it can see which company is linked to the user. The company **views the information** and then **replies** by classifying the attack severity and instructions for any further actions.

**Scenario 6:** Receive notification

The user **receives notifications** via email/SMS stating that new **information has been shared with their profile**. Prior to that, the user selected what type of information should trigger a notification. When the user has received a notification, a link, when pressed, **will redirect them to the shared information**.

**Scenario 7:** Edit shared information

After discovering new information about last month's incident, the user **goes**

**to their profile**, **lists logged activities** and **views the event** they created about the incident and choose between **Edit** and **Delete**. Since information needs to be edited not removed, the user clicks on the **Edit** button and **add newly discovered information** to the event log button.

**Scenario 8:** User comments on an event

A user can **see** that an **incident event** reported on the community platform group resembles one of the discussed incidents in the user's sector group. As some interesting information about how to handle this type of attack was discussed in the sector group, the user, decided to share some of that information by **commenting on the event log** in the community user group.

**Scenario 9:** Sharing (IoCs) with the public (Optional)

The general public can access only a limited display on the platform without being registered. A user with basic access rights visits the platform's home page. On the home page, they can **get an overview of indicators of compromise (IoCs)**. However, they cannot determine any other details aside from given IoC.

**Scenario 10:** View the shared information

A registered user **visits** the information sharing platform's **home page**, where general shared **IoCs are listed**. However, the user is an employee in a critical infrastructure company and wants to access more information from their sector. They **log in** with the previously provided credentials and get access to additional information like IoAs and other information. The user clicks on the menu option to **see additional information** within their sector, and the website takes the user to the page where their sector shares incident information.

**Scenario 11:** Contacting CERT

A system user received an alert about suspicious activity in their organisation's network. As they do not have an incident response team within the organisation, the user needs to contact the relevant CERT. In order to do so, they log in to the sharing platform and select the **initiate conversation option**. They firstly **send a text message** explaining the situation. The CERT or user can then **initiate a response call** for further dialogue.

### 6.1.2 Use case

Use cases or user actions describe ways a user can interact with a given system, in our case, an information sharing system, to achieve a desirable outcome. Deriving such cases from scenarios by highlighting potential user actions, we narrowed them down to 24 general use cases. First, we used generalisation to combine actions similar in nature or actions performing the same step under different word selections into one general use case. Then we assigned dependency to other use cases if applicable depending on the logical flow of the scenario. In Table 6.1, the use cases are categorised into *Name* and *Index* of the use case. Moreover, we added

*Pre-conditions* and *Outcomes* explaining actions required prior to the use case and the plausible outcome of the use case. Lastly, we assigned *References* connecting use cases with scenarios in which they were introduced.

| Index | Name | Pre-condition | UC Outcome | Reference |
|---|---|---|---|---|
| UC1 | Create user account | User does not have account | Account creation initiated | Scenario 1 |
| UC2 | Fill registration form | User belongs to stakeholder group | The registration form was sent to Admin | Scenario 1 |
| UC3 | Select login method | UC2 | Method selected as login mechanisms | Scenario 1 |
| UC4 | Review information | UC2 | Request is approved or denied | Scenario 1 |
| UC5 | Create sub-account | User has account | A new user is added with User's profile | Scenario 2 |
| UC6 | Login with credentials | User has account, UC3 | User is logged in system | Scenario 2 |
| UC7 | Select receiver | User has account | Receiver selected | Scenario 4, 5, 11 |
| UC8 | Join sharing group | UC6 and UC4 | User becomes member | Scenario 2 |
| UC9 | Share with group | UC8 | Group for sharing selected | Scenario 2-5, 9 |
| UC10 | Share information | UC7 or UC9 | Information shared | Scenario 3-5, 9 |
| UC11 | Comment on event | UC10 | Comment to event is attached | Scenario 8 |
| UC12 | Edit information | UC10 | Information is changed | Scenario 7 |
| UC13 | Add information | UC10 | New information is attached | Scenario 4, 7 |
| UC14 | Delete information | UC10 | Information is removed from display | Scenario 7 |
| UC15 | Initiate responce call | UC7 and 8 | The call receiver dialed | Scenario 11 |
| UC16 | Send text message | UC7 and 8 | Message sent | Scenario 11 |
| UC17 | View IoC's list | UC10 | Information displayed | Scenario 9 |
| UC18 | View user activity | UC6 | Information displayed | Scenario 2, 7 |
| UC19 | View home screen | UC6 | Redirected to home screen | Scenario 2 |
| UC20 | View user profile | UC6 | Links to user displayed | Scenario 5, 7 |
| UC21 | View additional information | UC13 | Information displayed | Scenario 5 |
| UC22 | Receive notification | Selected alerting condition, UC10, Notification sent | Users is notified | Scenario 6 |
| UC23 | Redirect to group | UC6 and UC19, Click on notification icon | Group space displayed | Scenario 6 |
| UC24 | View event (incident record) | UC10 and UC23 | Event displayed | Scenario 6, 8 |

**Table 6.1:** Use cases overview

To provide a contextual relationship and overview of the relatively large amount of use cases, we categorised them even further into 4 phases: *Registration*, *Involving*, *Viewing* and *Sharing*, all based on the core purpose of the action. We distinguish between a user and an admin when it comes to users. Some users have an account on the platform, and some do not but have limited access. Users have different classifications, Authority, Security Company and Critical Infrastructure. An organisation can have multiple users linked to the initial higher privilege user account (sub-users). The last element depicted in Figure 6.1 is different sharing groups. We can see the group for all registered users, groups created within a specific sector to

share, and a trusted group created between a regular user and their sub-users or their security company or relevant authority.

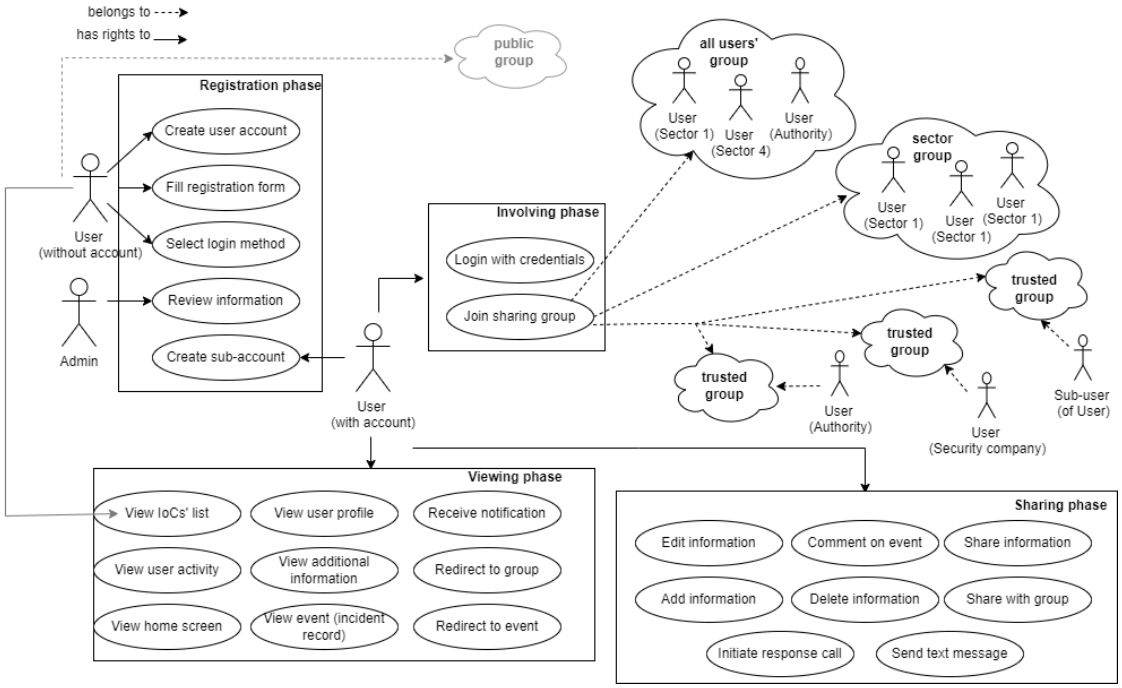


**Figure 6.1:** Use case diagram

## 6.2 Requirement prioritization

This section reviews all the requirements gathered and justifies their importance for the framework. There might be overlaps or similarities as the requirements originate from different sources. Therefore, we generalise and combine some of them in Section 6.2.1. In order to indicate the importance of each requirement, we subjected them to MoSCoW analysis in Section 6.2.2.

### 6.2.1 Requirements updates

The first requirement in the final list is *R1-Implement security*. To cover all security requirements (like encryption, securing the system against common vulnerabilities and intruders, securing data transfer and securing data), we create one general requirement, R1, which serves as a reminder to implement security best practices like a backup. In addition, it helps developers to be mindful of security when implementing several of the other requirements in the table (for example *R3-Authentication*) indicated by dependency on R1.

*R2-Identity provisioning* requirement is based on one same-named IAM1 requirement, but it also covers (IS12, S19) user registration and user verification requirements, respectively.

*R3-Authentication*, this requirement was mentioned twice as IAM2 and S16. In the final table, it is naturally represented only once. Similarly, *R9-Establishment of trust* is based on two identical requirements, IS2 and S12 and *R12- Control of data* is based on same-named requirements IS8 and S22. *R17-GDPR compliance* and *R19-The confidentiality disclosure* requirement is another example mentioned several times throughout the requirement gathering phase.

*R4-Authorisation* is a combination of three similar requirements, IAM3, IS11 and S11 that all handle either authorisation or access control.

*R5-Role/attribute management* is again a combination of two requirements: Role management and Attribute management. This requirement is highly dependent on the implemented access control policy and is there to remind the need for mechanisms to manage the life-cycle of roles/attributes.

Requirements: *R6-Session management, R7-Privacy for identities, R13-Selected choice of data receiver, R14-Data transfer, R16-Verify data integrity, R18-Data in a unified format, R21-Multifactor authentication, R22-Data usability, R25-Send notification, R26-Single-sing on, single sign off, R27-Support identity federation, R32-Provide transparency, R33-Measure platform efficiency, and R34-Instant messaging/forum* are all based on their corresponding requirements identified in their respective report chapters and are deemed to be relevant for the framework.

The Mattermost requirement from S36 in Table 5.2 is removed not to force the technology on th platform, as it was mentioned as a solution that only some used.

*R8-Log user's activity* is based on the same-named S28 and logging requirement form Chapter 3 IAM12.

*R10-Data anonymity*, the need for this requirement was brought up several times by requirements IS18 and S8, as well as emphasising the protection of sensitive data in the system.

*R11-Sharing incident data* is a generalised requirement covering sharing data like IoAs (IS6, S6), IoAs (S2), attack type and threat actor (S3, S10) and others. Similarly, *R29-Sharing non-incident data* requirements cover sharing data like procedures and strategies (S30, S31).

*R15-Data storage* is based on the same-named requirements IS16. The security aspect of IS17 of storage is also covered by R1.

*R20-Using TLP* was not only based on the same-named S21 but also supported by the protection of sensitive data requirement IS5.

*R23-Sharing groups* is about the system supporting the creation of different groups like trusted groups and sector groups (S25, S25, S13).

*R24-Utilise MISP* is based on IS14 and S20 indicating that MISP should be included as part of the system. By implementing MISP, the requirement for data

analysis (S32) is directly supported.

*R28-Public access* was derived based on requirements IAM11, S38.

*R31-Assign reliability score* is based on same-named requirement S5 and also directly supports requirement S34 which specifies data verification need where reliability indicator can be helpful.

### 6.2.2 MoSCoW

In order to provide the priority order amongst our 35 final framework requirements, we applied the MoSCoW method. The criterion for the *Must* requirement was based on the Minimum viable product (MVP) concept [133]. Therefore, the requirements classified as *Must* are the necessary features for the Information sharing framework to work and provide the basic functionalities for a system like this must-have.

The set of *Should* requirements might be very useful and need to be implemented in early-stage after the MVP is deployed despite the system being unable to function as it should without them. On the other hand, the *Could* have requirements are mostly an addition to features that are not the most important but were requested by stakeholders and would add to user experience as well as improve the overall usability and expand the variety of the system features. For example, the amount and possibly also the quality of information shared would be expanded by implementing, for example, *Could* requirements (R29-R31). The list of requirements grouped as explained in Section 6.2.1 ordered according to MoSCoW is displayed in Table 6.2.

| MoSCoW | Index | Title | Category | Reference | Dependency |
|---|---|---|---|---|---|
| Must | R1 | Implement security | NF | IS13, IS15, IS17, S33, S35 | R8 |
| | R2 | Identity provisioning | F | IAM1, IS12, S19, UC1-UC3, UC5 | R1 |
| | R3 | Authentication | F | IAM2, S16 UC4, UC6 | R1, R2 |
| | R4 | Authorisation | F | IAM3, IS11, S11 | R1 |
| | R5 | Role/attribute management | F | IAM4, IAM8 | R4 |
| | R6 | Session management | F | IAM5 | |
| | R7 | Privacy for identities | NF | IAM6 | |
| | R8 | Log user's activity | F | IAM12, R12, S28, UC18, UC20 | |
| | R9 | Establishment of trust | NF | IS2, S12 | |
| | R10 | Data anonymity | NF | IS5, IS18, S8 | |
| | R11 | Sharing incident data | F | IS6, S1-S3, S6, S10, S27, UC10, UC11, UC17, UC24 | R1, R14 |
| | R12 | Control of data | F | IS8, S22 UC12-UC14 | |
| | R13 | Selective choice of data reciever | F | IS10, UC7 | R11, R20 |
| | R14 | Data transfer | F | IS13, IS21 | R1 |
| | R15 | Data storage | F | S16, S17 | R1, R14 |
| | R16 | Verify data integrity | F | IS19 | R1 |
| | R17 | GDPR compliace | NF | IS20, S35 | R12 |
| Should | R18 | Data in unified format | F | IS4 | |
| | R19 | Confidentiality disclosure clause | NF | IS1, S15 | R9 |
| | R20 | Using TLP | F | IS5, S21 | R13 |
| | R21 | Multifactor authentication | F | IAM7 | R1, R3 |
| | R22 | Data usability | NF | S32 | R18 |
| | R23 | Sharing groups | F | IS9, S13, S14, UC8 S25-S27, UC23 | R3, R4, R5, R9 |
| | R24 | Utilize MISP | F | IS14, S20, S32 | R18 |
| | R25 | Send notification | F | S17,UC22 | R8 |
| Could | R26 | Single sign-on, single sign-off | NF | IAM9 | R3 |
| | R27 | Support identity federation | NF | IAM10 | R2 |
| | R28 | Public access | F | IAM11, S38 | |
| | R29 | Sharing non-incident data | F | IS7, S9, S27, S30, S31, UC21 | R1, R14 |
| | R30 | Assign reliability score | F | S5, S34 | R11 |
| | R31 | Assign attack severity | F | S7 | R11 |
| | R32 | Provide transparency | NF | S23 | R8, R9 |
| | R33 | Measure platform efficiency | NF | S24 | |
| | R34 | Instant messaging/forum | F | S29, UC15, UC16 | R13 |
| | R35 | Using Mattermost | F | S36 | R34 |

**Table 6.2:** Overall requirement list

# Chapter 7

# Analysis

This chapter analyses different legal aspects and privacy best practices for the information sharing platform in Section 7.1. In addition, we discuss different angles on trust in regards to using such a platform and the means to handle data in it (Section 7.3). Lastly, we continue the topic of data handling when talking about sharing platforms and data formats in Section 7.5.

## 7.1 Legal obligations

This section will dive into the legal obligations for information sharing. These legal obligations are twofold as the companies have obligations to share, but the platform also has requirements on how to handle data and continue sharing, and will address both. Only general law that applies to all the sectors will be considered in this section, whereas sector-specific regulation (for example DORA [134]) will not be discussed.

When taking business and business communications within the European Union, all operating businesses must comply with the Company law rules [135]. It represents a collection of Directives that regulate *"formation, capital and disclosure requirements, and operations (mergers, divisions) of companies"*. In addition to this, the sectors may also have individual directives or legal requirements, such as Digital Operational Resilience Act in the financial sector [136].

General Data Protection Regulation (GDPR) is one of the most well known legal frameworks in the EU [137] regarding the privacy of the user and data handling. Privacy is a crucial aspect to consider when designing the information sharing platform, as it concerns the rights of the data subject and data quality. Article 12 of GDPR concerns transparency and communication and refers to the legal disclaimer of how the user can be informed about the data collected by the system. Additionally, Articles 18 and 19 concern another aspect relevant to the information sharing scenario: the right to restrict data processing. In the context of our prod-

uct, the data subject has a right to know all the processes of data it handles and processes. Furthermore, if they disagree with the means of processing the data, they also have a "right to be forgotten", as stated in Article 17. These are a subset of GDPR articles that the platform would have to comply with (R17).

National Standard for Identity's Security (NSIS) is a Danish framework that dictates security standards for Identity Providers and the strength of the authentication process via a list of mandatory technical requirements. It is worth noticing that NSIS only addresses core Identity for Brokers and Electronic Identification schemes, both public and private. However, it does not address other identity management mechanisms, such as provisioning, authorisation, rights and attributes handling. At the time of writing this thesis, there are no national standards that establish those requirements [138].

As mentioned in Chapter 1, the critical infrastructure companies are obligated to share information about cyber security incidents according to the NIS directive [139]. NIS Directive is the first attempt to normalise and standardise the network security requirements across different critical infrastructure sectors in the European Union. Furthermore, it addresses the national governance requirements, such as establishing a national point of contact for the international cyber security incident management, CSIRTs and defines cooperation on the national level.

NIS states that disclosing information to the public should be done voluntarily and with interest to inform about the current threats. Sharing should not be done against the interest of an enterprise if they were to suffer reputational and commercial damage. In addition, information sharing should happen concerning the processing of personal data legislation.

Due to the growing cyber threats to critical infrastructure, NIS Directive is scheduled to be replaced by an updated version, NIS2 [140]. In addition, NIS2 aims to expand the scope to 10 sectors: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration and space [136]. Furthermore, the directive aims for tighter regulation and more strict reporting obligations regarding information sharing.

Throughout the project, a new **Proposal for Cybersecurity Regulation** was published on March 22nd 2022 [141], under which all the enterprises, institutions and agencies will be required to have a cyber security framework implemented within the organisation. This would require governance and risk management frameworks that correlate to the list of controls correlating to the risks. Furthermore, the proposal would have to be considered when implementing the information sharing platform in the future.

This section presented legal frameworks covering the digital realm for critical infrastructure, information sharing, and data processing. We chose not to continue with the legal scope since covering each sector in detail would change the research direction for this project and require us to plan the timeline differently. The section

does not cover inter-business relationships that would regulate in the legal realm, intellectual property protection, liability limitations and usage of software licences. However, this section provided awareness of the directions, including which would be mandatory in framework planning.

## 7.2 Privacy

In a multi-business scenario, such as ours, data can be linked to the separate entities and the specific individuals in the target organisations. Privacy preserving techniques enable stakeholders to build trust in the platform and reduce privacy-related risks to an acceptable level. Privacy-centred requirements often cover legal, social, ethical, and technical domains of system implementation. As a result, there are multiple frameworks and best practices to follow when it comes to making a platform privacy-friendly [142], [143], [137].

Data minimisation is one of the principles stated in Article 5 of GDPR, where not collecting and processing any unrelated and unnecessary data is advised against [144]. When it comes to the privacy of data stored on the platform or in the cloud, some simple yet effective techniques can help to protect the privacy of the data:

- **Defining data classification scheme** - comes from the need to know own data, where sensitive data can be classified and protected according to the level of confidentiality.
- **Data usage policy** - refers to both the governmental and technical domain of the information sharing platform, where defining the types of accesses and rights for data use enable only authorised users to perform actions on the data.
- **Implement data life cycle management** - allows having an overview of the data through the different stages the data goes through the collection, processing, review, retention and destruction.

The main goal of the privacy domain for the proposed framework is to achieve privacy by design required by GDPR [145], [146]. Therefore, embedding it into the final product requires careful planning and agile implementation rather than bringing privacy-related requirements as an afterthought of the design process.

## 7.3 Trust in information sharing

Trust is a common denominator throughout this report, as mentioned in the Section 4.2.1, where ten interview respondents stated trust as a concerning factor but also an essential condition for information sharing. In order to create not only a

functional but voluntarily used system, trust needs to be embedded into the solution (R9). However, trust is perceived and must be established in two directions. For one, mutual trust between parties involved in information sharing we refer to as 'trust in people'. Secondly, trust in the system to secure and handle the information according to providers' requests we will refer to as 'trust in technology'. Both perspectives on trust are codependent, as one has little to no chance of existing without the other. People's trust will be addressed from a theoretical angle only where a system might be a part of the solution. Nevertheless, the psychological aspect of the problem is much more significant than our platform can tackle and, as we are not experts, it is considered out of the scope of this thesis.

Considering that the information shared is inherently sensitive, it is only natural to share it with the parties one trusts completely or is obliged to share with. In the scenario where two parties do not know each other, one being the provider or source and the other being the receiver, trust establishment becomes the broker's responsibility, in our case, the information sharing platform. Therefore, it is required that the system provides means to secure people's trust between entities on both ends of the information flow. Several interview participants proposed an agreement to set rules for disclosure **(R19)** as a potential means to secure initial trust and prevent undesirable dissemination and possible misuse of the data. Similarly, research conducted by ENISA [147] emphasises the need for strict rules for the parties. It also states that smaller groups are easier to manage when it comes to trust maintenance and preservation; thus, the requirement **R23** is relevant. If the sharing parties met in person, that could provide an additional layer of trust between them (interview CI9) but would not be scalable with the growing amount of platform users. **Skopik et al. [148]** propose the reputation system to direct the trust to involved parties someone trusts or has provided helpful information in the past. This solution partly solves the network/circle of trust problem, but it requires some prior information sharing as a downside. Authorities or IT security companies could play the role of a *trusted party*, approving other entities' trust reputations.

However, not only does the receiver has to be regulated and trusted, but equally important is trust in the source of information. Therefore, verifying the information and the provider is required (R1, R3, R16, R30). **Fuentes et al. [120]** propose a digital signature mechanism to ensure the integrity of the message, but it does not solve the content accuracy or the confidentiality of the source. Therefore, Section 7.3.1 will dive into this problem in greater detail.

### 7.3.1 Data handling

To enable information sharing, sharing policies for the distribution of data can aid in an increased level of sharing, in addition to NDA. To customise content shared,

categorisation of the data would need to be implemented (TLP). This section breaks down what type of data will be handled by the platform and how it should be organised and handled in the system. Based on the requirement lists (Table 6.2), several types of data shared within the platform have been identified. In addition, IoCs were requested by users, which means the system needs to be able to handle different data structures such as IoCs, user and company data, log files, etc. The advantage of using MISP to process data is its well defined taxonomy for data classification and tag system [149]. For example, information can be regulated, commercially confidential, financially sensitive, and more. Similarly, an IoC can be assigned as malicious or non-malicious based on its nature and, as previously mentioned in Section 4.2.2. TLP implemented in MISP represents the disclosure range and condition for sharing information by a colour-coded principle. To ensure data is protected if, in the worst-case, access gets compromised, the encryption of the data when exchanged (as showcased in the PRACIS case 4.2.2) and privacy-preserving mechanisms need to be in place for the system.

#### Data anonymity

In addition to secure information in scenarios where a spoofed account tries to access it, the data would need to be anonymous and encrypted so that only authorised, genuine, and trusted receivers could read it.

#### Anonymisation and Pseudonymisation

Anonymisation and pseudonymisation can help achieve unlinkability and de-identification by utilising techniques that strive to enhance the privacy of the data. Moreover, basic pseudonymisation techniques are recommended as a best practice for handling personal or sensitive data [150]. In the business-to-business communication scenario, data manipulation can increase trust in the platform, adding an additional security levels to the shared and stored data.

Pseudonymisation is a technique where the original data is substituted with a similar type of data - a pseudonym. An example of this could be the original company name substituted with the pseudo-randomised name. ENISA provides guidelines for the best techniques for pesudonymisation in regards to the GDPR [151]. Anonymisation provides a complete unlinkability to the data subjects given the data set. The difference between anonymisation and pseudonymisation is that pseudonymised data can be recovered by knowing the technique or a cryptographic secret while anonymisation irreversibly alters the data so that individual records cannot be linked to the data subject. Figure 7.1 demonstrates the schematics on how anonymisation and pseudonymisation work.

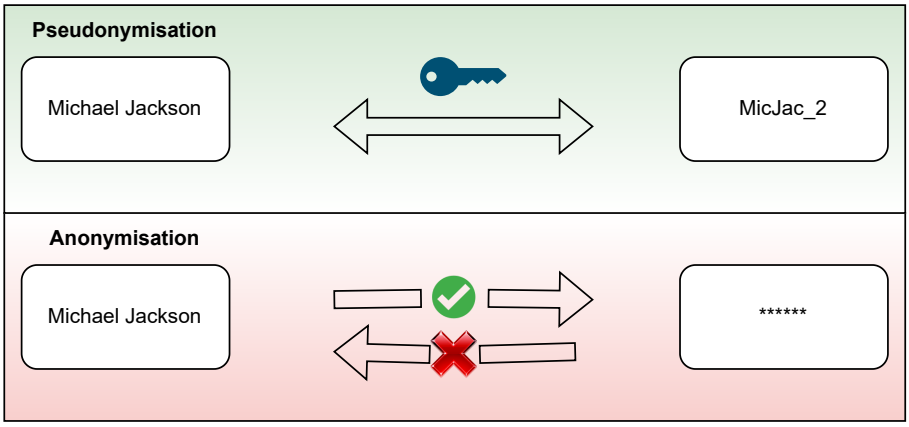


**Figure 7.1:** Schematic representation of Anonymisation and Pseudonymisation [152]

Both anonymisation and pseudonymisation are recommended and are required by the GDPR. If the proposed framework suggests transferring the data to third parties, the design would require anonymisation. If the data is not leaving the platform's network, pseudonymisation would be the design choice.

### Data generalisation

There are multiple ways to de-identify individual records and personal data: data masking, K-anonymity, data obfuscation, and data generalisation are examples of protecting the data and preventing data leaks [153]. Different techniques have different use cases, but most of the techniques rely on mathematical functions. Therefore, choosing the correct data manipulation technique is challenging in system planning. This section describes some techniques for the best data pseudonymisation and privacy preservation techniques.

Data masking is a technique that allows various operations on the data at rest, data in transit or data in use. For example, replacing, swapping and rotating are some of the mathematical operations that mask sensitive data while preserving the structure [154]. This technique is used primarily on the personally identifiable information, which in this case is company identification data, but also on intellectual property, which can include design and planning, and high-value data, such as incident details.

K-anonymity is a privacy-preserving technique where confidentiality of the data set is preserved by generalising and suppressing the attributes. The data set can be called K-anonymous if each record shares the same attributes with at least K-1 records [155]. In our scenario, k-anonymity can be useful when anonymising both the employees from the same company and the groups' records. Such quality of the data set can also promote trust among the participants of the private groups.

In the scenario of multi-business communication and a high volume of sensitive data, it is crucial to ensure the identity protection of each individual. For the framework proposal, we suggest multiple pseudonymisation techniques. First of all, data masking should protect data at rest, in use and in transit by utilising Dynamic Data Masking techniques suggested, for example, by Microsoft [156], [157], or Amazon Redshift for sharing information [158], as well as to pseudonymise data at rest by applying k-anonymity to the set of records.

Of course, when it comes to the implementation, there is no preference for a cloud provider; thus, the data pseudonymisation technique is needed. It is a complex topic that should be addressed during the framework implementation. However, K-anonymity is vendor-independent and because the public has a limited overview of the activities on the platform can be utilised to provide an additional data protection layer.

## 7.4 Authentication

In order to prevent a malicious third party on the platform, user authentication mechanisms to check the confidentiality and identity of a user should be implemented on the platform. Based on Section 3.1.3, the suggested authentication should be both flexible and secure. Flexibility will ensure that a larger amount of stakeholders can access the platform. On the other hand, security brings additional trust and ensures that the information shared on the platform will not go beyond the platform.

ref to specific requirement

The authentication flexibility can be achieved in two ways: by either providing multiple authentication methods or by providing a method that most Danish companies currently use. Furthermore, the security of the authentication can be provided by the authentication scheme, choice and implementation of authentication protocols and additional authentication factors.

Due to the scope of the project (Danish critical industry and supporting entities) and the requirements from stakeholders regarding trust and security in the platform. The solution for the platform should be something that all the participants know and trust. As multiple interview participants have mentioned, the NemID [159] solution would be an authentication possibility in the transcriptions in Appendix C. However, the NemID solution will be outfaced throughout 2022 [160]. Therefore this section focuses on the new emerging solution, MitID [161], to find the best fit for the multi-industry scenario.

MitID is a digital identification solution used in the Danish private and public sectors. The MitID platform is designed to improve security for the user compared to NemID, as well as meets the newest legal EU requirements [162] and Danish identity security standard, NSIS [163]. MitID replaces and expands together with the public sector's solutions, NemLog-in [164] and the upcoming MitID Business,

the functionality that currently lies in NemID. NemLog-in also handles the role of MitID broker for all public service providers through digital public services (e.g. taxation authorities) can get access to MitID.

When it comes to the infrastructural level, the new MitID solution interacts directly with certified MitID brokers, entities that act as an intermediary between the MitID infrastructure and service providers and also contribute to the platform's overall security. Fewer brokers reduce the number of agents who interact directly with the MitID infrastructure. In its turn, the fewer certified actors improve the digital safety of the platform [165]. MitID also supports SSO, which means that from the user perspective, there is a possibility to change from one service provider to another service provider without the need to log in multiple times. MitID supports OpenID Connect and SAML 2.0 as authentication protocols [166].

A MitID flow results in one of the NSIS [163] and eIDAS [167] defined levels of assurance. Ranging between Low, Substantial and High, they refer to the number of the authentication factors and their various combinations, which result in different strengths of the authentication process. Figure 7.1 depicts multiple combinations of authentication factors and resulting assurance levels. The underlying identity security used in identification means like MitID app, MitID code viewer/-code reader and MitID chip are expressed as a single security level.

| 2-factor / 1-factor | Password | MitID code display | MitID audio code reader | MitID app | MitID app enhanced security | MitID chip |
|---|---|---|---|---|---|---|
| **Password** | Low | Substantial | Substantial | N/A | N/A | High |
| **MitID code display** | N/A | N/A | N/A | N/A | N/A | N/A |
| **MitID audio code reader** | N/A | N/A | N/A | N/A | N/A | N/A |
| **MitID app** | N/A | N/A | N/A | Substantial | N/A | High |
| **MitID app enhanced security** | N/A | N/A | N/A | N/A | High | High |
| **MitID chip** | N/A | N/A | N/A | N/A | N/A | Low |

**Table 7.1:** MitID authenticator combinations [168]

## 7.5 Sharing technology

Throughout the State of the art in Section 4.2, multiple sharing platforms and possibilities were discovered, which can be used as the framework for information sharing in the Danish critical infrastructure. Chapter 4 shows a great opportunity for MISP to be used in this project due to its features and capabilities. In addition to the Section 4.2, multiple respondents from the interviews mentioned MISP as an information sharing platform. While primary authorities and security compa-

nies mentioned it, this is an indicator that MISP is interesting to investigate. The reasoning behind this can be that it is the authorities and security companies that primarily work with this information sharing, whereas the critical infrastructure may utilise one or the other for this.

### 7.5.1 MISP

MISP was shortly described in Section 4.2.2, which included using the TLP, different sharing possibilities and sharing formats. In addition, the section also mentions the possibility of exporting data to Intrusion Detection Systems like Snort or Suricata, which can help with awareness aspects, as discussed in the Section 4.1. MISP offers many features, of which the stakeholders also mention some during the interviews, including TLP (R20) and pseudonymous sharing (R10). This is done by sharing through another organisation, like a DCIS or CERT, meaning that they would be shown as the sharing party rather than the actual company [169]. MISP also provides access control (R4) of sharing groups (R23) and an in-built feature to assign reliability of the origin of the information shared (R30) [170].

In addition to technical features, it is possible to do data analytics with MISP as seen in Figure 7.2.

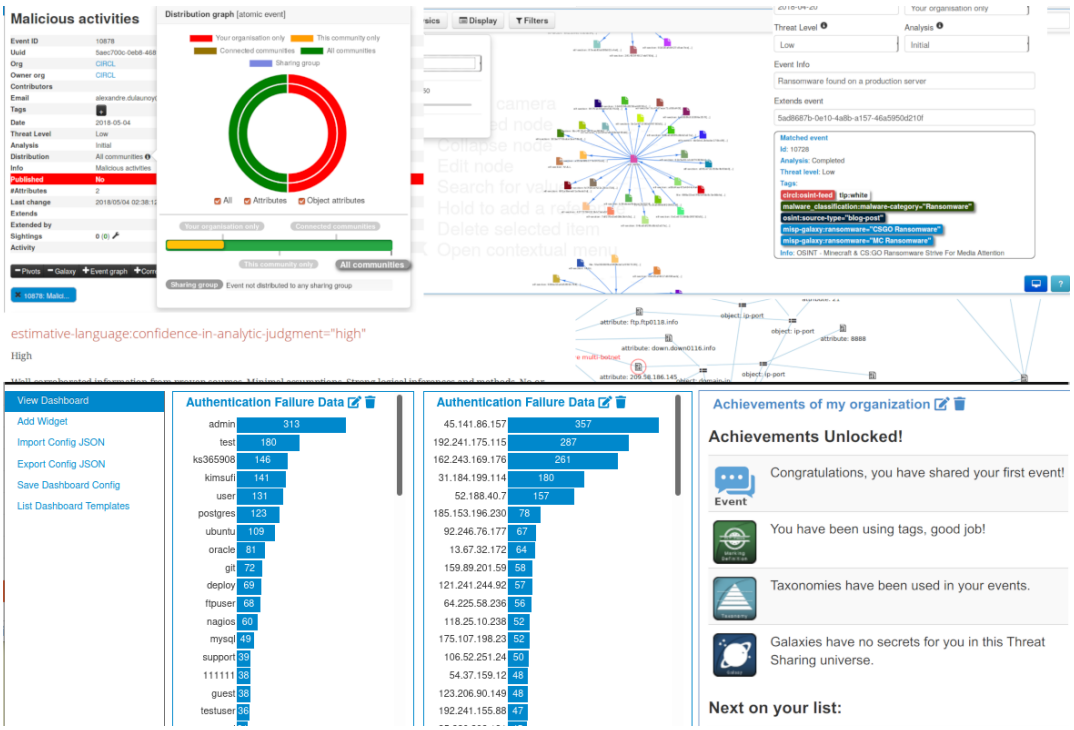


**Figure 7.2:** Example of MISP user interface [171]

It is possible to have external authentication using MISP, meaning that the built-in authentication can be replaced with other solutions if this is preferred by the developer [172]. In addition to multiple features, MISP is open source and have libraries built, such as PyMISP for Python, which enables the users to integrate the platform into their solutions [169].

### 7.5.2 STIX

STIX is supported by MISP, and the Section 4.2.2 identified it as a popular format for sharing information. This section will describe STIX as to why it is used and beneficial. STIX is a serialisation format for processing and exchanging cyber threat information and information of a similar nature. Section 4.2.2 mentions STIX briefly as a common denominator for translating raw data into graph-based object format (see Figure 7.3 showing raw data classified as objects and domains) by multiple IS platforms discussed.


**Figure 7.3:** STIX 2.0 structure example [173]

This process preserves privacy and can adapt to different degrees of data sensitivity. Levels 0 and 1 apply to less sensitive information protected by fuzzy hashing; level 2 requires more protection and encrypts data. Finally, at level 3, data is secured by implementing a PSI (Private Set Intersection) protocol [174]. In addition, automatic conversion of information into a unified format, assuming the organisation within information exchange supports STIX can strengthen common

understanding between entities and remove the burden of additional data processing into the compatible format as it uses simple JSON to serialise [173].

### 7.5.3 Mattermost

Mattermost is an open-source chat service mentioned by multiple respondents in the interviews Section 5.3. It offers file sharing, searching, and integrations as an online service hosted on the organisation's systems. This allows an organisation to use it for sensitive information as it can control where the information is being networked and stored, which can be beneficial for GDPR and data transfer regulations [137]. Mattermost also offers a paid version that can be used; however, it is hosted on their server, losing the flexibility of owning the server it is hosted on.

As mentioned, it allows integrations into other applications, which means that it could potentially be integrated into a system with MISP as the sharing platform and Mattermost as the communication part; however, this would have to be implemented by the developers of the system.

## 7.6 Summary

This chapter presents an overview of various aspects of information sharing that were brought up by both non-functional and functional requirements.

Regulations and directives were analysed, providing legal insights into digital communication. We provide an overview of directives associated with digital communication using the software for private individuals and businesses. The most important directive and regulations that might influence the IS platform's design and potentially introduce additional requirements are GDPR, NSIS and eIDAS.

Privacy and data security are part of the requirements. Thus, privacy solutions, including data protection, are discussed on a governance level by defining data policies and management and following best practices. Even strong technical security cannot ensure individuals trust other users of the platform, which is often mentioned as a key motivation for not sharing the information by the stakeholders. Technical mechanisms, however, can facilitate an increased trust, for example, using data masking and pseudonymisation.

Additionally, having the governance layer around handling the data provides transparency to the platform users, which adds to the trust aspect. When it comes to preserving data, confidentiality at transit, use, or rest can ensure the platform's users that the data is protected in case of a data leak event. Therefore, using privacy-enhancing schemes, like k-anonymity, is beneficial to the platform.

The second half of the chapter dives into the possible solutions for the platform's functions. Authentication and identification processes are examples of some of the processes that establish the aforementioned trust in technology. Finally, the

MitID solution is discussed in detail as the upcoming national identity provisioning system for both private individuals and businesses. The existing sharing technologies mentioned by stakeholders for communication and information sharing, namely MISP, STIX and Mattermost, are analysed by presenting their features as they relate to the requirements in Figure 2.2 and our final list of the functionalities for the platform.

# Chapter 8

# Framework design

This chapter starts by presenting a high-level information sharing framework concept (Section 8.1).To validate the choices we provide user perspective in Section 8.2. Taking the user's feedback into account we propose a framework guidelines for the platform in Section 8.3. The following Section 8.4 provide potential solutions, our recommendation and alternatives to them if applicable. At the end of this chapter, we present an overall framework diagram and summarise choices made within respective component sections and illustrate a suggested sharing flow Section 8.5.

## 8.1 Conceptual Design

We start this chapter with illustration of our initial concept of the sharing platform. As can be observed on Figure 8.1 we split the sharing concept into user, anything actionable and observable by user in the platform as 'front-end' and the logical technical processes happening inside the system as 'back-end'.

It shows three groups of users as previously mentioned in Section 6.1.2, Sharing flow, Joining a sharing group, Chat feature and CRUD function initiated using platform interface. It also illustrate the notification directed to users, Data processing, Storage, Logging and Authorization carried out without user interaction.

Lastly, we have Authentication which starts with user providing data in Registering and Login phases but the actual process out of user's sight. The features highlighted by yellow were further discussed during second round of user involvement.

## 8.2 Stakeholder feedback

Throughout the project, many elements to information sharing have been found. Some elements have been quite clear, such as using MISP for information sharing

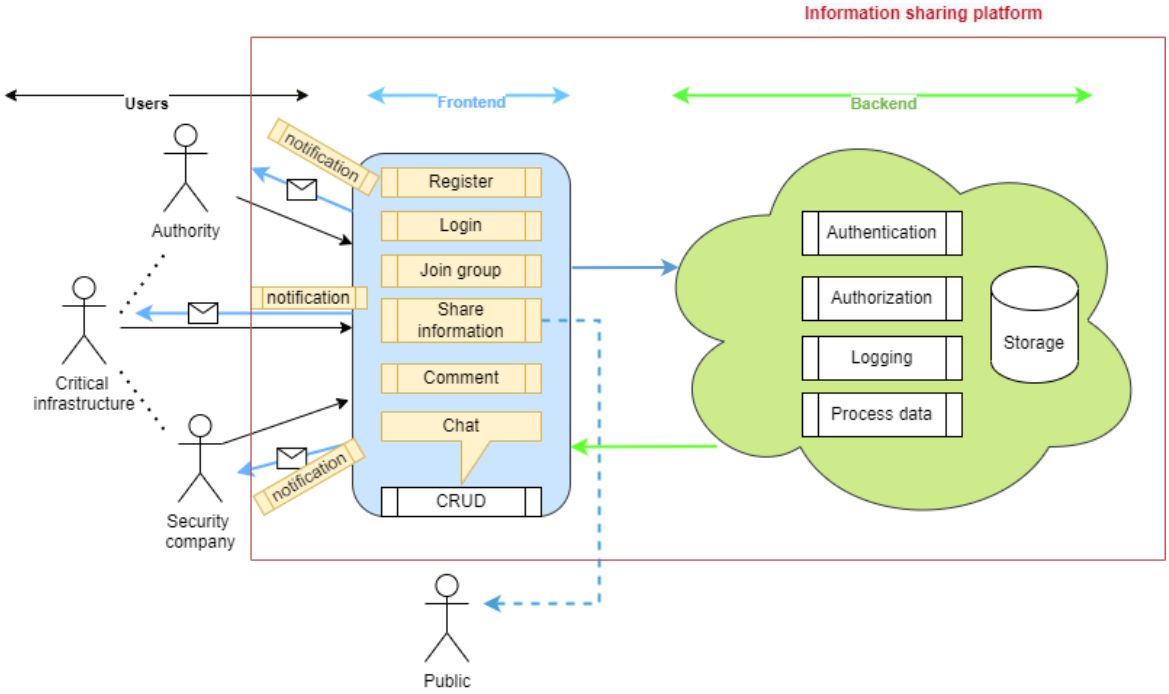


**Figure 8.1:** Conceptual design

as both the analysis and stakeholder involvement have found this to be the ideal solution. Other elements such as what authentication, who to share with, what to share and user rights have been less clear. This meant that a second round of stakeholder involvement was utilised, however, with a low number of respondents, due to the project time constraints.

Two interviews were conducted, one being online and one being physical. Neither interview was transcribed. The interviews were based on power point slides for a visual representation, which were based on the following topics:

- Solution for user authentication
- Joining sector groups
- Who to share with
- Severity, criticality & reliability of incidents shared
- Receiving notifications
- Public sharing
- Leaving a comment

**Solution for authentication** revolved around whether MitID, SSO or a custom login form should be the way to authenticate. Our initial idea was to utilise the Danish governmental identity provider due to trust as started in Section 8.4.2. This was not preferred by the stakeholders that were interviewed though, as it could have privacy concerns in terms of leaking their CPR numbers or other sensitive data. Another reason was that some organisations may have employees or partners from other countries and integrating all government identity providers may not be feasible.

Both preferred a custom authentication solution, which could be based on known technologies such as those mentioned in Section 3.2. In addition to a custom solution, SSO was also recommended for easy usage.

Both respondents mentioned that **joining a sector group** could be done automatically using industry codes which are publicly available. The other options given was manual or based on invites from the group, however, this requires an extra step for the organisation to join, making it less likely to join.

While discussing sharing groups, a question was also to **whom the incidents should be shared**. The same scenario set was presented to both respondents. Each scenario had its own set of options and context. However, all slides contained the same elements: *Scenario title, Scenario brief, Order number and task, Options and a pictogram* (illustrated in the figure in red). An example of a scenario about 'Who to share with' can be seen on Figure 8.2. Both respondents clearly expressed that custom sharing is the best approach.

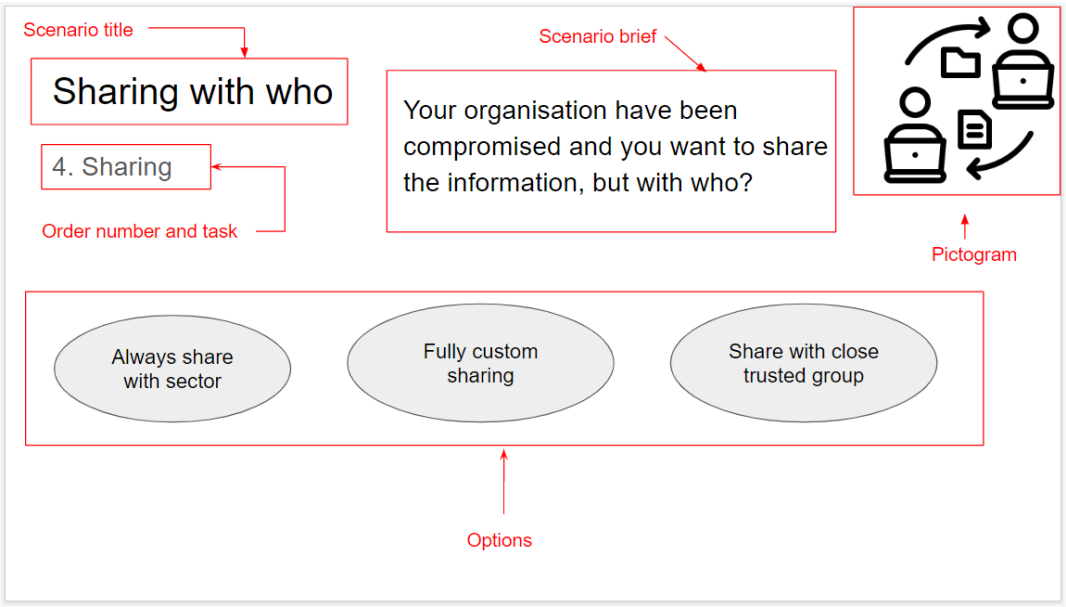


**Figure 8.2:** Slide example - Sharing with who

Many respondents in Section 5.3 have mentioned **reliability and criticality** as useful indicators of how critical a certain incident is. The question for the respondents was whether this should be based on a score that the sharer suggests based on their evaluation, the community voting or an objective score similar to that of CVSS [175]. Both an objective and community based scoring for these were seen as positive, whereas a subjective one from the company was considered negative. The primarily reason for this was that some companies may not wish to share if they are asked to suggest the criticality, as they fear being wrong in the suggestion.

In regards to **notifications**, both respondents agreed that the settings for when and how to receive these, should be controlled by the individual user and it should only be company users that should receive notifications. The reasoning behind this question was to determine if an admin should decide as it is a risk if all employees turn off notifications as this may increase response time for shared data. As mentioned above, privacy was the primary factor to limit notifications to the company and not include security companies or authorities.

The last two questions asked were 1) should it be **optional, mandatory or excluded to share with the public**? and 2) should it be possible to enter **comments on every event, only the companies' entries or no comments at all**? Both agreed that it should be optional to share with the public and that it should be possible to comment on every incident, as one user may hold additional information to be shared and linked to the incident.

## 8.3 Framework

A framework for information sharing in the Danish critical infrastructure has to consider multiple different elements (see Figure 8.3). These elements are:

- Users on the platform
- Authentication
- Access control
- Data storage
- Sharing of data
- User communication

This section will investigate these elements further based on the prior research from Chapter 4, Chapter 5 and Chapter 7, as well as feedback from the respondents in Section 8.2.

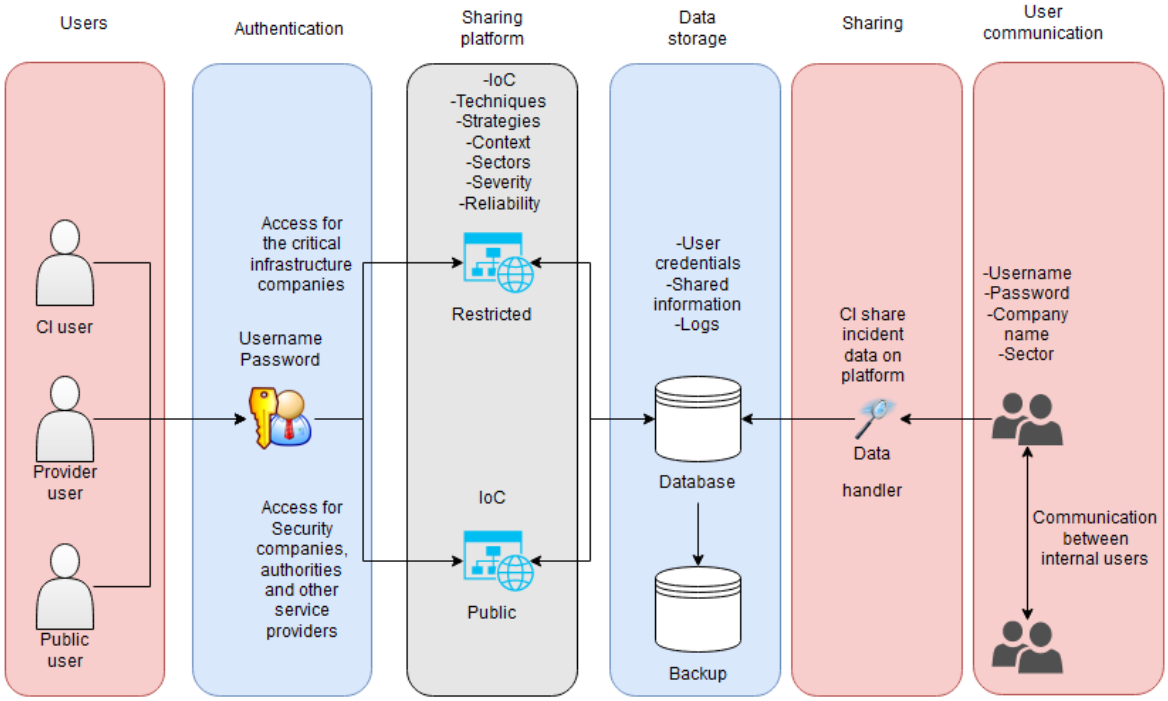


**Figure 8.3:** Framework elements

### 8.3.1 Users on the platform

The users that have access to the platform are a vital element as it alters the trust in the platform. While the technical elements can be sufficient, including confidentiality, availability and integrity, the trust in the users is essential, as stated in Section 7.3.

Different groups of users have been identified throughout the interviews, mentioned in Chapter 5 and should have access, however, with varying level of available information as stated in Access Control. The user groups identified are the following:

1. Critical infrastructure
2. CERTs and DCISs
3. Authorities
4. Security companies (partners of the critical infrastructure companies)
5. External entities (partners of the critical infrastructure companies)
   (a) External entities should be invited by the company to access the platform

   (b) The external parties should only have access to the information of the organisation that invited them and the public list of IoCs

6. The platform should automatically check new users adhere to the following criteria (based on interview transcriptions in Appendix C)
   (a) The company should have a valid CVR
   (b) The company should be part of the critical infrastructure
   (c) The company should have existed for at least one year
   (d) The company should have valid financial accounting to prove it is active

Both critical infrastructure, CERTs and DCISs makes sense as these will be the primary users of the platform. One being the main user and the two others being the current organisations available for the sectors. Additionally authorities, including governmental institutions, such as Finanstilsynet, should also have access to the platform. Security companies and external entities have the same role as being external parties for the critical companies, however, security companies will have a more active role in gathering information to defend the companies.

### 8.3.2 Authentication

Authentication increases trust as multiple respondents have mentioned they do not wish to share with the general public. Guidelines for this are as follows:

1. Such authentication must comply with the newest standards, such as those provided by NIST [176] and ISO [177].
2. The solution should offer multiple ways to authenticate Section 3.5
3. The authentication process should support the assurance levels according to NIST (Section 3.1.3) with the robustness of the authentication of minimum level of AAL2 and above. In case federated architecture is preferred, FAL3 level of assurance or above is preferred
4. The platform should offer multi-factor authentication

Having multiple ways to authenticate makes the platform more available. This can be necessary due to the diverse group of users that may access the platform. This also means that two different assurance levels have to be stated here, depending on what authentication solution is chosen.

### 8.3.3 Access Control

Access control Section 3.1.3 should take the following into account:

1. The access control should comply with relevant standards such as ISO [178] and CIS [179]
2. Sharing groups (Section 6.1.2) should be supported to enable sharing with specific users
   (a) Sector groups should have the relevant members of their sector and authorities and established for each of the NIS critical infrastructure sectors
   (b) Custom (trusted) sharing groups should be custom based on the invited members and only be created by organisation admins
   (c) The platform group is a group with all users of the platform for shared IoCs
   (d) The public group is a group with all users and unregistered entities for shared IoCs
3. The platform should allow for multiple user types (see Figure 8.4):

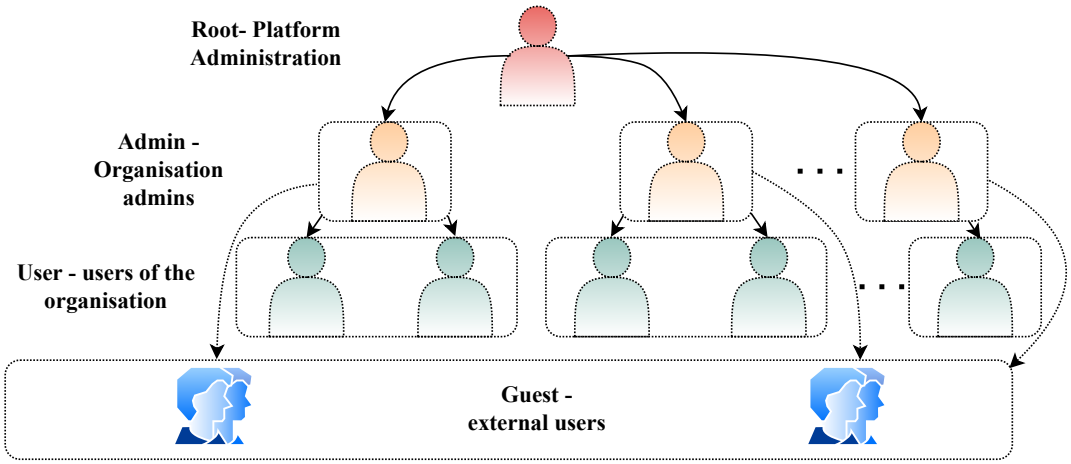


**Figure 8.4:** Suggested user roles for the information sharing platform

   (a) Platform admin - The admin and gatekeeper of the platform (respondents A4 and A6)
      i. Can administrate organisation admin and users
      ii. Can only see information from groups the super admin is part of
      iii. Can share new data in the sharing groups the super admin is part of

(b) Organisation* admin - The admin of an organisation, the user setting the organisation up for that platform (*covers critical infrastructures and authorities)
   i. Administrates the users of their organisation
   ii. Administrates external users they invite
   iii. Can only see information from groups the organisation admin is part of
   iv. Can share new data in the sharing groups the organisation admin is part of

(c) User - A user of an organisation administrated by the organisation admin
   i. Can only see information from groups the user is a part of
   ii. Can share new data in the sharing groups the user is a part of

(d) External user
   i. Can only see information from groups the external user is part of
   ii. Cannot perform CRUD operations
   iii. Can communicate with groups they are part of

(e) All user types should adhere to the policies above

4. A user should be removed from the platform if they no longer comply with the criteria in **Users on the platform**

5. An external user should be removed if they are no longer active with the organisation that invited them; see Section 8.3.2

6. Any data shared with external users should have a watermark to prove who shared this information and with whom

7. Logging
   (a) All user actions should be logged
   (b) The platform should conduct system logging
   (c) The platform should conduct security logging

Sharing should be possible with predefined groups, as well as individual entities as this may be necessary for specific incidents.

Most stakeholders have mentioned the users that should be allowed onto the platform; however, the answer varies. This is often due to the trust factor, as some companies or organisations may share or use the shared information for personal gain. This becomes a problem when for example, security companies may gain exclusive access to the site and are able to become experts in specific attack

techniques that others cannot due to lack of access. Thus, limiting the information shared can lower this problem.

Critical infrastructure should have full access as they are the ones to share and gain from such sharing.
CERTs and DCISs should have full access to their sector group as this is valuable data for them to aid other organisations within the sector.
Security companies should only have access to IoCs as this is information that can be fed into a Security Information and Event Management (SIEM) system to scan for those. While they benefit from the additional information, this can also be used to further their business, which should not be the case. A security company or authority can request further information, such as techniques, criticality and more, from the critical infrastructure companies they represent if this is needed for a particular incident.

The platform should have different user types, including the super admin being the admin creating and controlling the platform. Each organisation should be created as an entity by an employee in the organisation, and have an admin for the organisation controlling their users and external users related to the organisation.

### 8.3.4 Data storage

In order to ensure anonymity to a certain degree and comply with privacy standards such as GDPR, as mentioned in Section 7.1 and availability (Table 6.2), data storage should take the following into account:

1. All data should be encrypted with the current encryption standard, as of May 2022, AES256
2. The physical storage of data should adhere to local requirements, such as GDPR
3. The platform should adhere to GDPR and other legal directives and laws, as mentioned in Section 7.1
4. The platform should store the logs mentioned in **Access Control**
5. User data
   (a) Username, organisation, sharing groups and user type should be kept securely for each user
   (b) Password should be hashed and salted with the current standard for hashing algorithm, as of May 2022, SHA-2 256 or a later version [180]
   (c) User data should be kept at a minimum
6. Incident data

   (a) Incident data should be editable by the sharer
   (b) Incident data should stay on controlled servers
   (c) When sharing with external parties, the shared data with watermark should not be stored on the platform, but downloaded by the third party and deleted from the platform after download

7. Backup
   (a) All data should regular be backed up
   (b) The backup should be "write once read many" [181]

### 8.3.5 Sharing of data

Being the primary function of a platform (see R11 in Table 6.2) based on this framework, information sharing is required and includes what data to be shared and with whom and should take the following into account:

1. Information sharing should be automated as mentioned in Section 5.3
   (a) This should be available for security solutions such as SIEM and Antivirus, also mentioned in Section 4.1
   (b) Logparsers for the different logtypes are needed to automate this
2. The platform should use MISP for information sharing
3. The platform should support sharing incident data such as

| | |
|---|---|
| (a) IoCs | (b) IoA |
| (c) Timestamp | (d) Sector name |
| (e) Comments | (f) Description |
| (g) Attack type | (h) Reliability score |
| (i) Criticality score | (j) Threat actor |
| (k) CVE | (l) Incident severity |

4. A pseudo-anonymous method of sharing should be default, thus, opt-out and not opt-in
5. The platform should offer a criticality score
   (a) A predefined score based on the attack type
   (b) One based on feedback from the community
6. An incident should offer the possibility to set a reliability

7. Sharing should be custom and controlled by the sharer
   (a) Sharing groups
   (b) Individual organisations
8. The platform should offer notifications via mail and SMS
9. Shared information should have a time-to-live to prevent old IoCs from alerting if they are no longer active
10. Time-to-live should be based on the activity of shared information
11. The community should be able to vote on an incidents data to lower false positives and increase positives in the reliability score (Section 7.3)

During sharing, multiple data fields should be filled for better knowledge sharing. The fields criticality score, incident severity and reliability score are based on the incidents. Criticality is the impact, reliability refers to how sure a given IoC is valid and severity is the magnitude, such as minor, medium or major incidents.

### 8.3.6 User communication

To improve communication, sharing and trust among members, the platform should include chat features

1. The platform should offer a chat service for internal use
   (a) Users should be able to chat with their sector group they are part of
   (b) Users should be able to chat with other sharing groups
   (c) Users should be able to chat with individual companies

## 8.4 Component recommendation

In the following section we break down how the components of the platform presented in Figure 8.1 could be approached and why we recommend them.

### 8.4.1 Identity provisioning

To avoid a lack of overview of the identities created and removed from the platform, implementing a central unit that will manage all identity provisioning matters is a security benefit.

There exists multiple solutions that help to provide and manage identities on the platform. LDIF [182]: data interchange format-based on LDAP, Directory Services Markup Language (DSML) [183], SCIM (see Section 3.3) and others. The

usage of those depends on the solution architecture and additional modules and protocols utilised by the design choice.

**Recommendation**

Centrally managed identity and access management solution is beneficial, as it allows to have an overview of the users that have/requests access to the system. Automation of user provisioning and deprovisioning helps to spare the housekeeping tasks for user management. If the solution owners have limited resources in monitoring the access to the system, the recommendation is to outsource the provisioning to a trusted third party, otherwise implement the internal identity provisioning service.

### 8.4.2 Authentication

Based on the feedback in Section 8.2, MitID was not a preferred option, thus, the following options were considered:

- Option 1: SSO
- Option 2: Custom authentication

Single sign-on is a suggested way to authenticate the user, by implementing federation with the platform involved entities Section 3.2.1. It requires a certain flow, using the protocols discussed in the Chapter 3. The custom setup of each organisation may vary the presented authentication flow. The flow depicted in the Figure 3.6 should be considered as an example of an SSO authentication and defined in the steps described in Section 3.3.

The other option presented is custom authentication, where credentials are provided by the platform. While this solution requires users to maintain yet another set of credentials, it can also bring a layer of security to the system. By utilising, for example, the Kerberos authentication protocol Section 3.3, the system is able to authenticate users and provide a better security, as the credentials maintain cryptographic signatures.

**Recommendation**

When talking about authentication, unfortunately, there is no "one size fits all" solution. Judging solely by the stakeholders input, the identification and authentication should involve a trusted identity provider. The implementation of the Single Sign-on will permit platform entities to access the platform with the organisation credentials, providing seamless user experience as well as own security implementation.

The custom authentication, on the other hand allows to fully customise the experience for the user, security mechanisms, protocols and APIs for the authentication.

However, presented solutions cannot be seen as the direct competitors. One solution does not exclude another and the platform can support multiple types of the authentication.

### 8.4.3 Authorisation

Authorisation strategy defines mechanisms that defines the level of privileges a user will have on the platform. The rules that define the access level can be attached to both clients and resources. By checking the tags attached to the authentication request a user gets accepted or declined access to the resources. Authorisation combines two topics in itself, the authorisation protocol and the access schemes.

Protocols like Oauth2 and SAML as examples of authorisation protocols are capable to authorise clients assigning the level of permission to the platform Section 3.3. Oauth2 contains an *access_token* while SAML contains an *authorization decision assertion* which specifies if the resource can be accessed by the user.

In chapter 3 we discussed multiple authorisation schemes, yet for the information sharing scenario we suggest either of two major authorisation schemes:

- Attribute-Based Access Control (ABAC) - defines permissions based on the attributes assigned to the user/service
- Role-Based Access Control (RBAC) - permissions are assigned based on the role attached to the user in the system.

#### Recommendation

When it comes to access control, following the principle of least privilege is a well-known practice [184]. Based on the implementation differences (see Section 3.1.3), ABAC allows for a more granular access control, which impacts flexibility of the usage of the platform. Taking into consideration the framework defined access controls and Section 8.3.3 and different user roles (Figure 8.4) and sharing group access privileges the adjustable attribute based control over role based is recommended.

When it comes to the authorisation protocols, both OAuth2 and SAML can be a solution for authorisation.

### 8.4.4 Logging

Securing that the data owner/provider can track the changes in the information they shared was emphasised in the A1 stakeholder interview. To enable this feature

a 'change log' has to be implemented. According to requirement Table 6.2 we associate logging (R8) as a supporting requirement for the system security (R1).

Logging is implemented for various rationales and in different quantities depending on the purpose logs need to fulfil. This process needs to be thoroughly designed and planned from log creation and maintenance to their disposal. Logs can be generated by system-specific software like OS, firewall, and IDS, but also by database and user's actions which are fundamental components of any system.

To simplify the logging origins and purpose we identify three log types:

- Log type 1: System logs for alerting and troubleshooting (necessary)
- Log type 2: Logs generated from users' actions (partly necessary)
- Log type 3: Logs indicating system performance (optional)

**Recommendation**

According to Logging Standard [185] the logs required by any devices at the minimum, see Table 8.1, and stored at least up to six months.

| Device Type | Required Logging |
|---|---|
| All devices | • Successful and failed logon attempts<br>• Logout events<br>• Alerts raised by the access control system<br>• Activation and deactivation of protection systems (e.g. firewalls, intrusion detection systems or anti-virus software)<br>• Events raised by protection systems<br>• Initialisation, modification or deletion of audit trails<br>• User account creation, modification or deletion |
| Non-personal devices (additional requirements) | • Starting / stopping processes (services, daemons etc.)<br>• Changes to system configuration<br>• Use of privileges<br>• Errors and exceptions<br>• Alerts raised by changes in environmental conditions (high temperature, rack door opening etc.) |

**Table 8.1:** All device event logging [185]

Table 8.1 does not include performance type logs. On one hand, we see the burden in adding performance logs on the list of events the system should not

only trace but also provide storage. On the other hand, we consider the stakeholder requirement for means to measure and evaluate the performance (R33) of our proposed framework. For that reason, we suggest extending or adding a storage unit to save performance indicating logs on top of the standard recommended log types. Lastly, since R33 is only a *Could* requirement the step of adding additional log storage and even performance logs themselves should be carried out in the end-stage of the system implementation or even skipped all together to safe resources.

To sum up, the system needs to track all necessary logs from warnings, and performance indicators to users' actions. An important add-on is to ensure that implemented log framework or a custom logger does not log sensitive information.

### 8.4.5 Communication

While the chat feature is a "could have" requirement, from requirement R34 "Instant messaging/forum", it is a beneficial feature to have. Being able to communicate with other users on the platform can aid in sharing, building trust and easy communication.

It is possible to create a custom made messaging system for the platform, however this can be time consuming and add additional complexity and potential security risks to the platform. Thus, we recommend using existing solutions, namely:

- Option1: Mattermost
- Option2: Teams
- Option3: Email

#### Comparison

All three options are used by the organisations interviewed at the time of writing. Both email and Mattermost have been mentioned by multiple respondents and Teams were used for most interviews and was also mentioned as a communication solution.

They all offer many features such as secure communication, easy availability and usability. While both email and Teams are widely used by organisations and private people worldwide, Mattermost was found to be widely used too. Mattermost has the benefit of being open source and can be easily run on an organisation servers, rather than on third party servers. This allows control of the data flow while communicating with others, as well as control of the data at rest.

**Recommendation**

All three options are beneficial, Teams and email being widely used already and well integrated in many companies. Mattermost does however, allow for more transparency in where the data flows and how the system is built as it is open source, thus Mattermost is a good option for sensitive data communication such as on a sharing platform for incidents.

### 8.4.6 Storage

To save information in the platform and to display shared data, the platform needs a storage unit. Consider the following options:

- On-premise cloud
- Outsourced cloud
- Hybrid

With a growing amount of shared data that need to be stored and excessive logs, a cloud storage might be a more of a long term solution. It would be so in terms of processing and cost regulation and maintenance of large data volume.

However, when opting for a cloud solution one has to stay aware of the requirements for GDPR compliant cloud. One of the first things is to ensure control over data and data processing, and ensure that data does not leave the EU. The approach relies heavily on a resources available. Resource efficient approach is to beware and choose a cloud provider which complies with GDPR. While some of the bigger cloud providers like Google [186] and Amazon [187] provide a compliant version of their cloud service if requested. Thus, the ability to check the level of transparency decreases when selecting this approach.

On the contrary, the other approach could be to host an on-premise cloud and cover the full expense while having complete control of the situation but also taking the burden to set up such a solution and become liable if something happens.

**Recommendation**

The hybrid; a combination of self-hosted cloud and outsourced cloud is also a possibility. The setup could be to store sensitive and personal data, subject to GDPR, in local hosted storage, cloud. The remainder of the data could be stored on an outsourced cloud solution. This recommendation addresses the aforementioned concerns, however, it requires complex setup and skilful maintenance.

## 8.5 Sharing flow

Figure 8.5 illustrates a sharing flow between *User 1* sharing data and *User2* receiving the data. Firstly, *User 1* creates a data share file containing all information intended to be shared.

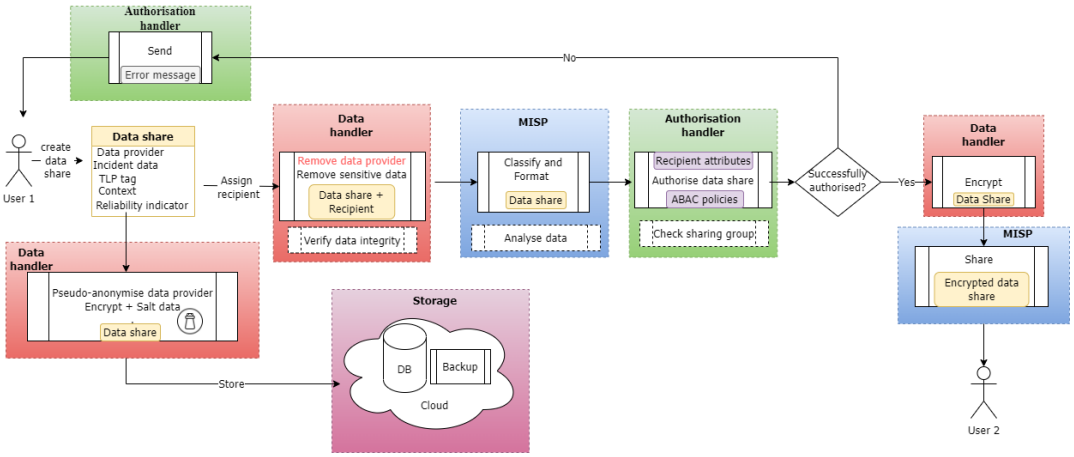


**Figure 8.5:** Suggested sharing flow

The data handler is a component responsible for encrypting data on transfer before it is sent to the respondent as well as removing the data concerning the *User 1* identity unless defined otherwise. The MISP module is responsible for data classification and formatting as well as delivering the data to the receiver. The authorisation handler utilise the access control policies (Section 8.3.3) and determines whether or not the receiver has the privilege to access the data. Lastly, all new data is encrypted and stored according to (Section 8.3.4).

## 8.6 Summary

In this chapter we presented outcomes of the second round of user involvement. Preferences on what should be part of the platform like: option for custom sharing and optional haring with public, were expressed. The user feedback came useful when determining the guidelines for the platform framework. To provide a possible solution on how the different guidelines could be implemented a set of recommendations are added. To incorporate the framework and some of the recommendations into the sharing flow Section 8.5 illustrates the scenario of sharing data between two platform users.

# Chapter 9

# Discussion

This chapter aims to discuss the choices made throughout the project and how they have influenced the outcome. Here we attempt to interpret our results, emphasise what limited our work, and give some recommendations for future research and development of the framework.

## 9.1 Reflections

This section will reflect the choices we made throughout the project. We will discuss the positive and negative influences related to those choices. Moreover, we touch upon what could have been done differently. Even though it can not be claimed with high confidence whether or not some things would improve the project, they are worth mentioning.

Firstly, we need to state that the research material and technologies included throughout the report influenced our judgment and the project's overall outcome. For example, not including unconventional technologies like blockchain in the analysis and excluding them from the recommendation set for potential solutions is certainly limiting. Despite the undeniable existence of related work in this area [188, 189], we did not consider blockchain technology as it did not come up in the literature review and stakeholders not mentioning this. However, by leveraging these materials in the state of the art, we could have introduced new dimensions to the final framework proposal.

Secondly, we look at the most influential methods utilised in the project, our process model and interviews. We took a leap of faith by introducing our process model in Section 2.1, as our model was not tested before but only inspired by other work. The fact that we have revised the process model multiple times gave us the liberty to pursue new perspectives revealed during the project. On the other hand, if we followed a strict model, we could have saved time revising, thus being more effective. For example, the initial draft of the process model included testing,

which was removed due to lack of time.

The interviews took a significant portion of our time and focus but created connections between the stakeholders and us. Nevertheless, we can say that the positive attitude of the respondents, level of detail in responses, and additional information received, which were not necessarily related to the interview questions but more as a part of the conversation, outweighed the time spent at least to a certain extent. Furthermore, the well-received initiative from the respondents led to a larger amount of interviews than we initially anticipated and planned.

To reflect on the topic of interview questions, with the knowledge and experience we have now, in the final stage of the project, we would ask different questions. When preparing the questions, we were more focused on awareness, while we would potentially omit that part altogether now and focus more on questions related to trust and the opinions on who should be in charge of gate-keeping the platform.

Another element that came up during the questionnaires and interviews was the lack of a unified definition of an incident. This included the actual meaning but also the different degrees as each company may have their own internal definition. This is also why the framework offers a predefined score of criticality, which should be based on current scoring methods, such as that of the Forum of Incident Response and Security Teams (FIRST), also mentioned in Chapter 1 [190].

In addition to things we did not expect, based on the interview outcome, we realised that the element of trust in other platform users is far more prevailing over the actual trust in the technology Sections 5.4 and 7.3. The way we decided to address things in the framework proposal was to introduce additional trust-building recommendations. In relation to that, the baseline for privacy and anonymity in our framework is set in a strict and an uncompromising way, as also seen in Section 8.3.5.

### 9.1.1 Delimitations

This project's scope focuses on the Danish scenario and conditions related to that entails a significant delimitation of this project. Even though our final proposal for a framework includes users not located in Denmark as an option, we can not claim that we have conducted the scenario of sharing worldwide sufficiently. Our background as people has potentially also influenced the project and affected the choice more than once. The legal obligation and psychology of the trust areas covered are not nearly the same level of detail as, for example, the identity and access management area. That might be because the areas we felt more confident in received more attention than those we did not. Ideally, if anything could be changed, it would be more objective when deciding on the report content.

An interesting perspective for the project to include would be investigating

how relations between the public and private sectors influence trust. Moreover, a follow-up question to ask our respondents could have been: *Who would be the best candidate to administer and be in charge of the collective information platform?* However, this was considered out of the design scope and was not prioritised. Therefore it becomes one of the delimitations for this project. Nevertheless, we deem this area a potential direction for future work and possibly necessary to explore before deploying the framework implementation in real life.

## 9.2 Limitations

Throughout the project, multiple elements have been found that limited the progression or results to various degrees.

One limitation was due to the Russia-Ukraine war. While it did not impact the project directly, it did impact the stakeholders, which impacted the interviews. Multiple stakeholders were late for the interview or could not make it for an interview due to higher cyber-attack activity, which was deemed due to the war. While no stakeholder mentioned where the cyber attacks originated from, they did mention it increased after the war started. This, in turn, decreased the number of stakeholders that were interviewed.

We also attempted to reach out to FS-ISAC [191] in terms of interviews, being a major information sharing and analysis center organisation. Being an organisation conducting information sharing with 16000 active users in 70 countries, according to their website, they would be interesting to interview as this is in the direction we also aim. They, however, replied that they do not conduct interviews regarding information sharing, and due to them being an American organisation, we chose not to pursue this further.

Finally, the most significant limitation of this project was secrecy, privacy and anonymity. While the respondents answered all interview questions, some limited their answers due to secrecy. This was also the primary reason some did not wish to be recorded and transcribed, as the information can be sensitive. This was expected from the start of the project, which is why the interview and questionnaire questions were created to be general and not too specific, to not push the respondents in terms of what they can answer.

## 9.3 Future perspective

This section will investigate and describe the elements and processes not completed in this report.

While a framework is created and multiple components have been identified and recommended, a risk analysis has not been conducted either. It is essential,

especially considering the nature of the system as an information sharing platform. Understanding one's risks, what an attacker may attempt to gain from breaching the system and the consequences, is essential for both the proposed framework and the platform that may be created based on the framework.

Validation should be done in multiple stages and with a variety of actors. While we gained some feedback, it was not based on the final framework and should be validated if additional elements are needed. Validation should be done with the stakeholders, such as critical infrastructure or DCISs and CERTs. In addition, it should be validated with security professionals and developers as to whether this system can be built and if additional elements are needed for its success.

After this validation phase, a platform should be implemented following the framework. This should then be tested, both in terms of security but also availability for the users of the platform.

In addition to the technical elements of finalising and developing the framework, an admin/owner is also necessary. As mentioned in Section 5.3, both governmental entities and cyber security companies can be troublesome. Governmental entities are subject to the access to documents in "Offentlighedsloven", and cyber security companies may attempt to monetise the platform, both mentioned by stakeholders. Both DCISs and CERTs have success establishing trust and conducting information sharing. Thus, a national CERT with no focus on a specific sector could be a solution for gathering the decentralised information and sharing it centrally.

Concerning the future in the field, additional research is required. While this report does address multiple core elements of information sharing, the psychological, economical, legal and whom to control the platform are still open questions. In terms of psychological elements, trust is essential and needed for the success of the platforms, however this can be hard to obtain, and easy to break, as stated by (A4). The economy, in terms of what the shareholders will do in case of a cyber attack, as well as fines, also needs additional research. This leaves legal and whom to control the platform, this both includes what the platform should comply with and how information sharing should be legislated in the future. This also includes who controls the platform, as this may be affected by legal constraints or lack of trust.

# Chapter 10

# Conclusion

The project dived into how information sharing in Denmark is currently conducted and how this can be improved. Before addressing the problem statement and concluding the project, we attempt to conclude all the subquestions.

When it comes to the user management and access management, it is a rather broad and complex topic. However, after research in both Chapter 3 and Chapter 7 we provide recommendations on how to build and operate a secure identity and access management environment in the multi-industry architecture. It includes identity provisioning by the trusted party, authentication via recognised secure protocols and the ABAC authorisation scheme, combined with secure storage of a user database (Section 7.3.1)

To conclude on the motivation for information sharing, we can state that the motivation is based on the fact that information sharing can increase cyber awareness and security. Regarding awareness and its influence on information sharing; it comes down to reporting incidents, as well as understanding the information that is shared between peers, as well as the type of information. Being able to get information from other organisations in regards to cyber security incident data can increase awareness and security, as to block the threats. However, it does require the individual organisations and their employees to both report and understand available information.

The most requested information by the stakeholders includes but is not limited to IoCs and IoAs, as mentioned in Section 8.3.5. Thus, they should be considered by platform users when sharing as well. Sharing non-incident data like procedures was also requested by a few stakeholders as useful, however as the platform's primary goal is to share incident data first, this should be only optional and not mandatory feature in the platform.

The security of the shared data is important, thus, anonymity and privacy became a significant part of the project. Most respondents in the interviews have mentioned anonymity as an important factor when sharing information with oth-

ers and are required for the success of a platform for information sharing (Section 8.3).

Research in different areas led to a long list of the platform requirements and relevant features for the platform. The requirements were restructured and prioritised in the final stage, Section 6.2.2. The prioritisation of the requirements helped to conclude the list of decisions for the framework design for the information sharing platform. The features of the platform are depicted in Figure 8.1.

After answering all the subquestions, the proposed framework helps to answer to the problem statement:

> ***How can a national information sharing platform for critical infrastructure in Denmark be designed?***

The framework addresses various aspects of the multi-organisational infrastructure, security, legal and trust aspects in Section 8.1. The underlying motivation was to present an alternative to the current information sharing in Denmark. We propose a solution where sectors, authorities and external parties can collaborate for the common goal of sharing and utilising information shared to protect the valuable assets and improve the incident detection and response. All in all, our suggestion offers a more centralised (compared to the current) approach to information sharing and reusing the shared information between the participants.

The project is considered a success in terms of the information gathered and the framework suggested. A big contribution in this area is a broad spectrum of the stakeholders involved. Additionally, the proposed framework spiked interest among the stakeholders. Combining academic knowledge with an industry practical approach gave this report a lot of dimensions to look into, making it broader. We can conclude that this project scoped out the problem of information sharing and suggested solution to the current challenges in this field in Denmark. Multiple respondents have mentioned additional research to be important for advancing of cyber security and information sharing, thus, supporting this project.

# Glossary

**AAL** Authenticator Assurance Level. 15

**ABAC** Attribute-Based Access Control. vi, 17, 18, 30, 101, 110

**ACM** Association for Computing Machinery. 31

**CERT** Computer emergency response team. ii, 3, 4, 5, 6, 45, 58, 59, 60, 61, 71, 85, 93, 94, 97, 109, 141, 145, 146, 147, 156, 159, 167, 168, 169, 170, 171, 172, 173, 175, 176, 178, 179, 180, 181, 194, 197, 198

**CFCS** Centre for Cyber Security. 3, 4, 5, 58, 141, 157, 159, 160, 161, 162, 171, 176

**CIRCL** CERT (Computer Emergency Response Team/Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg [123]. 40, 201

**CSIRT** Cyber Security Incident Response Team. ii, vi, viii, 3, 4, 5, 45, 78

**CTI** Cyber Threat Intelligence. 40, 43

**CYBEX** Cybersecurity Information Exchange. vi, 37, 38, 39, 42, 43

**DAC** Discretionary Access Control. vi, 17, 18

**DCIS** Decentralised Cyber Information Security. ii, 3, 5, 6, 45, 59, 60, 61, 62, 63, 85, 93, 94, 97, 109, 147, 156, 157, 158, 159, 160, 168, 169, 170, 171, 172, 175, 176, 177, 178, 181, 194, 197, 203

**ECDSA** Elliptic Curve Digital Signature Algorithm. 38

**ENISA** European Union Agency for Cyber Security [192]. 4, 81

**FAL** Federation Assurance Level. 15

**g-SIS** Group-Centric Secure Information Sharing. 42

**GDPR** General Data Protection Regulation. 40, 53, 77, 78, 79, 81, 82, 87, 97, 104

**HMAC** Hash-based Message Authentication Code. 39

**IAL** Identity Assurance Level. 15

**IDEA** Intrusion Detection Extensible Alert. 42

**IdP** Identity Provider. 20, 21, 22, 23, 24, 25, 26, 78

**IEEE** Institute of Electrical and Electronics Engineers. 31

**IoA** Indicators of attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in an attack [193]. 68, 70, 71, 74, 110

**IoC** Indicators of Compromise. 2, 55, 56, 57, 58, 60, 61, 62, 63, 65, 68, 70, 71, 72, 81, 94, 95, 97, 99, 110, 155, 156, 157, 158, 170, 173, 176, 204, 205

**IS** information sharing. viii, 2, 6, 7, 14, 31, 34, 37, 42, 43, 86, 87

**ISAC** Information Sharing and Analysis Center. 5, 38, 42, 43

**MAC** Mandatory access control. vi, 17, 18

**MISP** Malware Information Sharing Platform. iv, vi, 36, 38, 40, 42, 43, 44, 55, 56, 57, 60, 63, 65, 66, 67, 81, 84, 85, 86, 87, 88, 89, 98, 105, 155, 156, 157, 158, 170, 173, 176, 181, 185, 194, 195, 196, 197, 198, 199, 200, 202, 203, 204, 205

**NCSCFI** The National Cyber Security Centre Finland. 5

**NIS** Network and Information Systems. 2, 3, 5, 6, 78, 95, 150, 153, 154, 156, 159, 200

**NIST** National Institute of Standards and Technology. viii, 1, 2, 15, 34

**NREN** National Research and Education Network. 4, 40

**NSIS** National Standard for Identity's Security. 78, 87

**OES** Operators of Essential Services. 3, 4, 11

**OIDC** OpenID Connect. 22

**PRACIS** PRivacy-preserving and Aggregatable Cybersecurity Information Sharing [120]. 39, 42, 43, 81

**PROTECTIVE** Proactive Risk Management through Improved Cyber Situational Awareness [28]. vi, 36, 40, 41, 42, 43

**RBAC** Role-Based Access Control. vi, 17, 18, 101

**SAML** Security Assertion Markup Language. 22, 28, 101

**SIEM** Security Information and Event Management. 31, 97, 98

**SP** Service Provider. 21, 22

**SSO** Single Sign-on. 19, 20, 21, 22, 84, 100

**STIX** Structured Threat Information Expression. vii, 38, 39, 40, 41, 42, 43, 86, 88, 204, 205

**TAXII** eXchange of Indicator Information. 40

**TI** Threat intelligence. 35

**TLP** Traffic Light Protocol. 37, 40, 41, 42, 62, 81, 85

# Bibliography


[1] Check Point Blog. *Check Point Research: Cyber Attacks Increased 50% Year over Year*. https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/. 2022.

[2] Reuters. *Vestas data 'compromised' by cyber attack*. https://www.reuters.com/markets/europe/vestas-data-compromised-by-cyber-attack-2021-11-22/. 2021.

[3] *Ukrainian power grid 'lucky' to withstand Russian cyber-attack*. url=https://www.bbc.com/news/techno 61085480. Accessed:21-11-2021.

[4] *Russian Group Sandworm Foiled in Attempt to Disrupt Ukraine Power Grid*. url=https://www.darkreading.com/attacks-breaches/-russian-group-sandworm-s-attempt-to-disrupt-ukraine-power-grid-foiled. Accessed:21-11-2021.

[5] International Organisation of Standards. *Information technology — Security techniques — Information security incident management*. https://www.iso.org/standard/44379.html. 2011.

[6] Tim Grance andKaren Scarfone Paul Cichonski Tom Millar. *Computer Security Incident Handling Guide*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. 2012.

[7] Charlie C Chen, RS Shaw, and Samuel C Yang. "Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system." In: *Information Technology, Learning & Performance Journal* 24.1 (2006).

[8] Angela M. Sasse Maria Bada and Jason R.C. Nurse. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* https://arxiv.org/abs/1901.02672v1. 2019.

[9] *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN. Accessed: 19-02-2022.

[10] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. "The Importance of Information Sharing and Its Numerous Dimensions to Circumvent Incidents and Mitigate Cyber Threats 1". In: *Collaborative Cyber Threat Intelligence*. Auerbach Publications, 2017, pp. 129–186.

[11] *National strategi for cyber- og informationssikkerhed*. URL: https://fm.dk/media/25359/national-strategi-for-cyber-og-informationssikkerhed_web-a.pdf.

[12] Inho Hwang et al. "Security awareness: The first step in information security compliance behavior". In: *Journal of Computer Information Systems* 61.4 (2021), pp. 345–356.

[13] Jonathan Nield, Joel Scanlan, and Erin Roehrer. "Exploring consumer information-security awareness and preparedness of data-breach events". In: *Library Trends* 68.4 (2020), pp. 611–635.

[14] Adham Albakri, Eerke Boiten, and Rogério De Lemos. "Risks of sharing cyber incident information". In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 2018, pp. 1–10.

[15] *CSIRTs by Country - Interactive Map*. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Denmark. Accessed: 19-02-2022.

[16] *CSIRTS NETWORK MEMBERS*. https://csirtsnetwork.eu/. Accessed: 21-02-2022.

[17] *FIRST is the global Forum of Incident Response and Security Teams*. https://www.first.org/. Accessed: 21-02-2022.

[18] DKCERT. *DKCERT*. https://www.cert.dk/. 2022.

[19] *National and sectorial CSIRTs: implementation and cooperation models*. https://www.enisa.europa.eu/events/nbu-enisa-workshop-on-the-nis-directive-and-ciip/20181130-enisa-sk-coop-models. Accessed: 25-02-2022.

[20] *European Railway Information Sharing Analysis Center (ER-ISAC)*. url=https://www.enisa.europa.eu/e ERA$_{C}$*onference/enisa−era−conference−slides/8−initiatives−of−the−er−isac−devisscher.pdf*. Accessed:21-03-2021.

[21] *ISAC information sharing groups*. https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups. Accessed: 19-05-2022.

[22] *Den decentrale cyber- og informationssikkerhedsenhed for sundhedssektoren*. https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-informationssikkerhed/dcissund. Accessed: 10-03-2022.

[23] *Den decentrale cyber- og informationssikkerhedsenhed for sundhedssektoren*. https://www.finanstilsynet.dk/om-os/dcis. Accessed: 10-03-2022.

[24] *Telebranchens Decentrale Cyber- og Informationssikkerhedsenhed (Tele-DCIS)*. https://www.teledcis.dk/. Accessed: 10-03-2022.

[25] *Ny national strategi skal styrke Danmarks digitale sikkerhed*. URL: https://fm.dk/nyheder/nyhedsarkiv/2021/december/ny-national-strategi-skal-styrke-danmarks-digitale-sikkerhed/.

[26] Mille Skovgaard Hansen. "A STUDY OF THE DANISH CRITICAL INFORMATION INFRASTRUCTURE PROTECTION SYSTEMS OF GOVERNANCE". In: (2019).

[27] European Parliament. *The NIS2 Directive*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. 2021.

[28] *Requirements Capture, Specification, Architectural Design and Mode*. https://cordis.europa.eu/project/id/700071/results. Accessed: 28-02-2022.

[29] Adel Alshamrani and Abdullah Bahattab. "A comparison between three SDLC models waterfall model, spiral model, and Incremental/Iterative model". In: *International Journal of Computer Science Issues (IJCSI)* 12.1 (2015), p. 106.

[30] Wilfred Van Casteren. "The Waterfall Model and the Agile Methodologies: A comparison by project characteristics". In: *Research Gate* 2 (2017), pp. 1–6.

[31] Mitch Kramer. "Best practices in systems development lifecycle: An analyses based on the waterfall model". In: *Review of Business & Finance Studies* 9.1 (2018), pp. 77–84.

[32] Tousif ur Rehman, Muhammad Naeem Ahmed Khan, and Naveed Riaz. "Analysis of requirement engineering processes, tools/techniques and methodologies". In: *International Journal of Information Technology and Computer Science (IJITCS)* 5.3 (2013), p. 40.

[33] Chitu Okoli and Kira Schabram. "A guide to conducting a systematic literature review of information systems research". In: (2010).

[34] *Questionnaire Design | Methods, Question Types, Steps*. https://www.scribbr.com/methodology/questionnaire/. Accessed:28-02-22.

[35] Pamela Grimm. "Social desirability bias". In: *Wiley international encyclopedia of marketing* (2010).

[36] Deepti Mishra, Alok Mishra, and Ali Yazici. "Successful requirement elicitation by combining requirement engineering techniques". In: *2008 First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT)*. 2008, pp. 258–263. DOI: 10.1109/ICADIWT.2008.4664355.

[37] Michele J McIntosh and Janice M Morse. "Situating and constructing diversity in semi-structured interviews". In: *Global qualitative nursing research* 2 (2015), p. 2333393615597674.

[38] Ronald J Chenail. "Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research." In: *Qualitative Report* 16.1 (2011), pp. 255–262.

[39] Steve Campbell et al. "Purposive sampling: complex or simple? Research case examples". In: *Journal of Research in Nursing* 25.8 (2020), pp. 652–661.

[40] Ilker Etikan, Sulaiman Abubakar Musa, Rukayya Sunusi Alkassim, et al. "Comparison of convenience sampling and purposive sampling". In: *American journal of theoretical and applied statistics* 5.1 (2016), pp. 1–4.

[41] Lynne Davis and Melissa Dawe. "Collaborative Design with Use Case Scenarios". In: *Proceedings of the 1st ACM/IEEE-CS Joint Conference on Digital Libraries*. JCDL '01. Roanoke, Virginia, USA: Association for Computing Machinery, 2001, pp. 146–147. ISBN: 1581133456. DOI: 10.1145/379437.379472. URL: https://doi.org/10.1145/379437.379472.

[42] Martin Glinz. "Improving the quality of requirements with scenarios". In: *Proceedings of the second world congress on software quality*. Vol. 9. 2000, pp. 55–60.

[43] Javed Ali Khan et al. "Comparison of Requirement Prioritization Techniques to Find Best Prioritization Technique." In: *International Journal of Modern Education & Computer Science* 7.11 (2015).

[44] Sarah Hatton. "Choosing the right prioritisation method". In: *19th Australian Conference on Software Engineering (aswec 2008)*. IEEE. 2008, pp. 517–526.

[45] *MoSCoW Prioritization*. https://www.productplan.com/glossary/moscow-prioritization/. Accessed: 22-04-2022.

[46] Amjad Hudaib et al. "Requirements prioritization techniques comparison". In: *Modern Applied Science* 12.2 (2018), p. 62.

[47] JD Cem Kaner. "An introduction to scenario testing". In: *Florida Institute of Technology, Melbourne* (2013), pp. 1–13.

[48] *Access Control Models*. https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/. Accessed: 19-03-2022.

[49] Hosam Alamleh. "Unobtrusive Location-Based Access Control Utilizing Existing IEEE 802.11 Infrastructure". PhD thesis. May 2019. DOI: 10.13140/RG.2.2.34451.50725.

[50] Kim Cameron. "The laws of identity". In: *Microsoft Corp* 12 (2005), pp. 8–11.

[51] *NIST - Digital Identity Guidelines*. https://pages.nist.gov/800-63-3/sp800-63a.html. Accessed: 29-04-2022.

[52] Leslie Lamport. "Password authentication with insecure communication". In: *Communications of the ACM* 24.11 (1981), pp. 770–772.

[53] Art Conklin, Glenn Dietrich, and Diane Walz. "Password-based authentication: a system perspective". In: *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. IEEE. 2004, 10–pp.

[54] *Application Security Verification Standard 4.0*. https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf. Accessed: 19-03-2022.

[55] *Common Password List ( rockyou.txt )*. https://www.kaggle.com/datasets/wjburns/common-password-list-rockyoutxt. Accessed: 25-04-2022.

[56] James Wayman et al. "An introduction to biometric authentication systems". In: *Biometric Systems*. Springer, 2005, pp. 1–20.

[57] Himadri Biswas et al. "Smart city development: Theft handling of public vehicles using image analysis and cloud network". In: *Recent Trends in Computational Intelligence Enabled Research*. Elsevier, 2021, pp. 155–169.

[58] *FIDO2: WebAuthn & CTAPs*. https://fidoalliance.org/fido2/. Accessed:21-04-2022.

[59] Ali Abdullah S AlQahtani, Hosam Alamleh, and Jean Gourd. "0EISUA: Zero Effort Indoor Secure User Authentication". In: *IEEE Access* 8 (2020), pp. 79069–79078.

[60] Wenting Li and Ping Wang. "Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction". In: *Future Generation Computer Systems* 101 (2019), pp. 694–708.

[61] Markus Jakobsson. "Two-factor inauthentication–the rise in SMS phishing attacks". In: *Computer Fraud & Security* 2018.6 (2018), pp. 6–8.

[62] Hokeun Kim and Edward A Lee. "Authentication and Authorization for the Internet of Things". In: *IT Professional* 19.5 (2017), pp. 27–33.

[63] *Securing Linux with Mandatory Access Controls*. https://www.linux.com/news/securing-linux-mandatory-access-controls/. Accessed: 25-04-2022.

[64] Sherifdeen Lawal and Ram Krishnan. "Enabling Flexible Administration in ABAC Through Policy Review: A Policy Machine Case Study". In: *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE. 2021, pp. 69–74.

[65] *Policy Machine and Next Generation Access Control*. https://www.nist.gov/topics/identity-access-management/policy-machine-and-next-generation-access-control. Accessed: 06-03-2022.

[66] Emad F Khalaf and Mustafa M Kadi. "A Survey of Access Control and Data Encryption for Database Security". In: *Journal of King Abdulaziz University* 28.1 (2017), pp. 19–30.

[67] *Identity and Access Management (IAM)*. https://www.beyondtrust.com/resources/glossary/identity-and-access-management. Accessed: 31-03-2022.

[68] Mohammad Ghasemisharif et al. "O Single {Sign-Off}, Where Art Thou? An Empirical Analysis of Single {Sign-On} Account Hijacking and Session Management on the Web". In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018, pp. 1475–1492.

[69] Wanpeng Li and Chris J Mitchell. "Security issues in OAuth 2.0 SSO implementations". In: *International Conference on Information Security*. Springer. 2014, pp. 529–541.

[70] Christian Mainka et al. "SoK: single sign-on security—an evaluation of openID connect". In: *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 2017, pp. 251–266.

[71] *Hackers hit authentication firm Okta, customers 'may have been impacted'*. https://www.reuters.com/technology/authentication-services-firm-okta-says-it-is-investigating-report-breach-2022-03-22/. Accessed: 03-04-2022.

[72] Alejandro Pérez-Méndez et al. "Identity Federations Beyond the Web: A Survey". In: *IEEE Communications Surveys Tutorials* 16.4 (2014), pp. 2125–2141. DOI: 10.1109/COMST.2014.2323430.

[73] Jesus Carretero et al. "Federated identity architecture of the European eID system". In: *IEEE Access* 6 (2018), pp. 75302–75326.

[74] *Federated Identity Management vs. Single Sign-On: What's the Difference?* https://www.okta.com/identity-101/federated-identity-vs-sso/. Accessed: 16-04-2022.

[75] *OpenID Connect Federation Progress*. https://openid.net/2019/06/25/openid-connect-federation-progress/. Accessed: 02-04-2022.

[76] Abdramane Bah et al. "Federation of Services from Autonomous Domains with Heterogeneous Access Control Models". In: *International Information Security Conference*. Springer. 2019, pp. 83–98.

[77] *Trust Topologies and Security Token Issuance*. https://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html. Accessed: 02-04-2022.

[78] Oracle. *What is Security Assertion Markup Language (SAML)?* https://www.oracle.com/security/cloud-security/what-is-saml/. 2021.

[79] Peter Loshin. *Security Assertion Markup Language (SAML)*. https://www.techtarget.com/searchsecurity/definition/SAML. 2021.

[80] *eXtensible Access Control Markup Language (XACML), Version 3.0, OASIS Standard*. https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html#_Toc325047134. Accessed:28-03-2022.

[81] *The OAuth 2.0 Authorization Framework*. https://datatracker.ietf.org/doc/html/rfc6749. Accessed:28-03-2022.

[82] *OAuth 2.0 Authorization Framework*. https://auth0.com/docs/authenticate/protocols/oauth. Accessed: 30-04-2022.

[83] *Which OAuth 2.0 Flow Should I Use*. https://auth0.com/docs/get-started/authentication-and-authorization-flow/which-oauth-2-0-flow-should-i-use. Accessed: 30-04-2022.

[84] *What is OpenID Connect?* https://openid.net/connect/. Accessed:28-03-2022.

[85] *OpenID Connect Scopes*. https://auth0.com/docs/get-started/apis/scopes/openid-connect-scopes. Accessed:17-04-2022.

[86] *RADIUS Servers and Parameters for Subscriber Access*. https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/radius-servers-parameters-options.html. Accessed: 19-04-2022.

[87] *Diameter Base Protocol*. https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/diameter-base-protocol.html. Accessed: 19-04-2022.

[88] *Kerberos: The Network Authentication Protocol*. https://web.mit.edu/kerberos/. Accessed:02-03-2022.

[89] *Encryption types*. https://web.mit.edu/kerberos/krb5-latest/doc/admin/enctypes.html. Accessed: 03-03-2022.

[90] *Problem Statement on the Cross-Realm Operation of Kerberos*. https://datatracker.ietf.org/doc/html/rfc5868#page-5. Accessed: 02-04-2022.

[91] Network Encyclopedia. *X.500 - Network Encyclopedia*. https://networkencyclopedia.com/x-500/. 2021.

[92] Microsoft. *What is LDAP?* https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ldap/what-is-ldap. 2018.

[93] Ed. J. Sermersheim. *Lightweight Directory Access Protocol (LDAP): The Protocol*. https://docs.ldap.com/specs/rfc4511.txt. 2006.

[94] ldap. *LDAP.com Lightweight Directory Access Protocol*. https://ldap.com. 2020.

[95] *Introduction to System for Cross-domain Identity Management (SCIM)*. https://medium.com/identity-beyond-borders/system-for-cross-domain-identity-management-scim-def45ea83ae7.

[96] Federica Paci Stephen Hart Andrea Margheri and Vladimiro Sassone. *Riskio: A Serious Game for Cyber Security Awareness and Education*. https://reader.elsevier.com/reader/sd/pii/S0167404820301012?token=A7C682D50E0758DE07F6AD020EF0F819BE0 originRegion=eu-west-1&originCreation=20220323221223. 2020.

[97] Hamid Al-Hamadi and Ing Ray Chen. "Trust-Based Decision Making for Health IoT Systems". In: *IEEE Internet of Things Journal* 4.5 (2017), pp. 1408–1419. DOI: 10.1109/JIOT.2017.2736446.

[98] Moti Zwilling et al. "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study". In: *Journal of Computer Information Systems* 62.1 (2022), pp. 82–97. DOI: 10.1080/08874417.2020.1712269. eprint: https://doi.org/10.1080/08874417.2020.1712269. URL: https://doi.org/10.1080/08874417.2020.1712269.

[99] Dan DeBeaublen and Lance Spitzner. *2021 SECURITY AWARENESS REPORT MANAGING HUMAN CYBER RISK*. https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/. 2021.

[100] Jemal Abawajy. "User preference of cyber security awareness delivery methods". In: *Behaviour & Information Technology* 33.3 (2014), pp. 237–248. DOI: 10.1080/0144929X.2012.708787. eprint: https://doi.org/10.1080/0144929X.2012.708787. URL: https://doi.org/10.1080/0144929X.2012.708787.

[101] Ponnurangam Kumaraguru et al. "Protecting people from phishing: the design and evaluation of an embedded training email system". In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2007, pp. 905–914.

[102] proofpoint. *proofpoint*. https://www.proofpoint.com/us. 2022.

[103] Microsoft. *Empowering your remote workforce with end-user security awareness*. https://www.microsoft.com/security/blog/2020/05/13/empowering-remote-workforce-security-training/. 2020.

[104] PhishGuru. *PhishGuru: Learn How to Spot a Dangerous Email*. https://www.rtt.com/technology-articles/phishguru-email-tool.html. 2022.

[105] Priscilla Koepke. "Cybersecurity information sharing incentives and barriers". In: *Sloan School of Management at MIT University: Cambridge, MA, USA* (2017).

[106] Jason Mallinder and Peter Drabwell. "Cyber security: A critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber attack". In: *Journal of business continuity & emergency planning* 7.2 (2014), pp. 103–111.

[107] Chris Johnson et al. "NIST special publication 800-150: guide to cyber threat information sharing". In: *NIST, Tech. Rep* (2016).

[108] Vasil Rizov. "Information sharing for cyber threats". In: *Information & Security* 39.1 (2018), pp. 43–50.

[109] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing". In: *Computers & Security* 60 (2016), pp. 154–176.

[110] Wanying Zhao and Gregory White. "A collaborative information sharing framework for community cyber security". In: *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE. 2012, pp. 457–462.

[111] Ram Krishnan et al. "Group-centric secure information-sharing models for isolated groups". In: *ACM Transactions on Information and System Security (TISSEC)* 14.3 (2011), pp. 1–29.

[112] David FC Brewer and Michael J Nash. "The Chinese Wall Security Policy." In: *IEEE symposium on security and privacy*. Vol. 1989. Oakland. 1989, p. 206.

[113] Wanying Zhao and Gregory White. "Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security". In: *2014 47th Hawaii International Conference on System Sciences*. 2014, pp. 1987–1996. DOI: 10.1109/HICSS.2014.252.

[114] Wanying Zhao and Gregory White. "An evolution roadmap for community cyber security information sharing maturity model". In: *Proceedings of the 50th Hawaii international conference on system sciences*. 2017.

[115] Iman Vakilinia, Deepak K Tosh, and Shamik Sengupta. "Attribute based sharing in cybersecurity information exchange framework". In: *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*. IEEE. 2017, pp. 1–6.

[116] Intan Maratus Sholihah, Hermawan Setiawan, and Olga Geby Nabila. "Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform". In: *2021 Sixth International Conference on Informatics and Computing (ICIC)*. IEEE. 2021, pp. 1–6.

[117] Lucienne TM Blessing and Amaresh Chakrabarti. *DRM: A design reseach methodology*. Springer, 2009.

[118] Farhan Sadique et al. "A system architecture of cybersecurity information exchange with privacy (cybex-p)". In: *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE. 2019, pp. 0493–0498.

[119] Farhan Sadique et al. "Cybersecurity Information Exchange with Privacy (CYBEX-P) and TAHOE–A Cyberthreat Language". In: *arXiv preprint arXiv:2106.01632* (2021).

[120] José M de Fuentes et al. "PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing". In: *computers & security* 69 (2017), pp. 127–141.

[121] Caroline Fontaine and Fabien Galand. *A Survey of Homomorphic Encryption for Nonspecialists*. `https://link.springer.com/content/pdf/10.1155/2007/13801.pdf`. 2007.

[122] IBM. *Format preserving encryption*. `https://www.ibm.com/docs/en/linux-on-systems?topic=services-format-preserving-encryption`. 2022.

[123] *MISP - Open Source Threat Intelligence Platform*. `https://www.circl.lu/services/misp-malware-information-sharing-platform/`. Accessed: 27-02-2022.

[124] Cynthia Wagner et al. "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform". In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. WISCS '16. Vienna, Austria: Association for Computing Machinery, 2016, pp. 49–56. ISBN: 9781450345651. DOI: 10.1145/2994539.2994542. URL: https://doi.org/10.1145/2994539.2994542.

[125] *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. `https://www.enisa.europa.eu/publications/cybersecurity-information-sharing`. Accessed: 27-02-2022.

[126] *TAXII™ Version 2.1*. `https://docs.oasis-open.org/cti/taxii/v2.1/csprd01/taxii-v2.1-csprd01.html`. Accessed: 27-02-2022.

[127] *Proactive Risk Management through Improved Cyber Situational Awareness*. `https://cordis.europa.eu/project/id/700071/results`. Accessed: 01-03-2022.

[128] Sindre Rolstad, John Adler, and Anna Rydén. "Response burden and questionnaire length: is shorter better? A review and meta-analysis". In: *Value in Health* 14.8 (2011), pp. 1101–1108.

[129] Atlassian. *Understanding incident severity levels*. `https://www.atlassian.com/incident-management/kpis/severity-levels`.

[130] Foresite. *Classifying the severity of a cyber incident*. https://foresite.com/classifying-the-severity-of-a-cyber-incident/. 2021.

[131] Indeed Editorial Team. *How To Schedule the Best Time to Interview*. https://www.indeed.com/career-advice/interviewing/best-time-to-interview. 2021.

[132] Justitsministeriet. *Bekendtgørelse af lov om offentlighed i forvaltningen*. https://www.retsinformation.dk/eli/lta/2020/145.

[133] Valentina Lenarduzzi and Davide Taibi. "MVP explained: A systematic mapping study on the definitions of minimal viable product". In: *2016 42th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. IEEE. 2016, pp. 112–119.

[134] *Digital Operational Resilience Act ('DORA')*. https://www.aima.org/regulation/keytopics/digital-operational-resilience-act.html#:~:text=DORA. Accessed: 22-05-2022.

[135] *Company law and corporate governance*. https://ec.europa.eu/info/business-economy-euro/doing-business-eu/company-law-and-corporate-governance_en. Accessed: 04-05-2022.

[136] *The NIS2 Directive. A high common level of cybersecurity in the EU*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Accessed: 05-05-2022.

[137] *General Data Protection Regulation*. https://gdpr-info.eu//. Accessed: 03-05-2022.

[138] *National Standard for Identity Assurance Levels (NSIS) Version 2.0.1a*. https://digst.dk/media/24697/nsis-engelsk-version-201a.pdf. Accessed: 05-05-2022.

[139] *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016) Version 2.0.1a*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. Accessed: 05-05-2022.

[140] *The NIS2 Directive: A high common level of cybersecurity in the EU*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333. Accessed: 05-05-2022.

[141] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union*. https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_laying_down_measures_on_cybersecurity_at_euibas.pdf. Accessed: 09-05-2022.

[142] *PRIVACY FRAMEWORK - A tool to help organizations improve individuals' privacy through enterprise risk management*. https://www.nist.gov/privacy-framework. Accessed: 15-05-2022.

[143] *OneTrust - Privacy Program Best Practices*. https://www.onetrust.com/blog/privacy-program-best-practices/. Accessed: 15-05-2022.

[144] *General Data Protection Regulation*. https://gdpr-info.eu/art-5-gdpr/. Accessed: 13-05-2022.

[145] *Art. 25 GDPRData protection by design and by default*. https://gdpr-info.eu/art-25-gdpr/. Accessed: 03-05-2022.

[146] *7 Principles of Privacy By Design*. https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce. Accessed: 15-05-2022.

[147] *Public Private Partnerships (PPP) - Cooperative models*. https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperative-models-for-effective-ppps/. Accessed: 05-04-2022.

[148] Florian Skopik and Qin Li. "Trustworthy incident information sharing in social cyber defense alliances". In: *2013 IEEE Symposium on Computers and Communications (ISCC)*. IEEE. 2013, pp. 000233–000239.

[149] *MISP taxonomies and classification as machine tags*. https://www.misp-project.org/taxonomies.html#_misp_taxonomies. Accessed: 04-05-2022.

[150] *Pseudonymisation techniques and best practices*. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices. Accessed: 12-05-2022.

[151] *Pseudonymisation techniques and best practices*. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices. Accessed: 22-05-2022.

[152] Samson Esayas. "The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing'approach". In: *European Journal of Law and Technology* 6.2 (2015).

[153] Jinbao Wang, Zhipeng Cai, and Jiguo Yu. "Achieving personalized *k*-anonymity-based content privacy for autonomous vehicles in CPS". In: *IEEE Transactions on Industrial Informatics* 16.6 (2019), pp. 4242–4251.

[154] Guowei Qiu, Xiaolin Gui, and Yingliang Zhao. "Privacy-Preserving Linear Regression on Distributed Data by Homomorphic Encryption and Data Masking". In: *IEEE Access* 8 (2020), pp. 107601–107613. DOI: 10.1109/ACCESS.2020.3000764.

[155] Djordje Slijepčević et al. "k-Anonymity in practice: How generalisation and suppression affect machine learning classifiers". In: *Computers & Security* 111 (2021), p. 102488.

[156] *Dynamic Data Masking*. https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15. Accessed: 14-05-2022.

[157] *Get started with SQL Database dynamic data masking with the Azure portal*. https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-configure-portal?view=azuresql. Accessed: 14-05-2022.

[158] *Share data securely across Regions using Amazon Redshift data sharing*. https://aws.amazon.com/blogs/big-data/share-data-securely-across-regions-using-amazon-redshift-data-sharing/. Accessed: 14-05-2022.

[159] *The NemID code app makes digitally self-service easier.* https://www.nemid.nu/dk-en/. Accessed: 28-04-2022.

[160] *MitID is replacing NemID*. https://www.mitid.dk/en-gb/about-mitid/news/today-nemid-becomes-mitid/. Accessed: 30-04-2022.

[161] *NemID becomes MitID*. https://www.mitid.dk/en-gb/. Accessed: 28-04-2022.

[162] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. Accessed: 30-04-2022.

[163] *NSIS*. https://digst.dk/it-loesninger/standarder/nsis/. Accessed: 30-04-2022.

[164] *NemLog-in*. https://digst.dk/it-loesninger/nemlog-in/. Accessed: 30-04-2022.

[165] *What is the difference between the two eIDs at an infrastructural level?* https://penneo.com/blog/nemid-to-mitid/#infrastructural-difference. Accessed: 30-04-2022.

[166] *Protocols and attributes*. https://developer.signicat.com/enterprise/identity-methods/mitid/integration.html#supported-protocols. Accessed: 30-04-2022.

[167] *eIDAS Regulation*. https://digst.dk/it-loesninger/standarder/nsis/. Accessed: 03-05-2022.

[168] *Level of assurance and authenticators*. https://developer.signicat.com/enterprise/identity-methods/mitid/loa.html#nsis. Accessed: 30-04-2022.

[169] *MISP FEATURES AND FUNCTIONALITIES*. https://www.misp-project.org/features/. Accessed: 09-05-2022.

[170] Cynthia Wagner et al. "Misp: The design and implementation of a collaborative threat intelligence sharing platform". In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*. 2016, pp. 49–56.

[171] *VISUALIZATION DASHBOARDS*. https://www.misp-project.org/. Accessed: 09-05-2022.

[172] *Summary*. https://www.circl.lu/doc/misp/appendices/. Accessed: 09-05-2022.

[173] Farhan Sadique et al. "Automated structured threat information expression (stix) document generation with privacy preservation". In: *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE. 2018, pp. 847–853.

[174] Hao Chen, Kim Laine, and Peter Rindal. "Fast private set intersection from homomorphic encryption". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, pp. 1243–1255.

[175] *CVE Vulnerability*. https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/#:~:text=CVE%20is%20a%20glossary%20that,prioritizing%20the%20security%20of%20vulnerabilities.. Accessed: 25-05-2022.

[176] *Digital Identity Guidelines - Authentication and Lifecycle Management*. https://pages.nist.gov/800-63-3/sp800-63b.html. Accessed: 19-05-2022.

[177] *Information technology — Security techniques — Entity authentication — Part 1: General*. https://www.iso.org/standard/53634.html. Accessed: 19-05-2022.

[178] *ISO/IEC 27000:2018*. https://www.iso.org/standard/73906.html. Accessed: 29-05-2022.

[179] *CIS Critical Security Control 6: Access Control Management*. https://www.cisecurity.org/controls/access-control-management. Accessed: 29-05-2022.

[180] *Hash Functions*. https://csrc.nist.gov/projects/hash-functions. Accessed: 29-05-2022.

[181] *How To Prevent Data Tampering In Your Business*. https://www.cypressdatadefense.com/blog/data-tampering-prevention/. Accessed: 22-05-2022.

[182] *LDAP data interchange format (LDIF)*. https://www.ibm.com/docs/en/i/7.4?topic=reference-ldap-data-interchange-format-ldif.

[183] *Directory Services Markup Language (DSML) identity feed*. https://www.ibm.com/docs/en/sim/7.0.1?directory-services-markup-language-dsml-identity-feed.

[184] *Grant least privilege*. https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege. Accessed: 22-05-2022.

[185] *STANDARD ON LOGGING AND MONITORING*. https://docplayer.net/9024510-Standard-on-logging-and-monitoring.html. Accessed: 17-05-2022.

[186] *Google Cloud the General Data Protection Regulation (GDPR)*. https://cloud.google.com/privacy/gdpr. Accessed: 21-05-2022.

[187] *GDPR compliance when using AWS services*. https://aws.amazon.com/compliance/gdpr-center/. Accessed: 21-05-2022.

[188] Nikolaos Alexopoulos et al. "TRIDEnT: Towards a Decentralized Threat Indicator Marketplace". In: *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. New York, NY, USA: Association for Computing Machinery, 2020, pp. 332–341. ISBN: 9781450368667. URL: https://doi.org/10.1145/3341105.3374020.

[189] Nikolaos Alexopoulos et al. "Towards blockchain-based collaborative intrusion detection systems". In: *International Conference on Critical Information Infrastructures Security*. Springer. 2017, pp. 107–118.

[190] *CSIRT Case Classification (Example for Enterprise CSIRT)*. https://www.first.org/resources/guides/csirt_case_classification.html. Accessed: 27-05-2022.

[191] *Safeguarding the Global Financial System by Reducing Cyber Risk*. https://www.fsisac.com/. Accessed: 26-05-2022.

[192] *European agency for Cybersecurity*. https://www.enisa.europa.eu/. Accessed: 27-05-2022.

[193] Crowdstrike. *IOA VS IOC*. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/.

# Appendix A

# Questionnaire

## A.1 Questions

**Q1: How many cyber security incidents do you estimate your company have had the past 12 months?**

☐ No incidents

☐ 1-10

☐ 11-50

☐ 51-100

☐ More

☐ I am not allowed to Answer

**Q2: Do you share minor and middle size incidents (based on your company classification level for incidents) with external entities?**

☐ Yes

☐ No

☐ I am not allowed to answer

**Q3: Do you share major cyber incidents (based on your company classification level for incidents) with external entities?**

☐ Yes

☐ No

☐ I am not allowed to answer

**Q4: Do you have interest in other entities within the critical infrastructure sharing information regarding cyber security incidents with your company?**

☐ Yes

☐ No

☐ I am not allowed to answer

**Q5: Do you have any internal process for reporting cyber security incidents?**

☐ Yes

☐ No

☐ I am not allowed to answer

**Q6: Would you like to share additional comments?**

# Appendix B

# Interview Questions

## B.1 Critical infrastructure questions

1. Can you tell me what is your role in regards to incident management and information sharing?
2. In your experience in your current company, what are the positive and negative elements about information sharing?
    - What is the motivation to share or not disclose occurring cyber incidents?
3. Can you describe the process of information sharing in your company using a few steps?
4. What information do you share (internally or externally)?
    - Authorities (Danish, other)
    - Security company
    - Other companies
    - Are you aware of what reporting obligations your company has?
5. Do you have procedures where the employees can report incidents/suspicious activities?
    - Do you have any kind of training program regarding cyber incident awareness?
6. Could you describe the ideal information sharing system for your company?
    - What information to be shared
    - Data handling (Anonymity, encryption)

- Who to share it with
- Automation/efficiency

## B.2 Authorities questions

1. Can you tell me what is your role in regards to incident management and information sharing?
2. Are any of your customers in terms of cyber security, in the critical infrastructure?
3. In case of a cyber security incident what information is important for you to be shared?
4. Where is this information shared for the incidents within critical infrastructure companies?
    - Platforms, certs, authorities, internal, other companies
5. How do you establish and manage trust between the parties?
6. While talking to your customers, is awareness of preventing cyber attacks important and does this awareness include information sharing?
    - To what extent is information sharing mentioned
7. Could you describe the ideal information sharing system for your company?
    - What information to be shared
    - Data handling (Anonymity, encryption)
    - Who to share it with
    - Automation/efficiency

## B.3 Security company questions

1. Can you tell me what is your role in regards to incident management and information sharing?
2. In case of a cyber security incident what information is important for you to be shared?
3. Where is the information about the incidents shared?
4. What is the status of awareness from companies in terms of information sharing

5. Are the company/(companies) prepared and do they know the legal requirements to disclose?
6. Do you collaborate with other entities? And how do you establish and manage trust?
    - CERTs/CSIRTs
    - Companies (what kind of companies)
    - Authorities
    - DCIS
7. Could you describe the ideal information sharing system for your organisation?
    - What information to be shared
    - Data handling (Anonymity, encryption)
    - Who to share it with
    - Automation/efficiency

## B.4 Expert interview questions

1. How did this initiative start?
2. How many do you have as part of the MISP?
3. How do you ensure trust with the "clients"?
4. How do you make sure that a company is who they say they are?

# Appendix C

# Interview transcriptions

## C.1 Critical infrastructure

### C.1.1 Interview, respondent CI1

Interviewer (further I): Hi and thank you for participating in our interview. And before we start I would like to ask you for your consent to record this conversation
Respondent (further R):Yes, you are allowed.
I: Thank you,
R:Thank you,
I: All right. So, before we start the interview, let me briefly introduce you to the concept of our project. Just one more time... As you know we are creating a framework for cyber security incident information sharing for all the critical infrastructures in Denmark. For each of the sectors. And we invited you here because we would like to get first-hand input from the potential users and stakeholders, and how it will benefit them. We hope you can help us to understand the needs of the companies with your experience. So without further ado, Let's start with the first question.
R: Yes,
I: Can you tell me what is your role in regards to incident management and information sharing?
R: Ah... so, basically I am in information sharing. I am interacting with the users in the *our organization*. And that could be like again... *users* or pretty much everyone responsible for the IT, more or less. That's sort of information sharing I do.
I: So you do the internal information sharing?
R: Yeah.
I: Cool. So, in your experience and in your current company, what are the positive and negative moments about information sharing?

R: Since I work in a *naming the place of work*, there has always been this controversy about the *platform designed for our sector*. That, you know, it violates the privacy laws and rules and stuff, that it could possibly be the spectacle (note: subject) to breaches and stuff... so that is the biggest concern.
I: OK.
R: It should be said, I don't have anything to do with the platform directly, but it's more in regards to users who works there.
I: OK, and what do you think is the biggest motivation to share or to disclose the information about the cyber security incidents? What is the biggest motivation?
R: The biggest motivation, definitely, is to bring awareness of the issues. You know if you keep it in locks, and no one says anything about it, then there is no way to try to identify if there is another similar attack happening.
I: That's true. OK, so can you describe the process of information sharing in your company using a few steps? How do you normally share the information that something happened? An incident or ...
R: So, usually, it is a very centralised system, actually, so if you write anything and as soon as you save then it is visible to pretty much everyone in the organisation.
I: "Everybody"? So like coworkers? (anonymized)
R: It is actually for everybody... ammm... I am pretty sure it is everybody. So, if I, for instance, go into the server room, and I patch some cables to get some Internet, when I note that down, anyone can really see that: ok, this guy or I have installed some Internet in this room and this is the identification of the ethernet port. Something like that.
I: So they know that it's your work and you have been there.
R: Exactly. I am pretty sure, they can also, you know, tune the network. They can pretty much see, what you are doing.
I: Right, but you mentioned that *a user* would tell you that everything is not working, or they might suspect that there is an attack, how would the process happen for them to tell you. Will they come to you physically? Will they send an email?
R: Email is most likely.
I: Press the emergency button?
R: I don't think there is an emergency button there. I think they will pretty much mail me saying that "I might suspect that I get hacked", and then once it has been brought up, I will be forwarding it to someone "higher up", because our office is a local one. But we have central department a lot further away and I would assume that they handle all the cyber security issues.
I: Cool. All right. So if you know that there is some cyber security incident happened, what information do you share internally or externally? For example, do you show something to the authorities or show it to the security people?
R: Definitely the authorities. Since we are a government run enterprise, we defi-

nitely notice that. Also the security company notices that, because you know, we have so much software, that is run by other security companies, that they also need to be aware of.
I: I don't know if you can disclose, what security companies operate or help you to operate the company?
R: I mean, we do have some of the companies, that, you know, we use for authentication purposes, for the sign on. There is a company called "company", it's an American based company, and they are basically specialising on the *naming the sector* sector for authenticating stuff, like sign on, and such like that. There is also a cloud solution, such as *name of the company*, they also play a major part in our cyber security.
I: Yeah, and if there is a problem and you need to contact them, will you write an email to them, or are you writing it to your security people?
R: The security people. They will get in touch with the companies.
I: Ok, cool. Do you have any sort of procedures, standardised procedures, or is it always an email? Maybe some sort of a centre where a user can report an incident? So, how do users report incidents?
R: Can you repeat the question again?
I: Yeah, so, do you have any specific procedures where the employee can report an incident or any suspicious activities?
R: No-no, there are no other than sending an email or calling.
I: Ok, yeah. That's a very nice one. Do you have any sort of awareness training? Like telling the *users* not to click any emails or for *users* not to click anything? Do you have any awareness problem? "Please, don't touch it, report it."
R: We sometimes run some campaigns, because you know, when you log on, there is a front page (*meaning login page). And I think back in October we have a campaign where you could run both, where you could try to identify phishing emails and we gave them (users) hints to look for. For example, if it's a proper language, or the grammar is right, or email origin is a bit suspicious. Stuff like that.
I: Yeah, super cool. I just have the last question to you. So, imagine this platform where a lot of incidents can be reported by different sectors of critical infrastructure. How would you ideally imagine that this platform looks like? So, what information you would like to share? How and whom to share it with, and how efficient it should be? Just anything in your mind.
R: It would definitely be somewhat, like, you know, like if you try to report a bug. A bug report. Something like that, but maybe on a more technical scale. Specify user specification, Like what do you suspect is the type of attack, or some sublimitive (*sugestive) questions like "where do you think attack originates from?" Things like that.
I: Yeah.
R: A little more advanced version of a bug report.

I: Yeah, and this will be shared... whom do you think this will be shared with? Or good to shared with?
R: Probably the authorities. I think companies are more willing to trust authorities Private companies, (shaking his head) I am not sure about that, but that is what I would assume.
I: Thank you very much for your answers. Thank you for having me and having this interview.
R: You are welcome.

### C.1.2 Interview respondent CI2

Interviewer (further I): So, is it OK if I record it?
Respondent (further R): Yes, yes.
I: Thank you, so, before I start, I would like to introduce you to what we want to do, just a couple of sentences and then we can proceed with the questions.
R: Yes.
I: We want to create a framework for a cyber incident information sharing, in terms of critical infrastructures in Denmark regardless the sector.
R: Yeah.
I: So that is why we invited you here today to get some kind of first hand input for what people would like to use it for. You are kind of a user or stakeholder for the system if we create something like that.
R: OK.
I: And then we hope that your experience with working in the company can help us understand a little bit more of it.
R: Yeah.
I: And as we agreed it is going to be anonymous, so I am not going to mention your name or the company. I am just going to ask generally the questions.
R: OK.
I: So the first question. Can you tell me what is your role in regards to incident management and information sharing in the company you work at?
R: Did you say incident management?
I: Uhmm.
R: Yes. ..Ok, well my role in the company is primarily as a kind of CISO, so we have in our organisation.. Do you need any information about the size?
I: No, no. We are only interested in the sector you an mention what you do.
R: Yes.
I: Yeah.
R: Well, we have a team of people who take care of incident that come in and we also have an external service provider who helps us with managing some of the

incidents. So we have what it is called SAC?
I: Yeah SOC.
R: Yeah SOC sorry. We have this external team which helps us also with managing these different types of incidents. That is all kinds of incidents both related to hardcore IT security and we have also and internal team which helps us with GDPR incidents. So we have a broad spectrum of different types of incidents that go from traditional IT security GDPR related and that is of course if personal data is included in breaches or incidents or anything.
I: Yes. Do you take a decisions when you collaborate with those yourself or do you take common decision do you leave the decision up to them when it comes to how much you share?
R: It depends actually. If we start with the internal resources here at *company name* they usually take decision themselves. And we have an escalation process that involves me and some of my colleagues when needed.
I: Hmm.
R: But basically, they are in power to take decisions that can solve problems here and now.
I: Yes.
R: If we take the external provider they can not do anything themselves. They can actually look at the problem and then we can discuss between our internal resources and they, our internal resources can guide and take decisions for the external parties and what to do and they actually do it themselves the internal guys. So the external guys work as sort of counselors for what should we do and how should we actually solve the problem.
I: Uhm, perfect thank you. So in your experience what is the positive or the negative when it comes to sharing the information elm... regarding incidents?
R: Yeah, well the big thing is of course that our environment is scattered out so we have something that are on premise and we have something in the cloud and we have something at you know external parties that are sort of cloud but not really cloud so we have a very big environment and we have many areas that we need to cover. So that thing about actually being able to use different resources and their competencies to solve problems is very much needed for us to make sure that we are not being put down and our environment is actually not being able to work so.
I: Yeah, that is very much good that when you have someone external and or internal you can share the information but then you can take the decision with..
R: Yeah, we can take the decision but we can make it on an enlighted version with the correct information and with the correct details.
I: So that would be what would drive your motivation to disclose not disclose information?
R: Yeah, exactly. But we have confidentiality clauses with all of these vendor so that means that when they work for us they can not of course give any information

away to any others so we are very much focused on making that our agreements are with vendors that we can actually rely on and trust.
I: So, I see. You do not have any concerns? Of course you have NDAs signed but when it comes to or when you have to disclose to authorities as well is it something you would be concern about?
R: Well, the good thing is that we hardly ever, well except for GDPR issues actually we are not obliged to tell about our ransomware attacks or something like that.
I: Sure.
R: But in relation to security breaches that have personal data involved we need to give this to Danish Datatilsynet.
I: Yeah, OK.
R: No, no I think we are not worried because the thing is,.. For instance our security company that we work together with we have worked with them for I think at least 10 years and we were one of their first customers, so we have a common interest in securing both our environment but actually also when we share information with them so we are quite confident that they do what they can. And also just when we look at it we have to change our vendors every 3 yeas and they continuously won that assignment with us so we are confident that they are good at what they do and when we evaluate them we also look at what have they done to keep up to speed etc, and as for what I can see they have been heavily used all around in Denmark and actually quite good. So we make sure we always evaluate and work with those that are good and who are at the not at the forefront but you know quite a long way ahead of the rest of the security companies to help out when they help us.
I: So, if you would to describe a process of sharing the information with them do you use any platforms or an email or?
R: Yeah.
I: Could you just give me a little overview you do not have to go to any details.
R: Yes, for instance we log a lot of different things on our systems, on our Azure platform and on premise solutions. And we have decided to share the most important logs with this company. So they can actually see what is going on in our environment or also if somebody is trying to go into different area so they can actually warn us before because of different types of log management and alerts that they have on their system so actually we have double sort of double alert system. We have our internal but also our external which gives us a lot of.. More chances that we ensure that we actually react at the right time.
I: Yeah, to catch everything.
R: Or try to, it is a difficult area as you probably you know when you study it. But that is what we think that you know that if we have more than one platform than we actually better than if we just close ourselves.
I: Definitely, I agree with that. Hmm so you you have already answered that, but I

am just going to ask just so if you have anything else to add. So, what information do you share? You already mentioned internally and externally as well, and who you share with so you also mentioned companies and authorities and the obligations. But what about the.. Do you know the Danish CERTs or Centre for Cyber Security (CFCS) do you have any information sharing with them?. R: No.
I: No.
R: No, we are not obliged to our company is not obliged to that. We could if we wanted to. I know that there are lot of big move right now for companies to see if we could do a joint thing and for sharing all of this. But we have not engaged in any of the information sharing around this.
I: Yes.
R: But on the other hand, if we just talk networking and what do we do. We actually have some networks of companies where we share that are like us and our own where we can share information about the security. But that is not something that is specific to ..
I: The incident?
R: For instance, attacks or anything it is more what do we do, how is our set up, what are procedures what should we do are you doing, what can we do and then we can move on do you use a log management or what do you use. So we have that kind of information sharing with external parties that are similar to us. But it is not formalized.
I: Yeah, and do you see the value behind it or advantage when you..?
R: Yes, it is extremely important that we know what is going on in the different areas that are similar to us because it would give us a lot of speed in relation to solving our own problems. So it is both sharing very detailed information with our vendors but also with somebody that is similar to us. That is something that we need to do. That is also, earlier lot of us had different systems on premise and would actually tried to put guards and walls in our environment but now when everything is more open and is on cloud platforms you need to be more fast to know what it is going on and that also means you need to follow the trends.
I: Exactly.
R: So, we have a whole team that actually sits and keep up with what is going on both externally with the security provider but also internally.
I: Ok, thank you, that is great answers. I have one which is little different it concerns awareness so do you have any procedures where employees can report incidents or any kind of suspicious activities. And do you have any kind of program regarding the incident awareness?
R: Yes we do. That is also something I do with some one my colleagues. If we start or if you start as a newcomer to our company you can, you get different types of introduction programs and that is also including standard, what are the policies and what can you do and how can you report incidents, etc, to the Service Desk

that we have here in the company. So what we do is we educate all newcomers when they arrive and then we also have some online awareness programs that we roll out often. We have just roll out something two weeks ago actually in relation to all of the things happening in the Ukraine. So we try to follow what is going on in the world around and we push it to our user to see what hey can do to help us and we can actually also try and tell everyone but especially the new ones that they have now the obligation to support us with looking at the things that are suspicious and to report it to the Service Desk and then we can but the right team together to solve the problems.
I: Yeah. Thank you. I have the last question for you to ask and it is very broad. It is about if you could imagine an ideal information sharing it could be for the companies you try to share the procedures or anything else. What would that system look like? What would you like to have in terms of privacy or efficiency some sort of feature request you can just mention a few of what come out on top of your head.
R: Well, the thing is, I have thought about this a lot of times. But, I am actually more interested in having lots of of different sources than just one. Because having lots of different sources for you information means than this source says what we should do and the other one is like 'yes, but.'. and the third one says: 'yes, it is still,..' you know a lot of different for picking up your information is actually a lot better than just one source although one source would be nice but if you are too much reliant on that that is they have to be really really correct.. So, I am not sure that there is a good one source information place you probably have to look at different areas.
I: I see, but if it was something like a platform you could report things and let other people to see it who you want to see like you could control the information flow. Would that be something you would be interested in? R: Yes but it would have to be related to the platform for instance, if it is related to Microsoft Azure it is very important to know what it is going on but I would expect Microsoft to help me with what is going on. But if it is other platform or something more general than I would look at CRT or someone else to help me with this.
I:Yeah.
R: We actually do have a lot of news feeds that help us with what is going on. And the optimal platform would be something that delivers it right on my doorstep so to say ikke. I: Yes, that makes sense. Hm that is all I have for you to ask and thank you very much for your time. It was very knowledgeable for us. I will stop the recording now.

### C.1.3 Interview respondent CI3

Interviewer (further I): . . . so, can I please record this interview?
Respondent (further R): Yes, you can.
I: Thank you very much. I am just going to straight jump into the point. It will not take longer than 15-20 minutes, so let's just have it done and then I can leave you alone (both laughing). So, thank you very much for participating in our interview. This means so much for our project and for the value of the report and before we start I would like to briefly introduce you to the aim or the final goal of our report. So, we are trying to create a platform where all the critical infrastructures in Denmark can report their incidents or cyber security incidents. And we basically invited you here to feel and hear your opinions based on your experiences and knowledge of what is the best way and what are the challenges. As you also are the key stakeholder in this kind of platform. Let's just start without further ado with the first question. By the way, you also need to know that this interview is anonymous and will not be published anywhere and your name will not be recorded and the company will not be recorded, so, just so you know.
R: Good.
I: All right, so the first question is: can you tell a little bit about your position in incident management and how you are related to that? And your role in organisation?
R: So, I am the chief security officer in *name of the company* services and I am overall accountable and responsible for security as such. That also includes security incident processes. While being accountable, that doesn't mean that I have hands on to manage each and every incident. But when there are more serious and critical incidents I am also the decision maker and the one calling more strategic thoughts in, if there is a need to do that. I also tend to be responsible for stakeholder management, meaning that I stay in touch with an operational team, managing technical part, and I will align with the executive management if there are external stakeholders like authorities or customers that need to be informed. I will basically manage and handle that type of communication during an incident. And then of course post incident, I will push for driving any improvement actions. You know: root cause, lessons learned etc. to make sure we implement changes to improve and make sure that the incident won't reappear.
I: Thank you very much, and in your experience in the current company, what are the positive and negative elements about information sharing or if I could formulate it in another way, what are the benefits or the opposite, not to disclose the information?
R: Well, it's of course transactional. If I believe that there is something that I can give a value back when I am sharing the information. Because there might be someone that can bring me information that allows me to handle the incident better, that's one side. The other side is that you can always argue that there is always

something that alters meaning that... well... it's for the best of the community that you share. Because, others may benefit from getting your information, so they can also prepare or look for the same, you know? And the third part is of course, that there is a reappearance to share. You know there are regulators they require you to share, some customers require you to share. And sometimes, you know, what necessarily was not valuable during the incident, you know it is a mandatory side of it: sometimes to keep the key stakeholders and sometimes decision makers in the loop. So these are the main three reasons why we share in that case.
I: All right, that is a very interesting point. Can you describe, very briefly, the information sharing process in your company? Just in a few steps.
R: Internally, it's usually ahhh... well, we need to look at where we are. So if we imagine an incident that is ongoing, reporting from an ongoing incident means that the information is very time critical. It means that you might not have a full picture, so that means that all the information if fairly short, because time is of essence, not completeness or ... necessarily, so you always have a disclaimer that 'this is what we know at this point in time' and we will be informed about when we need to go out with information. Since, we know that an incident under development, as all of the things you might think you know, might be a challenge and might change. Where you have to kinda weigh the balance and the value of sharing, something that you might not know 100%, and the value of sharing in itself you know vs holding back on information in finding the back of the challenge or the problems that you might face by not sharing. So, that means, how certain do you need to be regarding information sharing, so that is typically something you need to consider. Is it sufficient to be 90% sure or do you only want to share 100% verified information? And that's basically what you need to consider. So there's typically one part of the process where you think: is it important to share now or is it important to be extremely precise and only share what you absolutely know. When we have an incident that has kinda passed and we are in the aftermath, then we can be more strategic. You can take a little bit more time. You can make sure that you take a little bit more context, more background.... You know, what do you know about the threat actor, if there is a threat actor? So you can start to put more context to the information. And then afterwards usually it is a very structured approach to do the final incident report. And that is also where we mostly include information regarding the root cause analysis, for example, and the Lessons Learned that I have mentioned before. So it depends a little bit on where you are: is it you are in, right after or in the controlled aftermath and Lessons Learned?
I: But at least there is different categorization of different incidents and where in time you are. Which is important.
R: And of course the criticality, you know. Because when we are having an incident, if it's in the medium category, as I said, we will not necessarily share the

information. It might be shared with the team. It might be daily routine. We understand quickly if there is no impact to business, there are no interruptions, so it might be kept in-house in the security department. But once we see that this might have an impact that goes beyond, we understand that this might have a business impact, that's when we interact and have it more structured and have it more step-by-step and process it more like a communication. But again, incident classification might also change during the incident. So, I have, for instance, experienced that we stopped, we have a critical incident, and at some point we realise we stopped, we have a false positive. So, then we had to wrap it up and say: "Hey guys, we stop it, false positive" (laughing)
I: But sometimes a middle range incident can turn into a crisis and then it is the other way around unfortunately.
R: Exactly.
I: Yeah. Ok, so, the next question is "what information do you share and with whom?" Do you share it with authorities, with stakeholders, other security community that you have and do you have any obligation to share the information?
R: So, again what you share depends a lot on whom you talk to. So, if you are a part of a trusted community like a CERT community. You might be familiar with the *anonymisation* CERT community. There we typically share any information we have regarding a threat actor, that means.... Also technical information- like indicators of compromise, it could be information about attacker URLs, or it could be country of origin or if we do think we can attribute a specific attack to a threat group... So, that's typically what we share in a very technical operational domain. So hmmm.... And that might also be relevant for other stakeholders, but typically for the technical, kind of trusted community. That's typically what we share, but that information again it could be fairly not sensitive, because it didn't say much about how vulnerable we are or what the impact is to our business, or if we've had a breach, because it's mostly about the threat. It's not about the vulnerability side. So there we can actually share quite a bit. The sensitive part and for instance what regulators tend to be more interested in this, of course, what's the impact. You know, how this threat has impacted our systems. So, we don't provide that much technical detail necessarily, but they need to have an understanding of did it have an impact on business. If it had an impact, what is the impact and do you go to the privacy authority as per GDPR regulation for instance, so it will trigger those types of things. So that's where we typically, if we have a suspected breach, that's typically where we have to involve the privacy experts and the lawyers, and they need to assess if they need to trigger a formal information sharing to, for instance, a VPA.
I: OK, and since you mentioned business, I will just ask you an additional question, if or during the incident you would use some sort of risk management framework you already have and just pull out the assessments from there or you would make

one on the spot. Some sort of BIA on the spot and then try to estimate there?
R: Hmmm... so what we usually... so, this is hypothetical: if an ongoing incident targets directly towards one product, we always seek to engage with the product teams. Because they have a unique understanding of not only what their application or a product is doing, but also they might also have context information about known vulnerabilities or if there is a specific risk assessment... So, during an incident we don't necessarily start looking into risk assessment, documentation as such or that type of framework, but you tend to find the right people to work with. So yes, we seek the information, but we seek that though people.
I: Thank you, and since we are talking about people, do you have any kind of procedures in place where employees can report these incidents. Also do you have any kind of program in place, where you can train awareness about the incidents and people know where to report, what to report in what case? Is there anything like this in place?
R: So we have both the 'starter training', which is an onboarding training, where they are informed about their responsibilities as an employee, and that includes, of course, reporting suspected or actual security incidents. And that covers 'how to report'. That's also part of the 'Acceptable use policy' that is something that all employees have to read and acknowledge every year. Incident reporting is usually also a part of annual security training, that all employees have to go through and that's also a part of the annual acceptance, where they are obliged to read and acknowledge the security policy of the company. So, there are a number of things there that make sure that on a regular basis. These are trained and they are aware of this. And that includes, you know their responsibility, but also the specific contact, so they know me, they know the email address to use or the phone number of the people to approach, so that they have that information at hand.
I: Alright, and the very last question. It's more of a 'make a wish come true'-question, I guess. Could you describe how would an ideal information sharing platform for... not only for *our* sector, but maybe also for other sectors, if you could be interested in getting the information also from other sectors, and how this platform would work. So, what kind of data you would like to share and receive yourself, whom to share it with , and how efficient it should be, how fast it should be.
R: Yeah, I think... When you talk about information sharing, it's really two parts of it: one is what you get and another one is what you give. I think to be able to give something, it has to be some trust mechanisms or confidentiality mechanisms in place. So, either it's a closed community like the CERT community where you know that a third party has been effective and authorised all the participants. So that you know that whatever you say to the group, stays within the group. That also goes with, you know, the TLP protocol, for instance. I guess you know that, so that you are kinda able to label the sensitivity of the information shared and

also how is this information shared further, or not shared. So, I think it's very important to have both kind of the specific mechanism in place, but also, the sense of kind of a trusted community, or the rules of how to.. How to... how to... you know, protect the information. When it goes to what to share and what to receive, I think it's important to understand that, you know, there is so much on the Internet. You can Google, you know, fairly good open source intelligence about the number of things. So for this to be very valuable, it has to be something that you can't necessarily just Google and find the same answer. And what does that mean? Well, that means, that it needs to have relevance, it needs to be contextualised to be of use for my organisation somehow. It has to do something to do with Denmark or the Nordics. Not something that has to do with the US or different regions. It has to do something with the type of distance we are in, you know, the *naming the sector* sector. It could even be something that is relevant for our customers, the ones that buy our products. So, it has to be something that is contextualised and relevant for us, otherwise, I can just Google it. Or it's irrelevant information. So that what makes the information unique and relevant.
I: OK.
R: Because if it's not unique, I can get it elsewhere and if it's not relevant, then why bother?
I: Exactly. Those are very good points... We are done with the recording, thank you very much.

### C.1.4 Interview respondent CI4

Interviewer (further I): So, now that the recording have started I will once again ask if it is okay that we record this interview
Respondent (further R):Yes, that is fine
I: So I will just start out by telling a little about the project. So I, our initial thought were that information sharing in the critical infrastructure in Denmark were lacking. Through our research we found that there are CERTs, DCIS and so on, but no intersector communication, so that one sector does not share with another, at least not to our knowledge. So, we are curious why that is and how to create a framework that could allow this to happen and still keep up the information needed, but still keep up the anonymity to protect you guys. This is also why we want to talk to you, as the critical infrastructure is kinda our customer in this case. So just to say, the interview is anonymous, so all the report would say is that you are a company in the critical infrastructure and otherwise it may be mentioned in a general list of companies within the critical infrastructure, but this cannot be traced back to this. So the first question is, "Can you tell me what is your role in regards to information sharing and incident management"

R: Yes, my role is head of support and IT for parts of the company operation *anonymised part*. The incident role I would have be would be mainly for the cyber security incident, in case of a cyber security incident of course. But also, we have a lot of investigation and reporting requirements for our own learning first of all and second of all for our customers. So as an example if any of our products *Changed from product name* have any critical failure that will lead to an incident, then obviously this would have to be investigated first and then shared based on its potential. Meaning if it was a high potential it would be shared, and if it was low it would not be shared. There is of course a risk level that we do.
I: Yeah, okay. "In your experience in your current company, what are the positive and negative elements about information sharing. So what are the motivation to share and what are the motivation not to disclose incidents?
R: Internally or externally or both?
I: Sharing externally.
R: Externally it depends on the level of the incident in principle. So if the incident is very high potential or even lead to an incident, then we are obliged to report to the Danish authorities. When it comes to an incident that lead to a minor incident, then the motivation is up to the individual unfortunately. Meaning that if the individual have the time or the willingness to do, then they are there to share, though we are not involved in that many platforms that are set to do so, to my knowledge at least. So smaller incidents tend to be kept internally unfortunately. For our business we also have quote on quote, issues with our customers that they are very "troublesome", so the problem is that they in any small incident will actually be seen as not opportunity to improve but an opportunity to take the business and find someone else to do. So that is also a very big obstacle that we are facing here in terms of information sharing.
I: Yer, that is understandable and we have heard this before.
R: Yes, I can imagine.
I: So the third question, "Can you describe the process of information sharing in your company using just a few steps."
R: Yes, so we have our software management system where we do all the reporting and incident reporting and all. And then, again, depending on the incident it will range up to the Danish authorities, it will range down to peers, like you know other similar companies *Changed for anonymity*. And then the last one would be sharing within the company through the software system
I: Yer, okay. So what information do you share and who do you share it with?
R: The number one priority is safety, so safety critical incidents are the ones shared the most. An example would be if you had a physical item which could hurt people, that would be a very serious incident *Shared an example very specific to the company*. Then this is shared with the industry, to my knowledge not outside the industry, so there is no inter industry sharing, it is purely inside the industry and

of course the authorities as I mentioned.
I: What kind of information in terms of cyber incidents, so like IP address or whatever. Do you know what you share there?
R: Actually we do not share much as of now. To be honest we have not had any such even internal sharing for way too long if any and that is something we try to improve right now. We are trying to actually raise awareness and treat cyber incidents the same way we would treat a safety incident or security incident. So we are not very good at sharing that. So the only thing that comes to my mind right now is on forums that we participate here and there, like the *name of the forum* forum or stuff like that. where we actually share some information, but there is nothing too standardised that we participate in.
I: No, okay. I heard you talked about awareness because the next question is "Do you have any procedures where employees can report such incidents/ suspicious activities.
R: Yes, we do. But that does not mean that they know what malicious or suspected attack is. Or some point they may be the perpetrators of such malicious acts right, for example connecting unauthorized USB's to critical infrastructure. They are not doing that because they want to kill our systems, but they are doing that because they want to watch a movie, but they do not know the difference or the awareness is not there to know that this should not be the case. So yes we do have procedures and processes in place to report, if they are followed to the letter, that is another story.
I: So I assume you also have some kind of training program.
R: Correct, but for the office staff and for the non office staff *Anonymized group of staff*.
I: Okay, so the last question is more in terms of our project, but could you describe the ideal information sharing system for your company. That could be what information to be shared, how the data should be handled and who do to share it with for example.
R: Right, I would say that in my opinion there should be nothing secret in all of this. Of course it does not expose your infrastructure or future attacks or anything, but when it comes to the incident itself there is nothing or there should be nothing hidden. My point is that if I was to design the perfect system I would have something similar like something called synergy platform which is for safety incidents mostly in the oil and gas sector. But what they mean is that you would have a platform that you would go in and you would write your report there and then that is accessible to anyone who actually have access to this. Now if you, if for very major incidents that require a lot of information, a lot of details, you could actually filter out specific names or company name and all of that. So that could also be an option of course, but that is not, yer, I do not know if that is even necessary. But I would say full transparency, I would think.

I: Yer, okay, what about in terms of login, because some things we have thought about is if there should be a login so only the critical sector companies could log in and their security companies could have an overview, and not the general public. I do not know what your view is here?
R: For the first step, it should definitely be only the stakeholders having access to this and not the general public
I: Yer
R: I guess for the second step, because you have to go in baby steps and you do not want to open to everybody, at the beginning at least. And also I do not see why it is of interest to the general public so much.
I: Exactly
R: Right, it should be of interest to the people that actually have something to learn from this and apply to the business also.
I: Cool, that was actually the questions, so thank you very much for your time
R: Excellent, that was quick and easy.

### C.1.5 Interview respondent CI5

Interviewer (further I): And then I will ask again now that I have started the recording, is it okay if I record?
Respondent (further R):Yes, that is fine
I: Cool, so the project is basically to, because right now there is some requirements to share information in Denmark, or the EU in general because of the NIS directive. We know there is some information sharing within the sectors, but we do not see any cross sector sharing like that. That is also why we want to determine why and create a framework that can allow this in a quite anonymous way and could be beneficial for any company in Denmark within the critical sector. Ehm, so, I fully understand that this is anonymous and you may not be able to answer all questions and that is fully fine.
The first question, can you tell me what is your role in regards to information sharing and incident management in your company? This is basically to determine that you are not a random student helper.
R: I am a the senior system security architect and I am part of designing the security for our products. I am not in charge of the information sharing, I just want to add that here.
I: Okay.
R: So I do not have any direct involvement with the incident management and information sharing.
I: No, that is fine. So question two, in your experience in your current company, what are the positive and negative elements about information sharing?

R: In terms of what?
I: In terms of cyber security incidents. So this could be the motivation to share, and maybe also the motivation not to disclose occurring cyber security incidents.
R: yes, so what we do in terms of cyber security is that we look at the, ehm, we have, each have protocols for the different cyber security incidents. And also, ehm, depending on the severity of the incident we have different ways to go in regards to managing the incident. So in terms of sharing it is beneficial for the broader sector to know what attacked one company. However some of the downsides could be that it can affect the shareholders and how other perceive the company. So while it is good to give information as it can help with security, there is also the economical aspects of this. Sometimes we are required to share to the authorities, for example in terms of GDPR (General Data Protection Regulation), however this is often up to the individual to determine if this is required at a given time. So I would say I see a lot of challenges in sharing information in an, as you say, anonymous way that would not put us at higher risk or put us in some legal implications. I think that is a general thing, I think. And would we benefit from more sharing? I think we definitely would, and in terms of incidents, it may even be a bit late because we want to get threat intel (intelligence) prior to some of the big incidents happening, but anyways. If we have a threat actor, from you know, a nation state, targeting a similar company within Denmark or even Europe, I think it would be great to know and have the ability to prepare yourself if you are the next in line. Of course I am not aware that we have such a nice framework nowadays. But yer, I think primarily because there is a lot of implications and if you have a look at what have happened recently, we have other companies with incidents where we learned very little from the companies themselves, but more from the leaks and people who were reporting on that. And, yer, that is one of those things, and companies are also publicly traded, so you cannot, you really need to make sure you know what you put out there. Because for a publicly traded company, putting out that there was an incident, could impact the shareholders and share prices. You know, it is much more complicated than for a private company and I assume the majority in the critical infrastructure are either governmentally owned or that they are publicly traded, I mean, maybe a combination. So it is, I think it is a valuable challenge you are taking (with this project).
I: Yer, and also kinda why we are trying to do this and why we want to reach out to all of you (critical infrastructure companies), to get this knowledge. So third question, can you describe the process of information sharing in your company, using a few steps? So just in general, so nothing specific necessarily.
R: To be absolutely honest, I am not aware of that process, that does not mean it does not exist, but just that I would not know about it. And especially in this regards, do we have a process of sharing information with external parties, we probably do, and we probably have that for legal reasons about I am not aware. So

sorry I cannot explain.
I: No, and that is also fine. And because the next question is also, what information do you share, either internally or externally, you may not know that either.
R: I really do not know, I think we, I do not know. So sorry.
I: That is fine, do you have any procedures where employees can report incidents/-suspicious activities, like a training program or anything?
R: Yer, I mean definitely, we have as many other companies incident response process and clearly defined ways of how people report cyber incidents. And of course to our knowledge, there is different ways to do that, but through common ways via our Service Desk and different ways you can reach them and raise an incident. So there is definitely a full blown process for incident handling.
I: Yer, and the last question, could you describe the ideal information sharing system for you company, this could include what information to be shared, how to handle information on the platform and so on.
R: Yer, so maybe again, I am talking as a cyber security professional and not somebody else working on this topic in my company. But definitely an ideal solution would be a solution that offer a certain amount of anonymity. So we would not put our company at the, you know, unwanted both cyber risks by revealing more about the knowledge of the landscape. But also you know, putting ourselves into the public's eyes or impacting from our shareholders and legal implications and stuff. And I think this kind of having the, you are gonna work on that, there are frameworks that are gonna be providing this means of sharing where you could feel sufficiently confident that your input into that system are anonymised enough would be very useful. I also know enough about anonymisation that this is not always possible.
I: No.
R: and it is kinda easy to deduct who are the one sending this information. I am a bit sceptical if it can be done in a way that you still get enough of context of the incident happening but without revealing who are the target. But again, that is the challenge that you have and about information, generally speaking, you would want as much information as possible, like who is the threat actor to understand the motivation, but also about the means. I mean, how would the incident happen to some of the other players in the industry. Is there a specific vulnerability you have to chase after, you know, let us say, take the example of this log4shell. I this was used in an incident, in the realm of critical infrastructure, we could then, you know, we know this is an important vulnerability but of course if it has already been used, we would definitely put more effort into addressing this vulnerability. also if there are some vulnerabilities, more of specific components, we had vulnerabilities in our own product and we would want to know if they were already used in the wild and in an acted campaign. So as much information, and again, this goes a bit, again, finding the right balance with anonymity. So, it is definitely

a balance I would say.
I: Yer, and just to round it up, who would you share this information with, so would it just be a sector or would it be cross sector, authorities, general public or?
R: So, that is the case, how do you define the cross sector?
I: For us, right now we are using the critical infrastructure sectors as defined by the NIS directive in the EU, which are basically energy, health, transport and so on. And cross sector would then be if energy put in something on this platform, health would also be able to see it, if that makes sense.
R: yes, I do not know. Now I am just think about, I guess, what I would, I would definitely like to share this information within our sector. But cross sector, would that be relevant, I do not know if that would actually bring us a lot of value to be honest.
I: No.
R: It comes with some trade offs. If you are talking about some Utopian, then you would definitely like to share with as many as possible, and yes we can maybe have that as a goal. That we have a platform to share with everybody on an incident, so that we can benefit from that. But I have my doubts, first of all many of these attackers that would be targeting some of the other sectors may not be super relevant. If we have ransomware, at the end of the day we know about this threat, it is not a very targeted one, so the value of getting information about this kind of incident is there, but not super high.
I: Yer.
R: But if we are getting information from our own sector, then it is really bringing more value if you are seeing some of the attacks that are more sophisticated that are targeted by nation states of something else. So I am a bit plaid on this, I mean, I understand that there is value sharing to the wider possible audience, but I also feel that maybe for us, the value would be relatively limited. Because, yer, I do not know.
I: Yer I understand.
R: And it would come with this trade off that you would be exposing your information to a wider audience. Again it really comes down to, if the platform and the solution that are in place would guarantee that this information sharing that are done would be done in a way that would actually only have positive benefits to the company, then it would maybe be something we would go for.
I: Yer, that was actually the interview.
R: Okay, it was not that bad *laughing*
I: Hopefully not, but thank you very much for your time and help!

### C.1.6 Interview respondent CI6

Interviewer (further I): So for GDPR reasons I will just ask again if it is okay that I record this interview.
Respondent (further R): It is okay.
I: Cool, so I will just give some initial knowledge about the project. So, our initial idea is to create a framework to allow information sharing across sectors in the critical infrastructure in Denmark. The reason we focus on the critical infrastructure is because the critical infrastructure is required according to the NIS directive, and because it is an interesting area to look at right. And some of the things we have uncovered throughout our research is that there is some sharing within the sectors but not a lot across sectors. So, our goal is to create a framework that allows to share across the sectors in terms of cyber security incidents and hopefully increase cyber security in Denmark. I just want to state that the interview is fully anonymous, so your company name would only be mentioned if we made a list of companies within the critical infrastructure in Denmark, but that will not be attached to the interview at all.
R: Okay.
I: So the first question is, can you tell me what our role in regards to information sharing and incident management is?
R: Well, regarding information sharing I take part in some information security networks where we can in confidentiality, we can share information. But it is for instance what we in Danish call "Foreningen for IT chefer I Danmark"(Union for IT leaders in Denmark).
I: Yer.
R: Which is a society where there is a lot of different companies, both from the private sector, public sector and you can say that there are several critical sectors among them and we can in confidentiality share what is going on.
I: Yer, cool.
R: So you can say, that is not formalized.
I: Yer okay, so in your experience in your current company what is the positive and negative elements about information sharing, so what are the motivation to share and maybe the motivation not to share.
R: The motivation to share is definitely to be smarter in solving cyber security risks. The other part, the negative, could be confidentiality problems or other kinds of legal problems about sharing information about what is going on in your company.
I: Cool, could you describe the process of information sharing in your company in general, so just a few steps, nothing in detail necessary.
R: Well, ehm, as I said, we do this in the society of information security leaders is very informal because we share information to different ways, either at meetings four times a year on a higher level. But if we had one incident going on in one company we can just mail to the other members what is going on, what kind of

compromise we are in. We can share some Indicators of Compromise (IoC) and something like that. Some of them, we are not in this company, but some of them are hooked up in MISP to share the incident. I know in some sectors, for example the energy sector, they use MISP to information sharing.
I: Yer.
R: For IoC and such.
I: Yer, and now that we are talking about IoC, what information do you share and with who do you share? For example, authorities, security companies and so on.
R: Yer, we share with other companies we trust in the network.
I: Yer
R: We do not share with the authorities at the moment. It could come either from MISP or the upcoming from EU, DORA, if you have heard about that, digital operation resilience act, which I think that could be a good idea for you to look into that. Also, because that is regulation coming from EU and this area also so cyber. I think I have read something about you are obliged to notice the authorities if you have an event.
I: Yer cool.
R: Today I think it is only, how do you call it in English, Datatilsynet we are obliged to send information to if you have a breach which involve GDPR. At the moment we are not obliged to information financial services.
I: Yer.
R: But that could come with DORA.
I: Okay.
R: So, have a look into DORA.
I: We will, thanks. Do you have any procedures where employees can report incidents slash suspicious behavior?
R: Yes, so internally we have procedures, we can use our Helpdesk to report if we see something hear something, some inside incident, yes.
I: Yer okay.
R: We also have an old incident management process with people taking care of that and databases for major incidents and that.
I: yer, nice. So, the last questions, so as I mentioned we want to make this framework for you guys, so could you describe the ideal information sharing system for your company, so that could include what information to be shared, how to handle, so anonymity and so on and who to share it with?
R: Just to ask you, just to repeat what was the question again, there was a lot of things.
I: Yer of course, could you describe the ideal information sharing system for your company.
R: The ideal sharing, okay.
I: Yer.

R: So, I think that should be automated into something that could be Servicenow like the one we use for incident handling. You could use MISP to external sharing, that is encrypted, confidential and so on. That would be nice, but it does take some resources to take that up, but I think that would be necessary. So, to share externally incident, I think MISP would be the right way to go.
I: Yer okay, so what information would you want to be shared on such a platform?
R: Whatever is needed because it is a trusted platform, and it is a trusted network of that community. So whatever it takes to be upfront with cyber security event and incident sharing. What is it called, IoC's and that, and stuff like that, so we can probably take it upfront.
I: Yer, you have mentioned trust a couple of times, how would you define an organization or company that you trust, when would you trust them?
R: When I have met them, or if they are a part of my network
I: Okay, that was actually the interview, thank you so much for your time.
R: Okay, you are welcome and good luck with it!

### C.1.7 Interview respondent CI8

Interviewer (further I): So, just ask again because of GDPR, is it okay if I record
Respondent (further R): Yes it is.
I: Perfect, so, just to give some initial information, you have seen our emails, but our idea is to create a framework to allow information sharing across sectors in the critical infrastructure. We focus on the critical infrastructure because they are required to according to the NIS directive, whereas the others are not as required to. And it is a very special usecase, so it is interesting to us and our research have kinda uncovered that, companies within the critical infrastructure does share some information with their CERTs and DCIS, but not really with the rest of the sectors. So if transport is hit, health may not get to know it, and the rest will not know it, until it is in the news. But you will not have any information about what attacked and so on. So that is kinda the purpose of the project, to create a framework which could allow this to happen easier and hopefully increase security right. So just to say, the interview is anonymous and your company will not be mentioned, apart from maybe a list of companies within the critical infrastructure to basically state who do we consider critical.
R: Yer, no worries.
I: So, the first question is, can you tell me what is your role in regards to incident management and information sharing?
R: Yes, I am the director of the companies' cyber defense center and therefore responsible for cyber detection. Our company is split into different parts, but our cyber defense center handles them all *Anonymised due to mentions of company

names*.
I: Yer, in your experience in your current company, what are the positive and negative elements about information sharing. This could be the motivation for sharing, but also the motivation not to share.
R: Yer. It is clear to me that according to the Danish national cyber strategy, which was just renewed, there was established six hubs as we call them where our sector have a DCIS *Anonymised*. That was a step forward on sharing both threat intelligence but also incident response and detection rates. It has not really spawned out that much yet, in the sector, for example in the energy sector are much more further in their knowledge sharing. So that is where we are right now. We can of course for commercial reasons not share everything.
I: No.
R: But we do have an open strategy that if we are hit with something that we can share, we have a MISP, which is a platform where we do this kind of sharing, both with the DCIS but also other external parties.
I: Yer, so can you describe the process of information sharing in your company, using just a few steps.
R: The process is that if we consider a threat or a hit or an incident to be shareable with others we will share it with the DCIS, who will share it with the rest of the national critical sectors *Anonymised*. And we will put it in an external MISP later this yer. It is not up and running yet, but it is in process and if it is related where we believe we need to involve the Danish authorities we do that according to procedures as well.
I: Okay, that actually leads up to what information do you share and with whom?
R: It could be Centre for Cyber Security (CFCS) if it is related to foreign threat actors, it could be GDPR. So it is all over the span, what is that "styrelse"(governing body) called, it is not me who report to them so I have forgotten that, but we both share with the Centre for Cyber Security (CFCS) and Danish defense if needed and the DCIS.
I: Yer okay, do you have any procedures, oh just to add, what information do you share, like IoCs or what kind of attack or do you share anything like that.
R: Anything in between, it could be the full hit, it could be IoCs or it could be that we have just been hit.
I: Okay, do you have any procedures where employees can report incidents/suspicious activities.
R: Yes.
I: Like a training program I assume.
R: We, well it is not my department, we have awareness programs where we train the employees. We have implemented, for example in our email a phish alarm button where employees can report for example a suspicious email. We also have so they can, we have an on call duty where they can call in 24/7 where they can

report if they see anything suspicious.
I: Yer, okay, so we are actually at the last question, which is, could you describe the ideal information sharing system for your company? Now you have mentioned you have, you are using MISP and contact a DCIS, but if you would have one platform for all of it to share cyber security incidents, what would be the ideal, like what should be shared, how should the data be handled, should it be anonymous and who do you want to share it with?
R: Since we are a technical operational department we of course need the technical details, so what I will share would be highly technical IoCs. So that is my need, what the company need, could be everything from that, to much more higher level, like for example this Ukraine- Russia situation, we share threat intelligence right now with other sectors *anonymised*. So it can be anything in between, both from high level management, to threat intelligence to IoCs.
I: Yer.
R: All of the scope, it depends on who is receiving and giving the information. But for me as a director of a cyber operations, it would be the technical part.
I: yer, who would you want to share this with, and how should anonymity be held, would you be fine with your company name coming out or should it only be the sector or should it just be that someone in the critical infrastructure have been hit. How would you?
R: I am missing a bit of regulation on that part, because the Danish national strategy does not involve us as a private company. So we can voluntarily click into a DCIS, but the governmental part of Denmark is obliged to. I need to consider every time I have something in my hand that is to consider, do I share this or not, but there is no clear process. It is about what is it, how often is it. I believe it needs a bit more openness in the community in general, because if you look at other companies hit, people share things when it is over.
I: Yer.
R: And that is because people have realised that we cannot do this alone, we need to share.
I: Exactly.
R: It is a non answer to your question, because it is the involvement into how do we share
I: Yer.
R: I think going forward there will be a lot more sharing compared to last yer for instance
I: Yer, just an add-on question that we talked about yesterday in the group is that a lot of people have mentioned this trust factor of who do we want to share with. I do not know if you have the same, but if you do, how would you consider someone you trust and how do you determine if you trust someone or not.
R: Unfortunately the cyber security in Denmark at least, is very personal oriented.

It is meeting in person and trust people. For instance we have an issue that Centre for Cyber Security (CFCS) does not want to share anything. They might have threat intelligence, but they do not want to tell anyone, probably because they do not want to bring panic. So if I know someone in another sector, I call one person personally and talk with that person. So it is a young industry in that sense that you need to have a connection with people and not clear processes or mutual law or whatever.
I: Yer.
R: And if you look at some of the European colleagues it is the same, we need to meet in person, we need to see face to face before you share stuff, but then you share everything
I: Yer.
R: But it is interactive, it is person to person.
I: Yer okay.
R: It is not an organisation to another organisation
I: Yer, and I think that is a very good answer, and something we have been wondering a bit about, so that is nice to hear. That was actually the interview and the questions I had, so thank you very much for your time and for participating.
R: No worries and have a nice day!

### C.1.8 Interview respondent CI11

Interviewer (further I): Okay, so for GDPR reasons I will just ask again, is it okay that I record?
Respondent (further R): Yes, absolutely
I: So as we just talked about I will just briefly mention what the project is about. Our project is about information sharing in the Danish critical infrastructure and we focus on the critical infrastructure because of the NIS directive which requires you guys to share, whereas it does not really cover the rest of the normal companies if you can say it like that. And our idea is to create a framework which allows information sharing across sectors, because from our interviews we have found out there is information sharing inside the sectors, so you share with each of your sectors, but there is none or at least little information sharing across sectors so you share where everyone can see it, within these sectors of course. That is why we want to find out why and create a framework which allows this in an anonymous way and in a way that you guys can you. That is also why we ask critical infrastructure companies and security companies who may operate these critical companies and also the authorities, so CERTs, DCISs and so on. Just to state, the interview is anonymous, this recording is purely used for transcription and if you mention your company or sector, that will be anonymised. I do not

know if you prefer that, but at least some of them do, so just to make sure. So the first question, can you tell me what is your role in regards to incident management and information sharing.
R: Well, you mean the information sharing in the sector wise context or?
I: Yer.
R: Okay, well, you can say I have to roles in the incident management, I am the chief operational risk officer and the chief information security officer in the organisation *anonymised*. But we have a, you can say, a first line incident response team and function who are responsible for the incident management and as long as we are on the lines of a regular IT incident, then I am not directly involved. I am involved if it materialised into a major incident and or a crisis level for the *anonymised*. We of course have two major suppliers, IT vendors, one on the *anonymised* systems, they are facilitated by *anonymised* and *anonymised. Then we have our general administrative platform for the general clients which are facilitated by *anonymised*. And each area would initiate incident management supported by an incident manager from the organisation and if it escalates then it reaches the point of the CIO and myself would then be responsible for the overall crisis management. And then we also, at our organisation facilitates this *anonymised* crisis management team, which is the, in a DCIS setting is the DCIS crisis response team for the *anonymised* sector.
I: Okay.
R: So in the *anonymised* sector we have a slightly different setup than you would find in other sectors, because in principle it is the *anonymised* that is the DCIS for the *anonymised* sector. But the different tasks are split between *anonymised* and the *anonymised* and the *anonymised* facilitate the crisis response team on a sector level, which are called the *anonymised* crisis management unit, and I have role there as chairman of that setup. Which means in case of a significant crisis or an incident that would effect stability, then we would activate that and that would then, inform relevant entities of an ongoing incident. So there would be information sharing both towards the *anonymised* and also the Centre for Cyber Security (CFCS) would be informed directly and potentially also *anonymised* if relevant, the overall crisis unit. In terms of internal incidents, we would inform Centre for Cyber Security (CFCS) if we have an ongoing situation with regards to cyber security or an IT incident where we are suspicious of whether it involves some sort of cyber related activity. But that would be the way that we share information to Centre for Cyber Security (CFCS), both in terms of sharing the information but also potentially in terms of getting support from Centre for Cyber Security (CFCS) to handle the situation.
I: Cool, I can say you mentioned quite a few of the questions we have also, but I will go through them all, just so we have them if there is any additions. But the next question is, in your experience in your current company, what are the positive

and negative elements about information sharing? So this could be the motivation to share and maybe the motivation not to share.
R: But I think it is an element of confidentiality primarily. Recently we had and this is of course confidential *Cut due to confidentiality*. Sharing that information you quickly dive into the boundaries in terms of sharing benefits and so on, but then also it is considered quite confidential information that you really want to keep on a need to know basis. So there is the element on one hand of sharing the information both also to other companies that we have this situation ongoing, or internally, also in terms of supporting prioritising security initiatives and so on. But then on the other hand you want the information to be kept on as few people as possible, because you do not want the information to be spread outside of the organisation or to people who should not know it.
I: Yer okay, can you describe the process of information sharing in your company, using just a few steps?
R: But we have our, we of course have an incident management procedure which would, in case of an incident we would report it, there would both be the incident management, so ensuring that the incident is managed and then subsequently we would initiate the incident reporting procedure. Where depending on the type and magnitude of the incident, we would report it in our risk management function, gather the information, root course analysis, further initiatives and so on so fourth. And then that would be reported to relevant layers internally, both in the IT department but then also to the senior management layer, they get the information on critical incidents and severe incidents. They are briefed on those and get the information there. Whether then actually, you know the *anonymised* is a lot of *anonymised* working as, so often they perhaps do not really understand what is being reported, but I think, we continue to do it, both because of an obligation towards, so the management knows what is going on, but then of course also the more you communicate about it, the more information they start to pick up and then hopefully also act upon, so.
I: Yer, cool, what information do you share, either internally or externally? And who do you share it with? You have kinda touched upon this, but not so much what you share.
R: Yer, I think internally it is of course, within the IT department and security department we share a lot of information and also with our vendors of course. And then internal incidents are also, if relevant, if they have this, you could say, cyber dimension in it, or if we are unsure if it stems from some sort of cyber related activity, then we would also share it with Centre for Cyber Security (CFCS). But, and then we have our internal incident procedure and then externally it is in case it is something very significant, then we have some crisis management function that then share it with both *anonymised* and Centre for Cyber Security (CFCS).
I: Ehm, so what do you share, so what kind of information? Now I do not want to

put too many words into your answer, so I will try to just wait for, hehe.
R: Yer, so it depends, we have I think, two years ago, we had a situation where we shared of course, the information we could extract from our systems and servers. We also did some, we provided a lot of detailed information to Centre for Cyber Security (CFCS) for them to initiate some analysis on our behalf. We also shared with other vendors. So you could say, that is part of the incident management procedure. Then in terms of information sharing, we would share sort of overall information on the type of incident, what has happened, the consequences and then if we are able to extract indicators of compromise or things like that, then we would share that also. As mentioned, we are members of various information security groups, including *anonymised*, where of course there are some requirements about what and how you share, what level of detail. And also, we are also member of something called *anonymised*, which is is an information sharing initiative on EU level of *anonymised* and other sectors. I think it is facilitated by *anonymised*. Where we would also, if we are affected by something, we would also play it into those groups, but it would be on a similar level, again, where there are these channels. They are of course to some extent secure, but they are not secure enough so that we would like to share very detailed information, so then we would rely on some follow up, bilateral follow up if necessary.
I: Yer, cool. Do you have any procedures where employees can report incidents slash suspicious activities? So do you have a training program and so on?
R: Yer, we facilitate both sort of a general awareness programs, in terms of, actually we are starting an awareness session on phishing campaigns today actually, it will run the next ten days actually. So with general training modules, tests, we have different sort of, general assemblies, about phishing and what to be aware of and so on. And then we have procedures if someone registers something suspicious, either mail or otherwise. Each employee is on a regular basis informed on how to handle, on who to contact, how to switch off the laptop if necessary and so on so fourth. Then we of course we also have an incident channel where all employees can register an incident if deemed necessary.
I: Yer, cool, so the last question is, and this is very specific to our project. But could you describe the ideal information sharing system for your company? So this could be, what information should be shared, who should this information be shared with and how should the data be handled and so on?
R: I think, the, yer, that is an excellent question. I think internally it would be, some sort of platform where you, because we have some information sharing systems, also for sort of the general IT management, they have some systems and so on. But it is always this aspect of confidentiality and so on and who can actually access what. So it would, I think it would be a system where you would be ensured that the ones that have access to this particular information, that is on a need to know basis or that you then disclose information in order for a wider sharing initiative.

And then I think amongst other sectors, or broader, I think one of the issues that we have seen in our work, is the information sharing across critical sectors in sort of a, I would say in an incident perspective. If something is ongoing, then there is definitely a need to enhance the information sharing procedure, if the, let us say the health sector is affected by some sort of cyber related incident. It might not affect another sector directly, but there might be some elements that would be relevant to share with the other sectors as quickly as possible. And there are some initiatives now in terms of sharing of information, but it is not on a, it is more on a general information sharing level, it is not on an incident management information sharing level if that makes sense.
I: Yer.
R: So I think, that would be something that, I think we would benefit from having, on the cross sectorial perspective, that we can easier push information from our side to other sectors and vice versa.
I: Yer, cool, that was actually the interview, so thank you very much for your time.
R: You are welcome.

### C.1.9 Interview respondent CI12

Interviewer (further I): So I have started the recording and will ask again according to GDPR, is it okay that I record?
Respondent (further R): Yes.
I: Cool, so I actually want to start by telling a little about what the project is about. So we are three students at Aalborg University studying cyber security at our master thesis which are about information sharing in the Danish critical infrastructure. And the critical infrastructure are very broadly defined, so it is hard to determine who are actually apart of it, but there are some sectors that we are going for. Our hope is to create a framework and have some openness and some information about the information sharing in the Danish critical infrastructure, which can help both the critical infrastructure companies, but also the authorities and security companies and that is also why we interview all three groups. because you all have different objects in this and based on our interviews you all have very different opinions and ideas, which is really nice and helps us a lot. So the end goal is to create a framework which can aid information sharing in Denmark, primarily in the Danish critical infrastructure because they are required to according to NIS. But other than that it could in theory be used by anyone. And just to say, the interview is anonymous, so sector and name will be anonymised, so you can also speak rather freely, and once again, thank you for taking the time.
R: No problem.
I: So I think I will just start. So the first question is, can you tell me what is your

role in regards to incident management and information sharing?
R: Yer, my role in incident. I am head of the cyber security function and have sort of a very broad responsibility across pretty much all domains within cyber security, including, a shared responsibility for incident management. So the security group is responsible for security monitoring which we do in collaboration with some external partners, to gain a 24/7 coverage. And then depending on the type of incident, we are either responsible for solving them or responsible for solving them in corporation with our partners in IT operations and external partners. So typically if it is minor things, if it is why a particular user is doing something or a machine is doing something that is strange but no immediately, obviously a malicious attack, then we probably handle that incident end to end. If it is what we term as a major security incident or an incident that involves our backend infrastructure, then we do it in corporation with operations, because we typically do not have administrative access to go into these backend systems to investigate what is going on or shut them down if needed.
I: Yer.
R: And if it something where we can see, uh that looks like, either we do not understand what is going on or this is an attack and we need someone to assists us, then we have an on call service where we call in some specialists. Luckily we do not have enough incidents so to speak, to have that regular practice on how to handle this, so that is why we call in external parties who handle this on a more regular basis and have up to date knowledge on attacks and how to handle them. And I am also involved in our information sharing, we have not been covered by the old, or the current NIS, but it looks like we are going to be covered by the new one with the expanded scope. So it does not look like it has been a formal requirement, but I am part of a number of community groups where we share formal and informal information about what is going on, on a person to person basis typically.
I: Yer, cool, so in your experience in your current company, what are the positive and negative elements about information sharing?
R: I think it is largely positive. We try to share as much as we can get away with, with other interested parties and we gain a lot of values from being able to talk to others and get their feedback on what they are seeing and how they are handling incidents. But again, there are things that we are not allowed to share from a higher management perspective, there are some issues and stuff that they do not want us to share about. At least not on an ongoing case, but other than that we are all for sharing and try to share as much as we can. I know that we have been in discussion with some others about sharing technical indicators of compromise and we do that in a fairly manual way because we do not have the tools to readily incorporate and react to these technical indicators. So it is more like, have you seen these specific IP addresses behave strange? Have you heard about this particular incident rather than have you heard about this specific hash file of something going on or similar.

But I know that some others are doing that knowledge sharing.
I: Yer, can you describe the process of information sharing in your company, using a few steps? So from an incident to you share.
R: It is probably not so much a process. When there are sort of major things going on, for instance around Ukraine crisis or of there are Danish company hit by ransomware attack or it is affecting others or others suspect they might be next in line. We do sort of an informal mailing list between companies, about if anyone know anything or have experienced anything. And that is probably the typical one. For us sharing incidents or experiences, we have not had many, sort of, larger incidents, but it is more a question of. If you have had an incident you probably share your own experiences in various fora, probably 6 months to a year after.
I: Yer.
R: I think that is probably what I have seen with other organisations that have been hit with attacks. Typically you get some initial information about what is going on, and then within six months they typically open up more about their experience and their learnings about what have hit them. We did get some information from a recent attack on a Danish company where they were fairly quickly communicating, what they at least saw as their Achilles heel. And it was something that was shared at a management level, so above my level, some technical details about what they felt was the vulnerabilities that was exploited in the attack on them. So then we went back to see, are we exposed to the same types of vulnerabilities internally?
I: Yer okay, cool. So when you share, what information do you share, and with who? So now you have mentioned indicators of compromise at least.
R: Yer, that is typically, indicators of compromise, affected IP addressed, specific types of malware we have seen, if it is anything new and scary and then that would be in the short term. In there long term it would be the whole story about what happened, how did we address it, what did we learn, yer, what vulnerabilities was present, what was exploited? It is a lot about a lesson learned, when it is larger incidents. And I mainly share it with other CISO's and security responsible in Danish organisations.
I: Yer
R: We do not have a lot of sharing with international, so it is mainly national sharing.
I: Yer, what about authorities or security companies, or what not?
R: Yer, to a degree yes. With GDPR, so some things are shared with Datatilsynet as part of GDPR if it is a GDPR incident. We also report it to the Danish *anonymised* authorities if we have an incident affecting our production. Security organisations, yes, the ones we are working with on the case, if we see something we will inform our current partners and we might get others involved in trying to resolving an issue, but only the ones that are directly involved in solving the case.
I: Yer, okay, do you have procedures where the employees can report incidents/

suspicious activity?
R: Yes, well, we have an email address where they can mail to. Most people would report stuff through service desk or through person to person, but it is part of the employee security handbook on the reporting suspicious and incidents.
I: Yer, do you have a training program for that handbook or?
R: We have some on boarding activities where we introduce the handbook and then we have some mandatory e-learning where people have to, I would not call it very advanced training, but they have to read the handbook and sign off that they have read it and understood it. But we do not have any quiz questions or fancy animations on that at the moment.
I: Cool, so we are actually at the last question now. Could you describe the ideal information sharing system for your company? And that is mostly because we are trying to create this framework, so it should fit for you guys and not based on what we thought it like.
R: Yer I think having a way to share anonymous data, sort of the right here incident stuff that we might not be willing, I mean, we have these closed forum where we can share stuff, but they are limited in size in how many you can know and still call it a closed forum. So, and that sort of put a limit on the sharing of what is going on. So a way of anonymous sharing incidents and experiences in some sort of feed mode that you could log in to. We are also looking into at what point is it possible to do IoC sharing, they have to be vetted to a certain degree these IoCs, so that also requires a certain level of trust among members sharing those, so you do not get a lot of garbage into your system. But those things, yer.
I: Who should it be shared with, so who should be on the platform and should it be shared with the public too or only within the authenticated layer?
R: I think it helps it is within a vetted group of people in organisations. I am part of different forums, but the common theme is that we try to exclude organisations where they are selling security. So typically we say, this is for internal use and we do not have that suspicion that people will use information to drive sales. In some instances we do have people from security vendors involved aswell but that is very much depending that we trust they will not use the information for sales purposes.
I: Yer.
R: That is frowned upon.
I: Yer, understandable. That was actually the interview, so that you very much for your time.
R: You are welcome.

## C.2 Authorities

### C.2.1 Interview with the respondent A1

Interviewer (further I): can you please give me your consent to record this interview?
Respondent (further R): if you say that it would be fully anonymized, then sure, you can record it.
I: Thank you very much. All right, so I will try to introduce you briefly to the concept of our project, so that we are on the same page. We are a group of Master students in Cyber Security, who are trying to build an information sharing platform for entities in critical infrastructure in Denmark. And we have invited you here because we would like to get your first hand input from the potential users and stakeholders, as you are one of them. And we hope that your expertise will help us to understand the requirements of the companies. So, without further ado we will just jump straight into the first question, and it sounds like: what is your role in regards to incident management and information sharing in critical infrastructure.
R: Yeah, so, the role that I have, it is managing security organisation. The team is responsible for timely response, and responding to the cyber threats. As a result of having these security responsibilities, we do value information sharing with not only internal, but also external stakeholders. It is important for us to share, share that not only we give the information to the community, but also that we get something back from the community. We are willing... with a lots of cyber threats that are common to us, and if we know something, then we can share in a way that we can all get something from learning about these cyber threats.
I: OK, thank you for that. And my next question is: in case of a cyber security incident, what information is important for you to be shared and what type of information you can disclose to other parties in the platform?
R: Ok, look, I think it all comes down to what kind of agreement there is between the different parties that participate in the information sharing. If we are talking about trusted parties, then we are sharing the technical information about the threats that we are dealing with. To put it shortly: indicators of compromise, timestamps, it can be any kind of data that helps understanding the threats, responding to this, and also maybe by doing such also giving the opportunity to engage in some sort of preventive and protective measures. So, in the first place I would say: what is interesting to be shared is technicalities, as what those are being used for, preventing the extent, possible, to other critical infrastructure areas.
I: OK, and can you tell me, where is this information about the incidents shared? Do you have anything else where you share the information to? To other platforms? Maybe to other CERTs, authorities, or maybe internally?

R: It depends on a case, but what is being shared, that would be with other counterparts (other CERTs) that we are cooperating with in the sector. In several cases we also cooperate with national CERTs or governmental CERTs. In other more rare cases, we will also be dealing with law enforcement. This is all the data sharing on all the threats that we have been dealing with essentially.
I: Ok, that makes sense. The next question comes from your personal experience I guess. It is about the status of awareness in companies about information sharing, especially in critical infrastructure.
R: Well, I would say that it is rather good, in my opinion. When we are talking about critical infrastructure, it is acknowledged that sharing is caring. Seeing these entities in the critical sectors, having different value when it comes to sharing, I believe that there is a consensus that it is all about interest to share the information, which seems that it fits, and seems to be common to the sector.
I: So, again in our experience, are there companies prepared to, or do they know the legal requirements to disclose the information in case of a cyber incident?
R: That is a very good question, when it comes to legal requirements, I think it very much depends (differs) from organisation to organisation. Different levels of maturity. There is this knowledge of data dissemination. I think there is no common point when it comes to implications of legal requirements or privacy requirements, which have to be fulfilled.
I: OK, the last but one question would be: do you collaborate with any other entities, and I think you partially answered this before, but how do you establish and manage trust with other entities you share the information with? So, other CERTs, companies, DCIS, or government authorities?
R: Well, look, first of all it is a matter of some sort of framework within which we operate, and when it comes to trust, it is something that happens overtime, which is difficult to build and easy to break. So, you are... it is about the rules that everybody agrees to and signed off on, and living by the rules, and showing the interest to operate in such a framework. So, it is not only the documentation binding, the legal binding, it is also, I believe to an extent, interpersonal relationship and relations that play a role in sharing the information. Again, having trust in peers, you may find having the information important and relevant for them. It is important and forces the feeling of.... I would say, security for sharing this sensitive information. So, this would be my answer to this question.
I: Ok, thank you, and the very last question. I would say that this is a wish-question: how would you describe or how would you imagine a perfect, or an ideal information sharing platform for different organisations? In terms of what information to be shared, how to authenticate users, who to share the information with, how to handle the data? Efficiency of the platform maybe? You don't have to go into technical details, but maybe you could give us a short summary.
R: Yeah, Just on top of my mind, I suggest, you can put it down to having users

authorised and authenticated in a platform will be definitely an important element of sharing the information. And the platform itself, I think it is also something to do with the data quality, before the information being shared. And also about having transparency in not only how this information is being used, but also to what extent, or what value is of the information in this sort of platform. So, giving some sort of measures, metrics, KPIs around the intelligence, has been used to what extent and what is the "return on the investment" so to say when it comes to sharing.
I: Yeah, thank you very much, I don't have any more questions.

### C.2.2 Interview with the respondent A2

Interviewer (further I): So I have started the recording now and will ask again if it is okay I record?
Respondent (further R): It is okay you record.
I: Perfect, so I will just give a brief introduction about the project and why we are contacting you. So, the idea is to create a framework for information sharing in the Danish critical infrastructure. And we have, throughout this project contacted a few critical infrastructure companies and discussed with them who do they share with and what do they share and so on. And obviously, authorities comes up quite a lot because we have these DCISs, CERTs, and all of these authorities which they use to share. But our understanding is also that there may not be as much cross sector sharing, so that is also what our framework try to deal with, because that is also important because one sector may be relevant to other sectors too. So that is also why we are contacting you. So, just to say, the interview is anonymous, and we will do our best for the transcription to make it very anonymous. So I think, if that is okay with you, I will start with the first question.
R: That is totally okay and thank you for the introduction.
I: Perfect, so the first question, can you tell me what is your role in regards to information sharing and incident management. This is basically to know that it is not some random person in the authority but someone relevant.
R: Yes, I am hired for doing the threat analysis of all the data we collect. We have huge amount of network sensors in Danish critical infrastructure. And all the data we get from there, I am hired as a threat hunter to find stuff that should not be there. The primary goal is to raise security for all the companies in the sector. So that means we actually help from the very small companies with one person hired to the biggest one, the very critical one, with 4000 people hired, so that is our member scope.
I: Yer, cool. So second question, in case of a cyber security incident what information is important for you to be shared. So what type of information can you

disclose to others too, so that could be companies, public, other authorities.
R: Yer, of course we have a lot of to find the IoCs that related to an incident so other companies can do the preventive the parts, that meaning blocking, firewall, all the technical stuff. But it is also to be very clear what risk are we seeing, what is the real scenario. We are so lucky we do are not selling anything to anybody, people are actually member of us with no cost. So for us it is most important give a realistic picture of the risk and what is going on when we have some incidents and not making it worse by saying not true stuff. But of course IoCs is an important part so others can do the preventions of whatever is going on.
I: So when you get this information, where is the information shared, so are there platforms, do you share to other CERTs, authorities.
R: Yes, we have a big collaboration with a lot of CERTs in Europe, and we are sharing there. We are also sharing on a MISP platform, the cross sector platform. We would also there. So when you say you do not think we are so good at sharing cross sector, I am not totally agreeing with you in that part. Because actually, the DCIS which is cross sector, and we are actually sharing cross sector in the DCIS MISP that we have in Denmark.
I: Yer.
R: So I actually think we are one of the countries that share the most cross sector.
I: Okay.
R: If I look at the other CERTs in Europe, yer. So, if something occurs, of course we need the permission to share, but it is a part of being a member in our entity. You say we can share stuff, of course sometimes anonymous, but again it is mostly important to get the relevant part out so that others can prevent. We also have a chat forum called sector forum, that we share stuff there. It is a forum for members, a digital forum for all our members. We actually also have a chat forum for our MISP users cross sector and for the other DCISs. Yer, so there is a lot of sharing going on.
I: Yer, okay, I think that is a very good answer and I think a lot of it is hard to find as a third part, because I think, maybe also happening a little inside.
R: Yer, it does and of course, if we can share to the broader audience it is of course possible to do. But it is always a balance of, you know, what should go out there and what should stay.
I: Yer.
R: At the members of the CERT and the DCISs. Of course we can be better, that is totally, that is what we are working a lot, at least with other DCISs *Anonymised sentence*. So, and the new regulation from EU is also stating some new sectors, so they will be invited as well.
I: Yer.
R: New critical sectors.
I: Okay, so yer because we have also noticed there is some new critical sectors being

added, so that is nice to hear.
R: Yer, actually a lot are being added.
I: Yer, and this is actually not an official question, but I would like to ask, so you say you share with other CERTs and DCISs, I think my add-on question to that would be, "why do you see the reason to split these CERTs and DCISs, rather than have one big for all sectors in, for example Denmark?".
R: Yer, I think it is a different area of, sorry I have to say this in Danish, ministerier (Ministries/departments).
I: Yer.
R: And the way we have structured in Denmark, we have different ways and different reporting back, but you could argue for one big DCIS/CERT. But at least for the sharing part, we are united there, cross sector.
I: Yer.
R: We definitely are, and all the exercises we have had until now that are conducted by the Center for Cyber Sikkerhed (Centre for Cyber Security), the national, what is it called.
I: Centre for Cyber Security.
R: Yer. We actually work cross sector. So when we have big incidents in Denmark, you can actually argue, if there is not power, there is no nothing else. So everyone is participating, all the analyst in other DCISs and CERTs are actually helping, cross sector *Anonymised sentence*. So, if something big happened in Denmark, the exercises have shown, that you do not care where you are working, you are helping each other cross sector.
I: Yer, so what I hear from that is that it is not necessarily because there is a technical reason to split it, it is more a political bureaucratic reason maybe?
R: Yer, I think so, but I think with the new sectors coming in, instead of having a DCIS for all of those sectors. I think, let us take the example of another sector which may relate to us, it would not make sense to make a new DCIS *Anonymised sentence*. Of course there is someone working on saying, can we, is it okay to put some of the other sectors into the existing CERTs. I: Yes.
R: Or DCISs, so I actually think it will be like that.
I: Perfect, thank you. So the next question, from your perspective, what is the status of awareness of companies in terms of information sharing, right now?
R: From minus 1000 to plus 1000.
I: (*Laughing*)
R: Yer yer, but of course a little company that have not worked with cyber security and do not see themselves as critical infrastructure, sharing is what, they do not look. So, they do not have the power, they do not have the knowledge and that is why we are out helping them, about the technical stuff, about looking, and then share. So you need to start look before you can share anything, so I can think a lot of them understand the concept. It is like the story about all the plane crashes, if

you go back in time. In the start no one would tell why the plane crashed, and then they made a deal that they start sharing this because it is not good that the planes crashed. And today that is actually why we do not see so many plane crashes, because they actually started sharing between companies. And when you tell them this story, everyone understands this. So I think everyone can see the idea here, that the threats against us are universal and we need to stand together in order to protect each other. So I have not really, only a few big dumb companies, I would not say, not in our sector, but in other sectors are thinking they are doing some violation of competition advances or something. I do not get it. From analytic to analytic, when you get under all the management stuff, people know the importance and know how to share without telling, secret stuff.
I: That is also our findings from the interviews with the companies, so that is nice to hear
R: Yer okay, and I am happy to hear that as well. So of course, you know, we will start talking about sharing, we are actually the *rest of the sentence anonymised*.
I: Yer, cool, so are the companies prepared and do they know the legal requirements to disclose in your opinion.
R: Yer, they do, otherwise we help them.
I: Okay.
R: So, and again, sorry for my language here, but it is so bull shit that sharing something that have hit you could ruin your competition advances if you do it the right way and if you share it with the right people. So, yer, I get so tired when some companies have that philosophy.
I: So the next questions is two fold, and you have actually answered one of them. Do you collaborate with other entities, which you have said, and that included CERTs and companies, and authorities and other DCISs, so that is, I do not want to ask that again. But the other thing is, and how do you manage and establish trust? So how do you establish the trust with companies, because a lot of them have actually mentioned trust as a big factor, and they need the trust in order to share with anyone.
R: Yer, but again, with entities, or DCISs and CERTs like us, you have this additional points where you have, hey I have seen this, can you share without telling anyone that it is me. So I actually think our rule is very important here. That we guarantee the trust, that what we share is not the 8.8.8.8 (googles DNS) IP address, it is actually stuff that have been seen, you know, it is not open source intelligence. It is actually stuff we have seen this in an attack and it is actually qualified as a, I do not like to call myself an expert, but by experts who work with this. So I actually think having these DCISs, the jump stations, makes it easier to get this trust. For the CERTs in Europe we are actually traveling to the CERTs and visiting them, because then we get the trust.
I: Yer

R: Meeting with people all over Europe, we have been around to a lot of those organisations like first members, there is a trust. In order to become a first member, you need to do a lot of stuff and show it, that you can do a lot of stuff and that you work seriously with this. So there is a lot of organisations around Europe and the world, where you need someone to say that these guys are good enough, they can join this circle of trust, and I think that is fine, it should be like that right.
I: Yer
R: But I actually think it is good for companies that they have us as the middle, if they do not want to get anything out.
I: So what you are saying is that one of the ways, that you at least, get trust to other CERTs, is through meeting them physically and meeting them.
R: Yes, definitely, and then when you have known four or five of them, when you have shown you are willing to share, it is like every other relationship here, you need to see.
I: Does any of the companies, within your sector, ever request to for example meet you guys before they share
R: No, but we actually prioritised, when we went out with these network sensors we have, we actually showed up physically, with them and us. So we actually drove those around.
I: Yer, okay.
R: In order to get some trust and understanding and so on. And of course we had meetings, but for now our CERT is, the member companies that own us. By owning us, having board members here, they actually tell their members that they can trust us, because we actually get our money from them.
I: Cool, so the last question and this is very specific to our project. Could you describe the ideal information sharing system, and you have kinda touched upon it a bit.
R: One word only, MISP
I: Yer, but like MISP is more of a protocol to share it, there would also have to be some authentication, and in this case that is kinda you guys right. So you have the MISP internally and then you forward the information. But if it was a more automatic system where all the sectors could come in and share the information, what information would have to be shared here. You have mentioned IoCs, I do not know if that is other things you could consider relevant.
R: For incidents or?
I: Yer for incidents.
R: Yer, of course you need to set up some rules around what to share right. And that of course have been the hard part about learning people to you know, I have been working in security analytics where someone have been sharing powershell.exe. And we had automatic alerting, so when we came in, there was like a 100.000 alerts, right, because powershell.exe runs when you have 3000 servers,

right. So that is of course the hard part. But for me, in order to share, maybe the possibility to be anonymous, or have someone to validate what you share, could definitely make it easier for people to share. But you need to look before you can share, and a lot of companies in Denmark, you know, do not look.
I: No.
R: Logging in Denmark have just started, so it is kind of hard because companies are as small as they are. And I do really not blame them at all, but it is not something you prioritise, right.
I: Yer, ehm, how would you authenticate users, because some of the other things companies have said is that you also what the information to be true. Because in your case you have people to authenticate it, but if it was automatic, how would you make sure, it is for example this company in the critical infrastructure, that have authenticated to the platform and not some, for example, malicious actor that are trying to snoop in or for example give false information?
R: There are possibilities to make that from a technical perspective I think. Yer, but of course you need to maintain this, and I do not have an easy solution for that one.
I: No, because, so I think I will give a suggestion and then you can of course say if it is a bad idea or not. So one of the things we have thought about is that the first login would be with NemID, because then you authenticate that it is actually a company, through the CVR system. And from then on our we do not care about the NemID, but then we make an account, based on that one authentication
R: That is a good idea. So the only problem I see, is that some of the people working in the SACs (Security Analytics Center) and SOCs (Security Operations Center), in the bigger companies, do not necessarily have NemID, but, or company NemID.
I: Yer, but then it would be one company NemID for example and then it would end up making an account and then that account could make several logins.
R: Yer, definitely, but again, always think about what is being shared, right. Again, I can discuss with some of the, for days, if I should, with some of the nervous people, right. It depends on what you share and that you trust the people and that they do not use it as competition advance, right.
I: Yer. That was actually the interview, so thank you very much for your time.
R: Yer, that is good, I hope you can use it for something.

### C.2.3 Interview with the respondent A3

Interviewer (further I): I have started the recording and will just ask again, is it okay I record?
Respondent (further R): Yes.
I: Perfect, so I will just start by introducing myself and the project. My name is

Michael and we study Cyber Security at Aalborg University in Denmark and we are writing our master thesis right now. And our idea here is kinda to look into the information sharing in the critical infrastructure primarily in Denmark. And some of our, in that regard we have interviewed some of the critical infrastructure companies in Denmark and some of them have mentioned you as a CERT. Therefore it is quite interesting for us to interview you too, because you are kinda an authority in this regard and that is kinda why we are reaching out. Just to say, the interview is anonymous so the maximum we will mention is that you is a CERT and we will not mention any sector or who, just for anonymity.
R: Okay.
I: So in that regard, I think I will start with the first question. Can you tell me what is your role in regards to incident management and information sharing.
R: So the *organisation name* role?
I: Yes.
R: So, we have a couple of roles and then they fit together. The *organisation name* is an association, and so we have members and these members they own us, they pay our past and they are our, and we are here for them. So they have created us in order to help them with the vision of a more resilient *anonymised* sector and to have cyber safe *anonymised* services in the *anonymised*. And we do that and one of the important things that we do is to help facilitate but also drive information sharing and connected to that, cyber incident response within the *anonymised* sector.
I: Yer.
R: And I can talk more about what and how we do that. The other, sort of, main role that we have is that we perform part of the *anonymised* sector DCIS in Denmark. The DCIS is owned by *anonymised* but most of the content of the DCIS already existed before that DCIS was created. So that is being filled by *anonymised* with *anonymised* and then other part of information sharing and cyber incident response coordination is filled by us.
I: So just as an addition, what is your role, so as a person in your *anonymised*.
R: My role, I am the head of the *anonymised*, so I have been the leader since it started.
I: Perfect, it was to also make sure if we are talking with the student helper or who it is.
R: Okay.
I: So second question, in case of a cyber security incident, what is important for you to be shared?
R: It sort of depends on the incident, but our main focus is the information that are useful for the other members to defend against the same attack. So there is one sort of idea, or vision which is that one members attack, is everyone else defense.
I: Okay, and what information do you feel like you can disclose to others, for ex-

ample other companies to the public and so on?
R: So, we currently do not disclose a lot of information to the public. We do, so what our members share among themselves and what we share with our partners around us, for instance the neighboring DCISs that are protecting the other sectors in society and others. It is, I mean, one thing we share or talk about is our threat picture, so what is the concrete cyber threat and we have as DCIS we also have an ongoing relation or a collaboration with the Centre for Cyber Security and in Denmark they create threat assessment for Denmark, but they also create threat assessments for some of the sectors. And we support that, so we work with them, we give them input, so in their assessment, there is also information that come from the *anonymised* sector. But we also, we appreciate them, we use theirs, which we think sort of a higher level and we work with that and we try to make it more concrete and accessible and workable or actionable is a better word, for our members. So we work at finding information and it can be sort of, what is it called, IoCs, indicators of compromise. It can be very specific stuff like binary hashes, IP addresses, domain names, URLs, those kinds of things, but it can also be sort of, more up to tactics and procedures, but still more concrete information on the actually threat that other members can use to prepare themselves. And then there is on the defence side, there is a variation that our members or what companies can use to defend themselves, I think where everyone is able to use, is sort of the concrete IoCs. And there is also a growing number of our members that can use and actually look for tools, tactics and procedures when they defend themselves, which I think demands a higher maturity, but it also takes the defence a nudge up.
I: Yer, cool, so when you have this information, where is the information about the incident shared, so do you have a platform or is just with other CERTs, authorities, internal?
R: Yes, we have a platform, and as a member organisation we have a sharing platform which consists of several parts. It is everything from general, I mean, similar to Teams, there is a wiki and a chat, and we also have a MISP to share sort of the technical indicators, the data.
I: Yer, cool, and now you have mentioned Centre for Cyber Security and collaborated with CERTs and DCISs. Do you share with other authorities or companies, so for example security companies, or whatever? Or is it only members of your CERT?
R: Well, so, our members, they use vendors, and those vendors, again, use other vendors. So there is a vendor ecosystem. It is a lot bigger than just the *anonymised* companies, so I think there is a lot other companies involved, at least, in the role of being a vendor to a *anonymised* company or something like that.
I: Okay.
R: But one part, also, we do have relations with the Centre for Cyber Security, but we also have relations with the police, because a lot of what we see is cyber crime.

And then if there is information that are useful or relevant to them, we like to share and especially if they open investigations. So against attacks, or groups that keep attacking, in Denmark or the Nordics. We will give them what we have, but also try to gather what they need if possible.
I: Okay, cool.
R: And then we have our neighbours DCISs that I mentioned. So there is an ecosystem within the membership, but there is also an ecosystem in protecting Denmark, where we try to contribute.
I: Yer, so what is the status of awareness of companies in terms of information sharing, in the critical infrastructure? Do you have any, like, idea of what is the awareness about information sharing?
R: My impression is that in the *anonymised* sector, the awareness is high and it is partially, more or less a requirement from the *anonymised*, that is a part of the picture.
I: Yer.
R: If you look at, I guess it may not be, I may not know the details currently, but at least according to the upcoming regulation from the EU, called *Anonymised*.
I: Yer the *anonymised*.
R: So one of the six or seven keypoints in there is information sharing, so it is, and most institutions in the *anonymised* sector are already reading *anonymised* and preparing to meet those requirements. So I think awareness is pretty high.
I: Okay, so and you may have kinda answered this, but I am asking anyways. Are the companies prepared and do they know the legal requirements to disclose? But I think that is kinda what you just replied to, right?
R: Well, yer, but I am also, cuz, to be honest, the legal requirements to disclose today are still not very strong. I think, at least in our case, our members are definitely ready to share more than it is legally required of them.
I: Yer.
R: Because that is a good idea.
I: Yer, so, and this is kinda a question again, do you collaborate with other entities, and how do you establish and manage trust with these entities?
R: So, yes, we do, even though you, let us see, I can show you, a slide maybe.
I: While you find it, are we allowed to potentially use this slide in the report, if we can?
R: Yer ehm.
I: It is okay to say no, it is just.
R: Yer, no, so I, at least, we do not publish these slides anywhere, but I do use them and show them, so if you google for my name and presentation, they are possible to find publicly.
I: Yer, okay.
R: So, just to illustrate, so we have the non member community and then of course,

since we are *anonymised* CERT and not just the *anonymised*, we have the Danish Centre for Cyber Security, *anonymised* and the police as we spoke about.
I: Yer.
R: We have a similar setup in *Anonymised the remainder of the sentence*. And then we have different, so we do not have the same DCIS type role in *anonymised*, but we do have an agreement with the *anonymised the remainder of the sentence*.
I: Yer.
R: And then we have down here, some of our neighboring DCISs in Denmark and Norway. So we do single out and create working relations with a lot of companies. The way we work with that, and that is actually also, and it might be in Norwegian, but I did a talk at *anonymised* in Norway two, three, four years ago, about exactly that. So there is a 20 minutes YouTube video if you want the details.
I: Yer.
R: But it, so I mean, you have to find some kind of common interest and then we have a formal agreement. It is often very useful to have a, yes we can collaborate. The next is sort of, what can we collaborate on, and it has to be something that adds value on both sides, very sort of generally spoken. So I think we are able to find those kinds of collaborations with lots of companies, but there are some missing logos here, that we would like to be on here, but where we have not found that yet, so it does not always work.
I: No.
R: So, yep, that was again, short question, long answer.
I: But we really love the long answers because that is really what contributes the most to our project I think.
R: Okay, good.
I: So, and one of the things we have heard a lot from the companies we have interviewed is, this trust, and often they do not mention the technical trust, they mention the human interactive trust. And how do you manage to get the trust from all of these companies and entities?
R: So, the building human trust is on some kind of level straight forward. It is again, it is to have some shared interest, it is often a very good start and then it is about sort of, saying what you are doing and doing what you have been saying you are doing and be a dependable partner. I think that is how to build trust, in very very general trust and we definitely do that, and maybe even more with our members, so not necessarily with our external partners. But with our members to build trusted sharing groups, and I guess I did not mention that, I said we have a sharing platform. A very important part of that is the group of humans, so we have threat intelligence sharing group, we have what we call incident response, what we would maybe now call cyber defence sharing group, we have a sharing group for leaders of cyber defence functions. And of course those groups works best if people actually know each other, if they have learned to get to know each

other, if they know that they can share things and that they will not be used in the wrong place. And to do that, you actually have to build some kind of common understanding. I think most times where information ends up where it should not be, the way I think about humans it is because of cluelessness and less about, sort of, maliciousness. So you have to know that your peer group understands the risks that you take when you share, sort of sensitive things and that they treat it like that. And of course, elements of that, in these groups, to have no passengers, so when people are sharing, everybody speaks, everybody shares, which also, then they have mutual beneficiency and this again, I could talk about this for half an hour. But it is because there is a lot of it, there is a recipe for how you can create good trusted sharing groups, and unless you have other drivers against you, I think it is pretty straight forward to make it work.
I: Yer. So you do not have to, they do not require you to meet up physically or on a Teams call before they trust you?
R: Yes, I think you build trust.
I: Yer.
R: So you do not start out with a 100% trust in the first meeting, so you meet, and I think it is better to meet physically than in a Teams call, but I mean, Covid years have shown it is possible to meet and build trust, also online. But then you start doing something and first you do something small and then you show you can be trusted and then maybe you do bigger stuff later.
I: Yer, cool, and that is also kinda what our interviews have shown, but only a few people have mentioned it directly, so it is nice to hear it from the authorities too.
R: Okay.
I: So the last question, and this is very specific to us, because we want to create a framework that allows the information sharing for all CERTs and security companies and critical infrastructure companies to be in one place rather than in many different. So our question here is, could you describe the the ideal information sharing system for your organisation? So for your CERT basically.
R: So I am, I think we have a pretty good working system. I, so if you create one system for everyone.
I: Yer.
R: It will be hard to trust. Because you will not, you cannot know who is consuming your stuff at the other end.
I: No.
R: So to have a sharing group of five people, or ten people or maybe even 20 people, you can build a group with high trust that knows each other and you can share lot of things, also sensitive things. But if you extend this group to 100s of people or even 20 people, but that live on different planets and actually do not understand each others world, then it is hard to build trust. So I am not sure if I, if it is about sharing, and it is, I mean it is, often for us what we are sharing,

it needs to be protected in some way. Because it cannot, it cannot necessarily be publicised, if you do that, then you actually give the attackers an advantage and that does not make sense at the moment. So I think you have to, I think the ideal sharing system, the way we see it, is something similar to what we are trying to do and it is to. Lets see, we is my sharing thing (finding slides). It is to have some trusted communities.
I: Yer.
R: And they can be like this, these are for the internal members trusted communities or you build other trusted communities, and I guess here we sort of mention them. And it is, and information flows, and I guess, I am not sure if I have, it is starting to get a little advanced. So you can have sort of a variety of trusted communities, but then information can also flow between them. And the way we also think about the job we do, we are a sharing hub, and so, and one of our jobs that our members gives us is to share as much or drive sharing in the community. And that does not necessarily happen by itself. So one of our jobs is to remove obstacles to sharing, and one of the others is to drive sharing in an area, there it would make a lot of sense that stuff was shared and that would sort of nudge people or tell them if they have too much to do, just throw the information to us and tell us if there is anything we should sanitise, to get out of it and then we can share those kind of things. And I think that is also a realistic sharing arrangement, I think that makes it easier to make it work over time.
I: Yer, so what I am hearing you say is basically, like, the more you have, the harder it is to ensure trust.
R: Yer, so the bigger the group is, and the moment that the sharing group is so big that there are people I do not know, then it becomes harder to have trust I think.
I: Okay.
R: You can of course have, you can have something that binds you together, you can all be in the same sector reporting to the same authority which is what we have and then it is possible to have a lot of institutions that have a lot in common *Anonymised sentence*, or you can be sort of national interest in Denmark, those kind of things. But also I mean, the matters of national interest in Denmark are kept quite closely I think.
I: Yer, so maybe restricting such a platform to only critical infrastructure companies and maybe, so, rather than having different CERTs, but maybe making subcategories inside one big CERT, so let us say, finance, tele and health are split up, but if something like ransomware which are quite common, that could be shared with everybody, but if it is very specific to an application used in one sector, then it would only be shared with that sector basically. Because then you know it is specific to me, so I do not trust the rest, but here it is.
R: And it is also, so I mean, one of the things we do is to, and even on ransomware and there is some dilemmas. So we get the information, we find the information,

we buy the information and we also sometimes end up with insights into the ransomware gangs and their infrastructure and how they work. And we do scrape that out and share it with our members and some of it as you said is actually interesting to everyone in the sector. So that is also things we share with as many as we can, but if we share it publicly, if we wrote blogs about it, then these gangs would know.
I: Exactly.
R: So we keep it nonpublic, but we do share it with all the neighbour DCISs in Denmark, we share it with all the, what is it called, *anonymised* in Norway, we do share it with other companies we partner with, it is not. But the reason it is valuable is that it is not public information, so that is one subset of special case in sharing.
I: Yer, because that is one of the things we are discussing in the group, how authentication goes. Because you could for example use something like NemID we have in Denmark and say, yer okay, the first time you login, you have to use NemID, because then we make sure it is a company, a CVR that is allowed on the system. We have an authority to make sure of that, right, and make sure it is not criminals and then make sure it is only shared within this group of companies that have been approved. But how do you do that? How do you ensure it is not some malicious actor trying to become a member basically?
R: So for our members, they have to be, they have to have a license from *Anonymised*, that is public information and it is pretty straight forward to verify. And also for other partners, the type of parts we try to connect with today, for us it is, we know the all. So it is, we do not, and we have, so for MISP sharing for instance, we actually have several MISP, what do you call them, communities or something. And one is sort of the, the one we use to share with the neighbour DCISs, the companies we work with, maybe the least protected one. But we still know who we are talking to, we still have communications with a human there we probably met, or at least have been able to verify somehow, and then they get user access. And I guess in those cases it is still a manual process, we do not have that many and as long as it is organisations, it is, we do not have that many we have to relate to.
I: No, Yer okay, and I guess one of the benefits of having the CERTs split up, that one CERT can manage within the sector.
R: And we can, so for us we have the *sector* as members and then the others that want to share things within our sector can get in touch with us and that does happen. We have someone getting contact, basically via email or something, sharing information that they feel that should be available to our members, or there is maybe a more long term relation like with the other DCISs or governments or some companies and then we set up a MISP connection. So they get what we have, and we get something from them.
I: Yer, cool, that was actually the interview, so thank you very much for your time

and all of your, actually very good answers in my opinion.
R: Okay, thank you, so yer, hopefully useful.
I: Yer, it was.
R: If it is possible, I would like to see your master thesis when it is done, it is always interesting to read and see fresh perspectives.
I: Yes of course.

### C.2.4 Interview with the respondent A4

Interviewer (further I): Okay, so I will ask again for GDPR reasons, is it okay that I record the interview?
Respondent (further R): Yes, I consent.
I: Okay, so I will just start by explaining briefly what the project is about. So we are three students studying cyber security at Aalborg University Copenhagen and we are writing our master thesis about information sharing in the Danish critical infrastructure. The reason we have chosen the critical infrastructure is that they are required to by NIS, so it is a usecase at least and we are really interested in the information sharing, so it is an interesting topic. That is also why we ask you guys, both from authorities, security companies and critical infrastructure, because that allow us to get some information that is not easy to google. And our hope is that we are able to create a framework that allows information sharing across sectors and for the entire community so we can share information about incidents that can hopefully allow others to prevent attacks too. So I think I will ask the question. Oh, just to say, the interview is anonymous so we will remove all names and all that, so you can speak rather freely. So the first question is, can you tell me what is your role in regards to incident management and information sharing?
R: Sure, well, I am the head of the department for the decentralised cyber and information security unit in the *anonymised* sector. So we are tasked with collecting, shifting through information, both on threats, vulnerabilities and incidents across the *anonymised* sector. My focus is on *anonymised* and my role is that I am the manager of the team, actually I have another manager I am working with. And that team does the information sharing across the *anonymised* sector and also the other sectors we are sharing with. We also receive information from international partners, so Norway, Holland, EU, Austria, US, across the globe we also get and share information.
I: Yer okay, cool. In case of a cyber security incident, what information is important for you to be shared? So what type of information and what can you disclose also to others?
R: So if I get information about, in let us say, another *anonymised* (organisation in the sector), the main thing would be how did they attack, where did they come from, how to detect, for the others in the sector. My main focus is not that partic-

ular *anonymised* (organisation in the sector), they will take care of themselves, my job is to share across the sector and the other sectors as well.
I: Yer.
R: The first thing would be, what IoCs, what IoBs, where did they come from, how did they approach the attack, can it be replicated, is it something against all the sector or just a single target?
I: I have not heard the term IoB, what is that?
R: Indication of behavior, so instead of just having the compromised IP, we would have, so they start by attacking or reconning like this and then they do like that, that is the behavior. So it is not just the indication from the technical part, it can also be, okay, how do they operate?
I: Yer, cool, so where is this information shared? Do you have any platforms, do you share it with others and so on?
R: Yer, of course we have from non structured platforms like email or message boards, but the more structured way is that we have a Malware Information Sharing Platform (MISP), which is created by NATO and EU, and is an open source platform, I hope you know.
I: Yer.
R: So we have trusted communities inside that, we have one MISP with our sector, we have one MISP with the other sectors in Denmark, then, you can say, what we read in one of them we shift through and say okay, what is relevant for our sector and what is relevant for the other sectors, it is between those two. So they are not connected, we are the connection.
I: Yer, cool, what is the status of awareness from companies in terms of information sharing? So do they know they have obligations to share and all that?
R: They only have obligations to share if they are an operator of essentials services.
I: Yer.
R: We have those.
I: So are they aware of that and the benefits and so on?
R: Well actually it depends, because that is two different questions, having to do something and having benefits of it.
I: Yer, true.
R: So the benefits that a lot of other people also have. We are also having sharing sessions, almost like anonymous alcoholics every month. So we say the whole sector counties and regions and others, and then we share what are our most critical vulnerabilities and how do we approach them and what can we learn from each other. That is not necessarily in the NIS yet, but it can just be an advantage. That is not just the NIS guys, it is also the others.
I: Yer.
R: So the question was, yes the NIS service providers of essential services know they should share, but they are not sharing because they are getting benefit from

it, they share because they have to. We handle the sharing for benefits.
I: Okay, cool, and that actually answers the next question. So ehm, the next question is, do you collaborate with other entities and how do you establish and manage trust with them? And this includes both the companies within your sector, but also the DCISs, CERTs and other authorities and so on.
R: The quick question is that it just takes time, the other answer would be, if you have a benefit to share, you can get something back. So we approach and, let us say, we had a network with *anonymous* and they had established the circle of trust with Holland, Australia, the US and so on, and we went to Norway to talk to them and then to establish the trust to be included in that circle. Another example could be the *anonymised* information sharing, there you are vetted by that organisation, are you the one you are saying you are and so on, which is a formalised process. There is also a community inside, it is called *anonymised*, it was established during corona, there you are also vetted by other members of the community. We kinda use the same approach with the sectors in Denmark. We have one that we established because we are the critical sector, the energy sector in Kolding established the MISP very very soon, and we went there and the more we share, the more we get.
I: yer, cool.
R: Long answer.
I: Yer hehe, the long answers are nice, that is where we get a lot of good information. So the last question, could you describe the ideal information sharing system for your organisation?
R: Actually we kinda like the MISP, so the ideal information sharing platform is where everything is automated. So when you see an IoC it gets added to a watch list you could say. So if someone uses this vulnerability or threat, attack vector, you could say it will immediately be added to the MISP when and where it is being used and where it is used from. So you can put it into your automated response like firewall. So the best sharing platform is the automated one.
I: Yer, what about authentication, both who should be on the system but also getting on the system. Should it be locked behind login prompt or should it be public or?
R: I would say behind at least 2-factor authentication.
I: Yer.
R: You are sharing vulnerabilities, so you have to have some kind of trust in that platform.
I: Yer, and should it be possible for any other, like, the public tobe able to see some kind of list of example IoCs?
R: No. There is the problem of you have to base it on trust because you will not get people to share if you do not base it on trust and you cannot trust anybody.
I: No.

R: So you have to set some kind of repore or trust between them. The other, you can this day, if you just install MISP and add all the different public feeds, you will get the whole world of information. That is already there.
I: Yer.
R: But the real information, when it gets from data, to information to knowledge, that is where you have somebody shifting through it and actually saying this one, that one is important.
I: Yer.
R: And how you combine that with the automation, that is a hard one.
I: Yer, I agree on that. That was actually the interview, so I would just say thank you very much for your time.
R: That was easy.

### C.2.5 Interview with the respondent A5

Interviewer (further I): So I will start recording and I will ask you again for the GDPR reason, if it's ok to record?
Respondent 1 (further R1): It's ok, we accept, that you are recording the meeting and we will be conducting the meeting later as well.
I: Perfect . Ok, so I will briefly introduce the project. So, we are doing our master thesis in Aalborg University in Cyber Security about information sharing in Danish critical infrastructure. In this regard we are reaching out to companies within the critical infrastructure, but also authorities, who have some kind of connection to these, but also the security companies, because they may handle the security of the critical infrastructure to get a better overview of what is going on and how the information sharing is happening on all three levels.
R1: Yeah,
I: And this is also why we reached out to you guys, to get a better understanding. And just to say it, the interview is anonymous. I said that it will be recorde, but it's mainly for the transcription and we will remove all ideas of who you are, sector's names and anything. So, you can also speak rather freely. (both laughing)
R1: Ok,
I: Cool, the first question is: can you tell me, what is your role in regards to incident management and information sharing? So, this is basically an overall, so we have an idea of who we are talking to.
R1: Yeah, I am *anonymised* in Danish * anonymised* That means we are collecting all *anonymised* institutions (omitted part). So we are sort of ISP for *anonymised* institutions and handing out the IP addresses. And we are *anonymised*, so we have the responsibility to receive and filter all the contact about abuse stemming from the *anonymised* or to the *anonymised*.

I: Cool,
R1: And we are also doing vulnerability scannings for public institutions. I: Yeah, and more on... what is your personal role in your *anonymised*? So what do you work with?
R1: So I am the head of the *anonymised*. So I help and have a manager role in all of what we are doing and *anonymised* is also doing a lot of practical stuff.
R2: Something like incident handling and things around that.
R1: and I: Cool,
R2: Our MISP platform that we are using on an occasion and then sharing.
I: Yeah, ok. So,
R2: Maybe we should sum up here, because we are mainly a communication hub for the other *anonymised* and institutions that are connected to the *anonymised* net. So, regarding the practical incident handling, yeah, we have some incident handling, but it's not as heavy as you might think.
R1: Depends on what you are thinking,
R2: We are filtering and distributing these incidents. Filtering that means, that we are filtering out non-important stuff, Sending out the real incident reports to the *anonymised* and other institutions, so that they can handle it.
I: Yeah, ok,
R1: So, if they should at some point experience a cyber incident, they should go to us and then we will contact *anonymised*.
I: I think this is kinda what we thought your role was, so...
R1: Yeah, probably yes.
I: So, in case of a cyber security incident, what information is important for you to be shared? This could be what type of information can be disclosed. Also, what type of information can be disclosed to other companies? So it's DCISs, whatever...
R1: It's not all that can be shared among other institutions and so on. So, we have MISP and malware... what do you call it? ... information sharing portal, where we put our indicators of compromise. And we "what" how they are going to handle this information via the TLP protocol. Traffic light protocol. And in some cases we are sharing the information with other MISP around the world, because it's the same enemy we have when the days rising.
I: Cool, And this is kind of the answer to the next question, which is: where is the information about the incident shared? This also includes platforms, now you also mentioned MISP platform, is it shared with other authorities? How is it shared internally also?
R1: That depends on different cases and what we agree on , we pack when we are being hit by an attack. And so, some are more closed than others, some are not interested in sharing, so we agree, we respect other *anonymised*. If we can share it with the Centre for Cyber Security or the police, or other authorities, mainly be

those two. If we can share it within our community, if we can share it outside of our community, it can be with other MISPs within critical infrastructure in Denmark, or with the MISPs in other countries, CERTs in other countries. We have a network yeah... with 700 almost CCIRTs (Computer Incident Response Team) around the globe in 90 something countries at the moment. So, I think it's ninety nine countries now. It's a global community, to international organisations, where CERTs *anonymised* ... for as long as we could.
I: Perfect. And now it sounds like you have quite a lot of insights, so what is the status of the awareness from companies in terms of information sharing? In this case the companies that are related to your CCIRT (Computer Incident Response Team).
R1: Awareness or maturity whatever you... yeah. It differs, I'd say. Some uh... how can I put this in a meaningful way? It's very different, the level of maturity in regards to sharing, to see what should be shared, what could be shared, so... What can we say about that?
R2: We are not ... in the maturity level, we want to be... we are much lower in fact.
R1: But as a sector,
R2: We as a sector and critical sector in general in Denmark is not prepared to share this information so far. But we are working to us to do it in a reasonable manner.
R1: We need to see in our sector *anonymised*, but for a couple of years until 31st of December, we also handled another *anonymised* sector. Which is probably pointless taking out of your strategy and the strategy for cyber information security. Now there is a new strategy, and that means that 15 areas of a societal importance, which all will contain some level of critical infrastructure. As to be with that. And that means also, that our sector will be regarded from now as one of the societal important sector. And that we will identify critical infrastructure at the entities *anonymised* and so on.
I: And this is kinda a follow up, but are the companies prepared and do they know the legal requirements to disclose in terms of incidents. I don't know if you have an idea of that.
R2: I have worked in a critical sector in *anonymised*, so... yes, they are aware of the requirements, but I don't think they are using it as an excuse for not doing the thing, they are expected to do.
I: Yeah.
R2: But it has to be as I mentioned before a maturity level we have to go through together both in the critical sector and in... what do you call it...
R1: The important societal...
R2: The important societal sector.
R1: And no sector is critical anymore. It can only be a part of the infrastructure

that is critical under the new definition, in the new strategies. The old strategy had six critical infrastructure sectors. We don't use that term anymore, so it's all 15 important sectors including these six former critical sectors that are not critical anymore. But some of their infrastructure might be critical. Or less critical of course, but...
I: Yeah, and that's also something...
R1: and looking at it in a different way we are using another model for definitions,
R2: But there is no secret, that there is challenges in what the authorities want us to be right now. But don't underestimate these, because, if something happens in Denmark, we are going to use unofficial channels to communicate these issues we have.
I: Yeah,
R2: For instance we have these encrypted channels we are using internally both in the critical sector and the important sectors
R1: They are all important sectors. There are no critical sectors anymore.
R2: But we still have critical sectors within the important sectors.
R1: Critical infrastructure within all of the 15 important sectors.
R2: Yeah, ok
I: Ok, nice. And this is kinda a follow up on the previous question: what you share and who you share it with, but do you collaborate with other entities and how do you establish and manage trust with these entities?
R1: Regarding out international community, remember, establishing trust is a question of knowing people, meeting people at international meetings. So when we meet up more than once or twice, seven times some people and you also have a communication within *anonymised*... trust. It's a trusted network, where you know people through others and other people trust that you trust these people and you are with them and talk to them. And as one of the former chairman of one of the communities once put it:" what we have here is not peer-to-peer network, it's a beer-to-beer network", because it's a question of: have you shared a couple of beers and met the person outside the more formal part of the meeting, it's easier to build trust.
I: Yeah,
R1: It's a little bit the same within our *anonymised* area, within Denmark, between other access here, that the personal knowledge of people, that is important for building trust. Also what institutions, what teams are they member of, what are their territory. If they are employed in one of our peer's teams and other CERTs or the police or the Centre for Cyber Security, It's easier to trust these people. Because you know, they have been vetted by the employer. And that is also a part of building trust. So, true collaboration between the teams and true ... yeah, meeting people, talking to them that's the way that we gradually build trust. We don't have trust from day one. Don't misunderstand me, we trust you Michael, but you seem

like a nice guy. We trust you, because I know your professor
I: Yeah
R1: So, that's also a part of... I have a good personal relationship with Jens. And when you put his name forward, he was under your mail, that you sent. That's part of the way that we know, we can trust you.
I: Exactly. And that's also what we have heard, that it may not be directly, but it can come from an intermediary that you trust and then you trust one day, *unclear speach*
R2: but I think we in general in Denmark we are on the right track right now are on the right way to build trust between different sectors and within the next three-four years we are going to build this trust into a formal structure of how we are doing and warning each other. So, it's on the way, we are on the right direction, but it takes some time. We are much more than the Centre for Cyber Security has expect from the strategy
I: Yeah, and I think, I would also like... because you have also mentioned the international partners, but how many did you partner with inside Denmark, so the DCISes and CERTs we have inside Denmark
R1: more or less all of it I'd say.We have a relationship with other CERTs and of course the Centre for Cyber Security, that's what it's called "the cyber situation centre now". We have good personal relationships there. We have good personal relations to *anonymised* CERT, we meet up with *anonymised* CERT from time to time, also teams in *anonymised*, also a small CERT in a company *anonymised*, that we have personal relations to... who more?
R2: the *anonymised* sector...
R1: the *anonymised* sector. We know *anonymised* and a couple of his people. Head chief, of course *anonymised* that was... they live here, they used to live here... so we know them. Very good, so... also the *anonymised* sector, we meet with the *anonymised* from time to time. *anonymised* I don't know so much
R2: No, *anonymised* sector and *anonymised* sector are ´not so active, as we would expect them to be. Because they are still extremely...
R1: NO, nevertheless, in another network, I actually meet with *anonymised* sector from time to time, but not *anonymised*.
R2: That's not true I just, one of my colleagues just ended up in *anonymised*, and I met her in cyber network just recently, so she is new there. So, we are actually digging up contacts in there (all laughing), so,
I: Nice
R2: There is life in the end of the tunnel, so it's good. So, I would say, what's on the international list of CERTs in Denmark, we know them. We have a close list within the Nordic countries between the different types of network *anonymised*. Then we meet on the regular basis, like we meet with CISOs, the chief information security officers of the *anonymised* also on a monthly basis.

I: Cool,
R2: Plus extra, So there can be some work in between the meetings as well.
I: Cool. So, the last question and this is more specific to our project, because we want to create a framework, which allows information sharing within the important sectors as it is now. Could you describe the ideal information sharing system for your organisation.So this could be, what information to be shared, who to share it with, authentication, all of this.
R1: Yeah, yeah, ok. Alongside MISP, I take it as you know MISP.
I: Yeah.
R1: And how it works, yes. We are set up on *anonymised* network and we are connected to other MISPS as well. Along side of this we also use a chat called Mattermost. It's used as one operator by *anonymised* CERT, used for CERTs and DCISes. We have set up Mattermost between the entities *anonymised* and between the cyber information security professionals at those entities *anonymised*. We've been there often within the IT departments. Byt yeah, the cyber information security professionals are our reference group for security.Som we have Mattermost there alongside with MISP. It is protected , it's using. . . and I think It is using internal encryption. And we use two-factor authentication with *unclear speech* that's also important both *unclear speech* or what you call it. So we can be sure that those who are on these platforms bith MISP and Mattermost they are vadid people and they are using this two-factor authentication. That's a requirement for such a tool that we support all the normal security functions.
R2: well I would say that MISP and is the new "black" in the community.
R1: also internationally
R2: yeah, internationally too. And we have this Rocket tool..
R1: Oh, yeah, in the Nordic countries it's another chat. And in other parts of Europe you'll see Slack, also internationally, but Mattermost that's mainly in Denmark I think. I am not sure we have so much use of Mattermost in the international security environment. No, but still we are able to communicate through encrypted communication channels , whether it is in Denmark or abroad.
R1: Internationally we are using PGP encryption, so we can encrypt messages and sign and encrypt messages
R2: and I think that one way that we are going to warn each other is that we are going to use those kind of Indicators of compromise, which we are in our case uploading in MISP, for instance, or we are telling the other constituency directly via Mattermost, that we have seen these Indicators of compromise. The idea of using these Indicators of compromise is that the different institutions can import it directly to their own interface . . . . So that is also another way of communicating these incident
I: That was actually all the questions I had, so thank you very much for your time.
R1: You are very welcome

R2: You are very welcome.

### C.2.6 Interview with the respondent A7

Interviewer (further I): Perfect, so I have started the recording, and I will ask again for GDPR reasons, is it okay that I record?
Respondent (further R): Yes, you are fully permitted to record.
I: Perfect. Just to briefly introduce you to the project, it is about information sharing in the Danish critical infrastructure and we want to create a framework to enable information sharing in the critical infrastructure. The reason we focus on them is because of the NIS directive which require this sector, or this part of the industry to share information, whereas the rest is not really required to by law. And in that regards we are contacting security companies, critical infrastructure companies and authorities. So that is why, it is interesting to talk to all of you because you in one way or another have something to do with critical infrastructure. So the first question, can you tell me what is your role in regards to incident management and information sharing?
R: I am a cyber security analyst and I am incident coordinator in our team. So I am working on a daily basis with both.
I: Perfect, are any of your costumers in terms of cyber security in the Danish critical infrastructure?
R: Yes.
I: Okay, and just to mention, it is anonymous and you can at any time say that you cannot reply if there is anything.
R: Mhm.
I: In case of a cyber security incident, what information is important for you to be shared?
R: From the customer?
I: Yer.
R: The most critical things is usually where things happened and what they have seen, and what are their critical assets in their environment? Those three things are in regard of planning and general execution of incident management, the three most important parts.
I: Yer, where is this information shared for the incidents within the critical infrastructure companies? So either, where do they share it with you, and do you share it with anyone else?
R: We do not share it with anybody else. We have a confidential channel with the customer. But usually it is shared where it is needed, either on a server at their end or our end, that depends on the criticality of the incident and the stages of their environment in general.

I: Yer, so, do you share any information at all with any CERTs or authorities in terms of incidents?
R: No, if we advise the customer to do it, we of course help them, but it will be them who are sharing the data, we are not doing it. We are helping them and preparing the data, but we are not sharing.
I: Okay, how do, so one of the things we have heard from the critical infrastructure companies, is this trust. So we are trying to figure out how do you establish and manage trust between the parties, so between you and the critical infrastructure companies?
R: I think, we have two sets up costumers so to speak. We have the customers who are customers in the house before the incident and we have those who call us and say "we need help", please help us. And the first type of customers, the ones we have in our grasp before the incident, we are establishing a trust relationship with them as part of the whole customer provider relationship. And they know us, and we are doing a lot to make them know us and to prepare for whatever cases might come and so on and it is an important part of the on boarding process. The other customers are harder. Usually they are calling us because they know somebody who have been in touch with us before and then it is like a trust relationship in a triangle with some unknown part. And yes, word to mouth type of relationship.
I: Yer, so in case it is kinda, because they trust the other party, they also kinda trust you because they say they trust you.
R: Yes, or they say our website looks professional and they want to trust us.
I: Yer, so while talking to your customers, is awareness of preventing cyber attacks important and does this awareness include information sharing?
R: Yes, awareness of preventing are important. Information sharing in general, no, and if you ask me there are too little in the general business of Denmark. People are sitting on the information, but no, there is no information sharing in like, no, we are not doing it as anything regular.
I: Okay, so the last question, and this is a little more open, but could you describe the ideal information sharing system for your company? That would be in regards to sharing with both the critical infrastructure, other companies, authorities and other security companies.
R: Yer, I think and it might not be for the customer, but my opinion in general or for our company, but my opinion in general. There are too little sharing in Denmark, we need some sort of platform and I can say MISP or anything like that, it does not have to be that, it could be a more custom made platform, but some sort of information sharing where everybody provides information and IoCs and tactics and techniques for general attacks they have seen and so on. We are behind the hackers, because they are sharing everything, we are not. An example, just after Russia invaded Ukraine, a little Danish company in Odense was hit by some Russian ransomware and they stated it might have been related to the attack, I very

much doubt that still, but they were very quickly out and say it was Russian, it was Conti (russian hacker group). But again, why not share any information about what happened? It does not have to be the silly part where they had open RDP or whatever was the reason for the attack, but what happened after the initial breach? How did they come around, how did anything go? We have not heard anything about that and it would help anybody else if we could share a part of that, could prevent things. So I think the information sharing you asked yourself earlier, the information sharing and the prevention thing is very much combined and we are very behind because there are so little information sharing.
I: And that it kinda what our project is about, trying to deal with this.
R: And the authorities are trying or say they try, the Centre for Cyber Security and FE (DDIS), but they are not even doing a really good job on doing it. There needs to be a more common authority that actually build up, I think it has to be an authority, I think it has to be some sort of related to the government.
I: Yer.
R: Or Centre for Cyber Security or something like that. That puts up a place where you can share part of fully information about. I think it is needed and all have to attribute to this, of course, to be able to, and that is the hard part, because of course there will be some companies who are feeding in a lot of things and there will be somebody who will be feeding zero things and just harvesting. And there has to be some fairness and that is where you project surely will find some exceptionally good solution. But I see the problem from a commercial point of view, but as a technician it is a problem that we are not sharing any more.
I: Yer, and I think one of the things a lot of people have mentioned, what if the hackers get a hold of this information, because if they know, oh they have found this or this or this, it might compromise their capability to secure themselves, because the hackers may just change their IPs or something. Should there be any authentication on this platform so it is not just anybody who can go in and see that?
R: I think the best part is if there is an open and a closed part of the platform, so you can actually see who are harvesting the information and without providing any new, so it might be easier to contribute this fairness thing. In my opinion, you are saying, then the attackers could change IP addresses and domains and so on, but yer, they are doing it anyways. I think, and it, I am more interested in sharing techniques and tactics. How did they come in, not from where, but how? How did they spread on the network, and how did they exfiltrate data, not to where, but how? It is a lot about how and not where, because IP addresses and domains, they are changing, but if you could say they are using powershell and tools that did this kind of things, then you would be a long way. And yes, the hackers might find out you know that, but it is harder for them to change their infrastructure from using DNS exfiltration to HTTP exfiltration, than just change their IP address, so no I am

not afraid the hackers will at all, yer.
I: Yer, okay.
R: It is a risk, but I think the advantages will far out weight it.
I: I know you are in a hurry, so my last question, just to sum it up, but now you said an open and a closed site. How would you differentiate, like what would you have on the open and what would you have on the closed?
R: The open would be the IoCs, domains, IP addresses, like that. And then on the closed site I would have the more interesting stuff, and it might also to ensure people are not only harvesting but everybody who are harvesting are also contributing to the platform of some sort. So it is also that half of the commercial companies are dragging out data to use without giving anything back. Because this is a community thing, for commercial companies and yes, it is a tricky part.
I: Yer, cool, that was actually the questions we had, so thank you very much for your time.
R: You are very welcome.

### C.2.7 Interview with Expert E1

Interviewer (further I): So, I have started the recording and for GDPR reasons I will ask again is it OK that I record?
Respondent (further R): It is perfectly okay that you record
I: And will just ask again is it Ok you are not anonymous?
R: It is OK that I am not anonymous.
I: Perfect. So, as we briefly talked just before, our project is a master thesis at Aalborg University in Copenhagen in Cyber Security and we are writing about information sharing in Danish critical infrastructure. Hmm.
R: Yer.
I: And in this regard we have contacted critical companies in Danish infrastructure and we have contacted Security companies and we have also contacted CERTs, DCISs and another authorities. Uhm, and this is kinda where you, your product of the Danish MISP came up, and your name came up which was very interesting so us because it is kind of the same idea we want to do. So, we want to hear how you have done it and how, what you see as challenges and potentially maybe what you could help us with throughout this interview, right?
R: Yer.
I: So, I think I will start by asking, so just to say we have not prepared any question per se, because I want this to be an open discussion rather than just strict questions. But I have thought about some things. And one of the first things are: how did you start this initiative.
R: Year, so, so the reason that I started this is that I have been using MISP for what is it now five to seven years, or something. I have started using it when it was very

new as a sharing platform. When I saw a issue of sharing information, because I have also been part of a closed source information sharing initiatives and it is typically going over email.
I: Yer.
R: The issue was: one thing is to get all this data but how can you actually consume it, how can you use it. So I said instead of it just being another email in a folder. So that is where I have seen the biggest use of the tools like MISP.
I: Yer.
R: So it also gives a good way to structure the data when it comes in allowing it for easy use, maybe into your SIEM solution maybe your firewalls, etc. But for actually making it functional that is the fancy buzzword.
I: Yer.
R: So, so with that in mind I started that. I utilised MISP myself and the companies that I have been with prior, but I also so that again there is a gap between sharing initiatives and so I decided to start up the so to say the Danish MISP community without knowing how many or if anyone was actually interested in attending.
I: No.
R: So, so it is a project that I am funding myself running the infrastructure, maintaining it at that is being done through my own company eCrimeLabs so that is the sponsor for that part. And then I actually started reaching out to whoever I knew in different companies that I have set this up if anyone was interested and then slowly a lot of companies signed up to it.
I: Yer.
R: So, that was so to say the initial stage of it. Now coming to so to say the key element of it is actually that one thing is setting up the infrastructure like that and the second part is how much do the individual organisation actually contribute. And that is where I think in Denmark is some sort of what can we say: I call it 'share scare' so either the companies are scared that the information is irrelevant to us or they are scared that the information is targeted to them that they are afraid that someone is going to use this information against them and that is sort of the key issues that I see when building communities like this, it is the trust. Figuring out how do we get people to share so, I would say that I am maybe the biggest contributor to the community MISP of data that I find interesting and pushing it into it. But my hope is that even though a lot of people are not sharing much for now, having the community, having people from organisations signing up to this a lot is that if sometimes it becomes really relevant it is in place.
I: Yer.
R: So, I do not see it as a negative thing that it does not exist yet. I saw that and I also heard from organisations that some of the information that I collected especially during COVID (refers to COVID-19 pandemic period) on some of the phishing campaigns that were utilizing that and sharing that information helped

them detecting attacks not necessarily successfully attacks but they could utilize it in their spam filters, etc. to actually identify that this was something potentially bad.
I: Yer.
R: When act upon it. So, so I see that the maturity of starting for organisation to start to share will take time it might take years it might never get up to speed but having the infrastructure in place, having the community in place brings a lot of, what can we say, possibilities similar to when you have a fire station. You hope that you do not have to never use it but it is good that is there.
I: Yer. Yer. Are you still here?
R: Yer.
I: Yer, perfect. (laughing) Cool. I think that it is a good answer. And kinda also what do we want to look into throughout our thesis. Uhm I think the next question is: now you mentioned that you reached out to companies that you knew and people that you knew in companies. How many do you have on the MISP right now? If you know.
R: I think there is around 30-40 organisations.
I: Yer.
R: And that is covering anything from, without leaking who is it attending anything from critical infrastructure, to governmental institutions to private companies.
I: Yer.
R: So it is a good subset across, yer the Danish industry. Of course I would always like to have more coming in but I think it is something that has to grow on its own and I am trying to push it wherever I need people to say: "Hey aren't you interested in this?", "Wouldn't this be interesting for you to be part of? ".
I: Yer.
R: So, yer.
I: Yer. So, I of the things that we have heard a lot is trust factor. And a lot of them say it is base on 'you meet them', so let's you and I met then the chance that you and I would trust a bit more than over the phone is higher right? Because we have seen there is actually another person there. Uhm, how do you make sure there is a trust? Apart from, now you have reach out to people you already knew. But with the remainder of the companies how would you insure trust and that would trust you the other participants?
R: (sighs heavily) I think that trust that is also a worry. You need to decide on what is it that sharing because, let's say that you have an incident in an organisation, you don't necessarily have to share that you were hit by this, or how it affected you or anything about your organisation but some maybe some parts around what was indicators that were identified, what were the actors doing. But there is a large physiological work that I think again, if we look back, it is always about the trust,

people have to meet and we to some extent need to also find the way to mature in this way. Also with the globalisation, with the new 'everyone is working from home', your colleagues may not be sitting in the same country and things like that. So, it is hard and that is one of the key pinpoints today. One thing is for organisations to maybe identify what is it that that they want to share and that have someone to sparre with on "Ok how can I do this in a way that I also feel comfortable with". And then the second part is finding the way to understand physiology. I fully understand that you will have some trust in network like "Okay, in these I would like to share much more information, much more details", but in others is more okay, this is, we gonna say the trust is based on that we have the common goal to try to also battle to them back as we can't do it ourselves. The bad guys have figured the way to also sharing information.
I: Yer.
R: So, if we aren't doing we will definitely be loosing the battle. And again we gonna say, the bad guys also have different trust levels so they also have someone who has proven that they are criminals and they can be trusted that that is where both the MISP and another is also the way that you can create a small sharing groups. So what you need there is of course to trust the infrastructure on it is being hosted.
I: Yer.
R: But after that you can also supported it, "Okay, here I have some I want to share with everyone in entire world" and that is the entire sharing design of MISP. "Here is something I only want to share on this instance", "Here is something I might only what to share with a small subset of organisations".
I: Yer.
R: And that is also why today there is, there is not, there is also within Denmark a small in DCISs there are closed environment for different sectors where they share only information relevant to telecommunications or energy or yer, the others health and that is where the understanding of how this is working, how you can also be as much as possible secure of what it is you are sharing. But seeing it as it was before as with the mailing list, the email has been in the past that you can create these embedded groups as well.
I: Yer, OK.
R: Where you say OK, I only want to share this with this group of the people where I have actually have meet the people. And there is where we have two companies saying, "OK, we share each other so much if I have any information I will send that to your MISP and vice versa", but that will not be shared outside".
I: Yer. Because this is one of the things we have looked at or when we have asked people I think they have trust a certain amount of people and they do not want to be shared further than that. Uhm, and that is also when we talked to the DCIS and CERTs as they also mentioned that if we talked to or if they have their clients, they

do not really want that to be shared further than that they do not even what to share with everybody in that CERT because they might be too many, or whatever it is depending on the CERT. So the trust is proven to be very big factor.
R: Yer. So I see the issue today is not the technology, the issue is people.
I: Exactly.
R: The issue is figuring out how can first of all, maybe change the mindset of people for some of the information because not all is, we gonna say, if you for example receive a phishing campaign abusing NemID or MitID or something, that is something that is hitting everyone.
I: Exactly.
R: So, why don't share it. And that is also what I see that when I share it as a consultancy company, I actually see that as also we gonna say show people that first of all that I would like to share I am not only in it for the money but it also brightens me to some extent. So, at least for the consultancy companies they can also to some extent use this as a branding because not everything is proprietary and "Oh, we are the only consultancy company that has ever detected this kind of threat".
I: Exactly.
R: So it is a way, we gonna say it is the people part that seems to be the biggest issues currently, and I don't know, hopefully generations will change because we are getting more and more virtual and we built these trusted networks by being virtual, being talking to each other but also understanding that not everything is a targeted attack and not everything needs to be protected in the same way as other information.
I: Yer, because yer, exactly.
R: Yer.
I: And I think we fully agree especially based on what we hear from, people are fully trust that whatever technology they use that is secure because it has been being used by thousands if not millions of companies and billions of people worldwide but the problem is that they don't trust each other. Because they need, it as kinda, we consider it, was it PGP or whatever, where you like have one person you trust and more people trust that person the more you also trust that person but you have to know that person before you even trust them in the first place.
R: Yer, and that is where the technology and the development is supposed to forge this because it can build anything from more or less person to person sharing to "I would like to go and share this as far as the information can go".
I: Yer. Yer, ok, and I think, yer. I think that is nice. One of the think that they have uhm, that we have also heard was that one of the big inhibitors of this would be if an attacker got into this MISP, basically, because then they can follow along, "ah, they found these domains, we need to switch domains" or "oh, they found these things" or whatever so they can kinda follow along how far are they and how far

are we from being protected.
R: Yer, and that is where I would like to challenge that thought. Because I fully understand it but I would like to challenge it a way so to say "ok, you have fifty people that you trust unlimited". If you have used the good old mail to share then you have fifty mail boxes that could potentially be compromised.
I: Exactly.
R: With MISP you have one system or maybe a few systems that you will add more security around, then it means that there is much less for it to be yer, public.
I: Yer, but I am also, I also think the fear if you make a common MISP kinda like what we are thinking and what you have done is that they fear who will end up going into this MISP. And of course it should only be relevant people, that makes sense. But how do you ensure that there is only relevant people and it is not some foreign hacker group that somehow got in?
R: Yer, so, so the way that's the setup is today with the Danish MISP community is that it requires for you to be present in Denmark and have a Danish CVR number.
I: Yer.
R: So that is the requirement for, for attending and of course foreign organisations might also get access to this or be able to create a company, but again you still decide what kind of information you share. Also if you, have you heard about the Pyramid of pain?
I: No.
R: So, guy called David Bianco invented Pyramid of pain, where he talks about that at least some of the, so to say, static information like domains, IP addresses these are usually changed by the adversaries and and higher up the chain you start to hit it the way it work with the data and perform an attack, similar to the way where you can see how did they utilised tools and based on that build the protections.
I: Yer.
R: But, technically if you start out small sharing information it could be on the level where we can see those IP addresses, that will actually allows other organisations to search for, if they have been attacked by this. So, even if the attacker got hold of this list but saw that they were in quote 'burnt' they would still be in the log files.
I: Yer.
R: So, so some of the data would be be seen as sort of aged, but it gives you a retrospective look into seeing "Have I been affected by this?".
I: Yer.
R: So, so one thing is with spam mail campaigns you can see "Okey, I can block this preventive to make sure that it doesn't, I do not receive anyone from this source or this IP address", but I could also use it retro-perspective (refers to retrospective) to look into "Have I been hit by this?" So it is also again the matter of understanding what it is that you are sharing and what is it the effect of it, it is a risk based approach that each company, each user of MISP or any other platform need to do.

If you share any information through email with a trusted source and that organisation is also hit by a targeted attack or state-sponsored attacker then they would also have access to the information.
I: Yer.
R: And so the issue is as far as my approach is: when it is in your mail box how do you utilise it? Would you sit and extract each IP address from your mail box from each mail that comes out around something from trusted sharing partners and then go and search one by one in your SIEM maybe add it into your anti-spam solutions maybe adding it into your firewalls, or do you like to have it in a structured location where it also gets context?
I: Yer.
R: And I think it is again, I think everything hits back to the psychology and the understanding on that there, there is so much data out there: How do we get it as fast as possible from one place to another in your technology stack?, From your threat intelligence parties to your infrastructure. And understanding that will, will help this.
I: Yer.
R: And again, lets say that you have information where you say: "OK, this is so targeted so that it might only be relevant to some." Then you still might go back and share it through email to only trusted people or you might have MISP instance where you share the information between those two. And again technology help you. Because MISP, if you wanted to you could use it to say: "Ok, for the community to share it, for the more targeted ones I maybe keep in in the MISP instance that is only accessible from the specific IP addresses, locked down with 2-factor all these things", but you can from the technology perspective use to protect the information.
I: Yer.
R: But, it is an understanding that needs to be we can say: 'grown to the people'. Not all information is related to state-sponsored attack, not all of it is fully targeting 'you', but again it is, with that understanding I think that will open up for more we gonna say sharing. And there is of course the element of people being afraid that: what they put in there is being seen as not relevant. But again, you can always get it it up for the discussion, because if you find it relevant, then maybe someone else might as well find it relevant.
I: Yer. Because that is what some of them have mentioned, now we focus on the critical infrastructure because they are required to share information according to the NIS directive and some other legal obligations too. Uhm, and that is what some of them have mentioned that we may not or the *name of the sector* may not care too much if the *other sector name* is hit or vice versa, because what if it's very specific to one application, but at the same time it could be an attacker is inside and trying some automatic attacks or whatever. So, to have this knowledge

could maybe gain them and even so ransomware hits everybody, DDoS attacks hit everybody, phishing and so on. So, having it is from our perspective still very valid, even though it may not be valid in every single use case.
R: And also, let's say that you have *refers to previously mentioned sector* and *refers to other previously mentioned sector* how, if I were sitting in the *refers to the first sector* and OK we have a targeted attack here, how do I know that it is only targeted to *the first mentioned sector* and not to also *refers to other two distinct sectors from the first one*.
I: Exactly.
R: Especially if you talk about espionage. Then, then some of these areas might just be the means to go.
I: Exactly.
R: And, and again we have a lot of time where we put the targeted attack or the state-sponsored attack up on the pedestal like they are so advanced. And of course some of the things they do are seriously advanced, but again they are also humans. They also make mistakes. And they also need to work on the budget where they might use the same infrastructure for two specific attacks. So, again the point of knowing when something is so targeted that it is not relevant to anyone else, that is really a hard question to answer without being biased.
I: Yer. So, I think I will ask the next question that I have in mind is: Do you think that there is enough sharing?, in, now we focus on the critical infrastructure, but it could be in general too. I don't know how much knowledge do you have into it but do you think there is enough information sharing in regards to security incident?
R: Uhm..(sighs), no. I would like to always see more sharing but again it is a maturity level that needs to in some way evolve.
I: Yer.
R: So, I am not hammering people for not sharing, I fully understand it, and that is where everyone needs to log into "Ok, what can we do to find the way to do this securely?". Find the way to get better at trusting. Do we need, if we need vetting what are the criterias for vetting or starting to talk openly of what is actually the though about it. Because, sometimes it can also be just time.
I: Yer.
R: So, so if you have a small organisation that only has one person or something: how can they spend the time to actually share this information, so also, there can be a lot of reasons why?. But I would say that the sharing part can be much better. I would say that one of the key examples on sharing initiatives is, you should look at  of Luxembourg, so the community and the things that they have been able to is really amazing.
I: Yer.
R: Because there is, we gonna say a private sharing community run by  that actually shares across multiple companies, organisations both consultancies, and also

privately held, and governments. And they are sharing different things. I also have seen some organisations, they do not share themselves but if they see events where they might have some additional information they will extend the event and add information to that, that event.
I: Yer.
R: So, it is also, I think it was on one of the trainings on the MISP where they took as example a small company where a guy there have set up a MISP, they figured out that they were targeted quite heavily and they are very targeted, he found some examples and shared that information. And then within a short time there was someone who actually reversed the binary and started to share additional information back.
I: Yer.
R: So, even if he did not have a full picture what was going on and only had a subset of it he were actually, it was possible for him to get the information back.
I: Yer.
R: So, again, we need to share more.
I: Yer.
R: Hundred percent. But we also need to do it in the way we feel comfortable with. And that is where talking openly about it: "OK, what is the it?", is it time, is it resources, again the 'share scare' that the information that I share is not relevant to anyone else, and what are the 'pain points'. With that in mind, then we can start figuring out how can we do this to support those concerns and minimize the risks that has been identified by some.
I: Yer.
R: And also support that some will share, some may never share, but as long as they are part of the community, a part of some of these things, they have access to the data that might help, again identify something with their environment that someone else has identified.
I: Exactly.
R: So again, when I run the Danish community MISP I never expect anyone when they sign up to share anything, I hope it, I emphasise it and I try to support it as much as possible but I don't expect it I don't put any pressure on so to say "you have not share anything so you will be popped out", no. Because it is important that you share and if you and your company get mature and have time, all the things that seems to be the 'pain points' gets removed they you might start.
I: Yer. And I agree on that. And I think that Danish Community MISP is very interesting to look at as an example for us. So, I also want to ask: now you said that in order to get onto this MISP you have to be located in Denmark and have a Danish CVR, do you check that manually or do you have the automatic process for that? And how do you ensure that is actually a company behind this CVR that says it is so I did not just come up with this, for example Maersk's CVR number

and said I am Maersk.
R: So, again I do not when creating, it has to be so to say an email attached to that company, so the domain has to be owned by that company so I am not, if you come with the 'gmail' account I wouldn't create that. Of course if you said you have a company who were attached and you decide that for some reason you would like to add every company comes organisation sign up, so the first people to sign up will be responsible for creating new users, maintaining the users in their organisation. So, if they choose to use Gmail or something else I wouldn't be able to just stop that. But I try to do as much so to say manual work and I actually had one request where I saw that the CVR number was created like two days after I told that person that there needs to be CVR number and that is not something specifically designed but I also tried to do as much vetting as possible.
I: Yer, OK. And this is done manually I assume.
R: Yer.
I: Yer.
R: Yer, so I have like 10-step guide like check the CVR number, check the email address, check the website. Open source intelligence.
I: Yer, OK. Uhm, nice. How do you ensure that people are anonymous in there. So, let's say I am just going to use Maersk again as random example. That how do you ensure that they are anonymous if they report anything. So, if they report it under MISP platform their name won't be leaked.
R: So their name, of course I can not ensure that if someone else gives to the system or if shared in that is shared but the data is staying in there. And when you create an event within MISP it will be attached with what user created the event and what organisation they belong to.
I: OK.
R: So, that is the part, an element of it. MISP also do support a functionality, what is called, where you can, you can have, we gonna say, what is it that I am looking for, the word. So, they can forward the event to let's say me. Then I can go in and accept this event, and when it is being published their reference will be removed.
I: OK.
R: So, you have like the capability or at least the possibility it is not something that has been use in the Danish MISP. But I know that is something that has been looked at in some of the DCISs. So I have to weigh that if someone would like to be anonymous there is the clearing house capability at least with MISP because then, the entire event will be rewritten.
I: Yer.
R: And that all, we gonna say you can then remove of course while you are vetting the data, you are looking at the data you can then remove anything that could potentially point back to the organisation that were being targeted or something.
I: Yer.

R: So, again technology and the solution supports this.
I: OK. That is nice to know. Do you think it would help getting more people on if they have now in the quotation marks 'more anonymous' way of reporting? Because this is some of the things we thought about, it should just be this sector, so not a company name but just a sector name is being mentioned so like telecommunication or health, transport of whatever is hit and these are the IoCs they see.
R: For some it would help, I don't think necessarily in quotes 'hiding under the common' we gonna say 'common name' for like TeleDCIS or SundDCIS or EnergyDCIS but I think the clearing part could potentially be or I would see as to be the best solution for it. I: Yer, OK.
R: Because also it the way you will have to do this yourselves whereas is to create one big organisation and then also how can you potentially something that is wrong report back to the people. That here is something that you need to log into or here is sending some information. So, the part of just putting every company withing the same bucket it is of course the possibility. Is it the best possibility maybe, maybe not. Again, it depends on if you feel like that you are not comfortable with sharing I would always prefer we gonna say the clearing house solution.
I: Yer.Yer, I understand that. Have you look into any other platforms than MISP or was MISP the first one you found?
R: So, I was looking into something that gives context, because there are many we gonna say solutions that are used for bulk IoC collection like IntelMQ and something like that. Where is just a large database but the issue that I always found is, the reason that I log into MISP is that you get the possibility to get context. Typically in lot of security solutions is that they will tell you: "Okey these IP addresses is bad". -Thank you. (laughing) Now, how bad is it? Is it bad spam-way, is it bad targeted attack, is it bad that it has port scans or something in what context is it that is bad?
I: Yer.
R: And that is also one of the pain points. Also I have seen somewhere, you get a list of MD5 checksums, and SHA-1 and SHA-256 but there are no correlation between these, so you have no idea again, you have just a list, you don't know what is it that you are looking at other than IP address or a checksum.
I: Yer.
R: So, the MISP has the potential of adding a lot of relations to it also the way that you can build the relations that you can say: "Ok, I received this email that contains these attachment, that when executed, downloaded another or went to this domain and downloaded another attachment. That was actual so to say code", so it was just a robber so you can tell the story. That is one of the things that I really like about it. There is of course the STIX format that was maybe one of the first, but it also has some issues. The implementation of it is not always I have not seen any open source solution that support this. So I would say that there are definitely

some commercial elements and I think, a lot of them are working with the STIX format and to have the context element of it but then you also have the bulk IoCs collectors. Where you just need to say OK I collected it from this source then I need to give it there to try to identify what is, what is this data.
I: Yer, OK. I think this is a good reason. Uhm, obviously something we have to look into the report, right? (laughing)
R: And then, of course I would say that at least in a Europe and I am starting also to see it quite extensively being used in the U.S. but it is more or less a 'de facto' standard for information sharing today. (refers to MISP in this paragraph)
I: Yer.
R: And that is also what I can see where the MISP is really good, but it is really heavily supported open source project so it is not something that goes away. It is something, that everyone can actually afford. So, you, if you are a small company you do not have to go out and invest like 2 million as continuous service for some enterprise intelligence sharing platform and I think this is also one of key elements of it being a success. An amazing work that the team behind is doing and the entire community about the development of it, then the support from also very trusted partners I think that's one of the main part that as high status as possible. As for now for all the work that I have done also working with incidents I haven't really found a way or a scenario where it didn't solve my problem, where I found something better for structuring data. There has come the OpenCTI project, but that is much more we gonna say focused around directly threat intelligence and some of the capabilities and again it is also integrating with MISP, collecting data from there. So, so I would say for sharing platforms and for also a lot of intelligence work, also for IR (Incident response) people incident response people for security departments this is an amazing platform.
I: Yer.
R: And I am not getting paid to say that.
I: (laughing)
R: It is my strong belief that this so many issues.
I: Yer. Cool. I don't know if I have much more or any more questions. I thing the or the things you have said are very good and I think they are very valuable for our project, which is also very nice that you could take the time for us.
R: Perfect, and if there is any additional things then please let me know, we can set up another meeting or throw me an email address or throw me an email, if there is any additional questions that you would like to have something put on.
I: Yer. Uhm, yer I will. Thank you for your interview and thank you for you time and thank you for that offer. I think I will just stop the recording from here.

# Appendix D

# Relevant Emails

## D.1 Email 1

Har svaret på jeres spørgeskema.
Her er nogle undren/feedback til jeres spørgeskema.

- Har I overblik over hvilke rapporteringspligter selskaber har ved en cyber incident?
- Hvad ligger i en minor og middle og major size incident? Snakker vi om kunde impact?
- Er det nok at I får at vide, at vi dele en incident med nogen (some entities)?
  - Eller har i behov for at vide om
    - vi kun deler med myndigheder og ikke selskaber eller begge dele?
    - hvilken detalje grad deler vi?
- Har i brug for vide, om der er nogle omstændigheder der gør, at vi ikke kan dele? Og hvad er disse?
- hvis man skulle lave en framework der kan samle nyttigviden og samtidig sikre, at firma ikke udstiller sig selv, hvad skal man så tag højde for??

Med Venlig Hilsen / Best Regards

## D.2 Email 2

Kære Michael
Tak for snakken – som sagt så har jeg kontaktet Dennis Rand og han har sagt god for at du tager fat i ham.

Dennis driver den danske MISP og har en masse (gode synes jeg) holdninger til det at dele

Du kan fange ham på rand@ecrime.dk (også cc på denne mail)

– Med venlig hilsen

# Appendix E

# Figure list

## E.1 Figures refereed in the report


**Figure E.1:** Finish ISAC [21]

| Purpose | Information Flow | Required Information Sharing Description | Examples |
|---|---|---|---|
| Routine and Awareness | Sector Group to Collaboration Group, Super Group to Collaboration Group, Collaboration Group to Sector Group, Collaboration Group to Super Group | General information that addresses awareness. | Routine security status update, daily cyber feed, external feed brought from outside of the community, general guidelines |
| Warning and Prevention | Sector Group to Collaboration Group, Super Group to Collaboration Group, Collaboration Group to Sector Group, Collaboration Group to Super Group | Information that helps incident prevention. Early indicators of potential incident. | *Technical Intelligence*: Port scanning records, exploited vulnerabilities from anti-virus application and system, tracked threats, IDS/IPS alerts. *Human Intelligence*: Warnings from other communities. Reports about abnormal activities for potential incident, such as suspected war driving. |
| Incident Reporting | Sector Group to Collaboration Group and Incident Group, Super Group to Collaboration Group and Incident Group, Incident Group to Super Group | Detailed information regarding the incident. Information about the type of attack, the source, started time, detected time of the incident, description, event data, symptoms, the destination port numbers involved, *etc.* | *Technical Intelligence* : Firewall logs, IDS/IPS alerts, system logs, data logs, port scanning records, network performance data, data from routers and anti-virus applications. *Human Intelligence*: Reports about abnormal activities (such as human errors) that caused a cyber incident. |
| Assessment | Sector Group to Incident Group, Super Group to Incident Group, Incident Group to Super Group | Information about impact, scope and severity and other information related to risk assessment. | Reports about the number of systems and sites impacted by the incident, the percentage of population denied access to the service. |
| Mitigation | Super Group to Collaboration Group and Incident Group, Incident Group to Sector Group, Collaboration Group to Sector Group, Incident Group to Super Group | Information related to the incident mitigation, response and recovery. | Mitigation resolution, incident action plan, recovery status report. |

**Figure E.2:** Overview by [113] of information exchanged

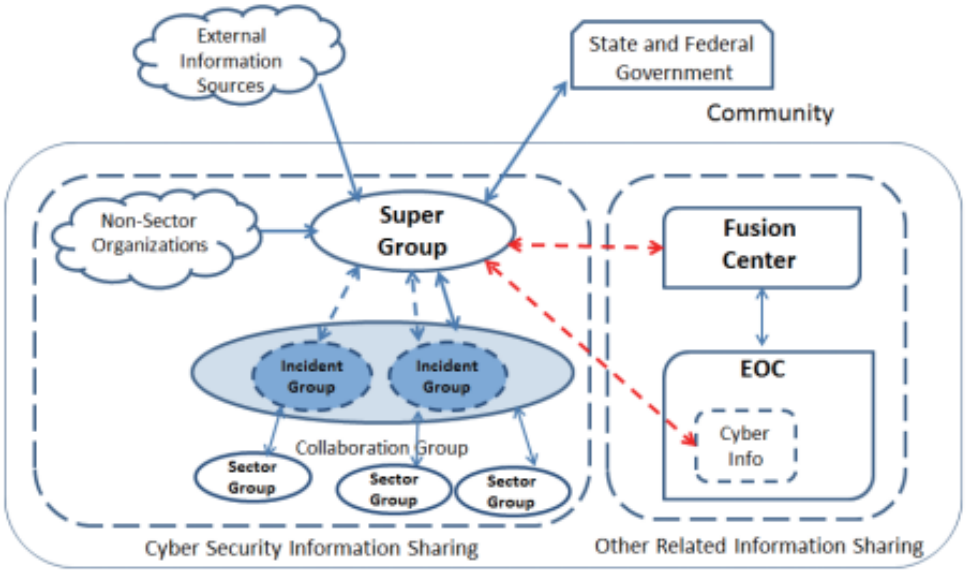


**Figure E.3:** Updated CGCISF [114]

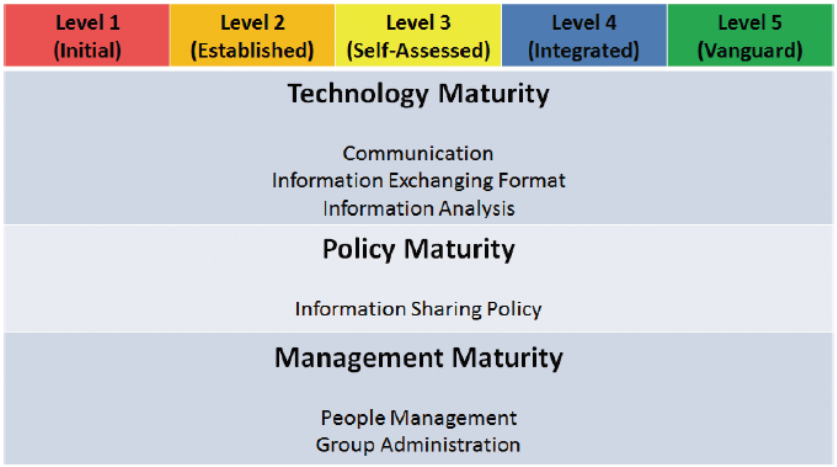


**Figure E.4:** Maturity model overview [114]

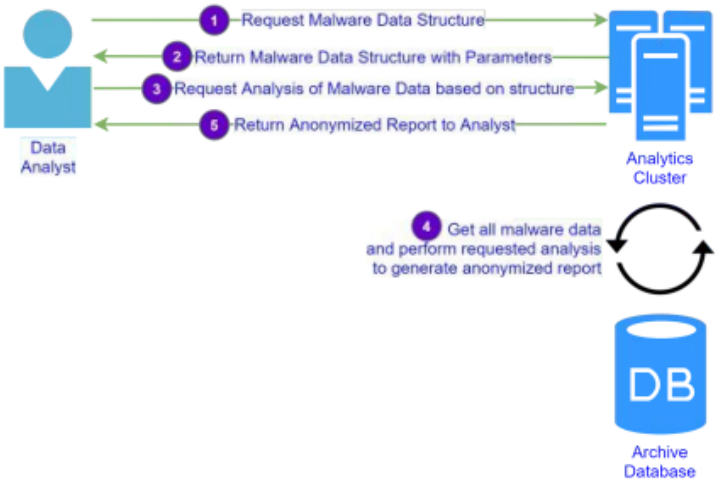


**Figure E.5:** Blind processing scheme [118]