Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Thea Svenkerud Rydjord
Ingrid Sørdal Volden

Cybersecurity Incident Management Process in Industrial ICT Systems

Master's thesis in Communication Technology
Supervisor: Maria Bartnes
June 2020

NTNU
Norwegian University of Science and Technology

NTNU – Trondheim
Norwegian University of
Science and Technology

Cybersecurity Incident Management Process in Industrial ICT Systems

Thea Svenkerud Rydjord

Ingrid Sørdal Volden

Submission date: June 2020
Responsible professor: Maria Bartnes, IIK and SINTEF
Supervisors: Lars Bodsberg, SINTEF
Roy Thomas Selbæk Myhre, TietoEVRY

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title:	Cyber Security Incident Management Process in Industrial ICT Systems
Students:	Thea Svenkerud Rydjord Ingrid Sørdal Volden

Problem description:

Industries face new challenges and threats, as systems and processes are digitalized. Whereas traditional industrial control systems had isolated systems, these systems are now highly interconnected due to the incorporation of information technology (IT) components. New technology makes it possible to remotely control and maintain an oil platform from land. However, it also opens up to cyberattacks, which can lead to loss of life and environmental and equipment damage.

Teams working with IT and operational technology (OT) (e.g., industrial control systems) may each have a distinctive work environment. Traditionally, OT has focused on safety and availability, while IT has been more concerned with security and confidentiality. This has resulted in differences when it comes to work culture, security goals, methods, time management, and priorities. Since OT needs to prepare for cyber security breaches, the need for cooperation between IT and OT increases.

This thesis will analyze both the IT and OT work environments in Norwegian oil companies and their incident management process related to cyber security events. By collecting information about the two processes, the intention is to map differences and similarities. Overall, the goal of the thesis is to produce a united process both IT and OT in Norwegian oil and gas companies can utilize.

Responsible professor:	Maria Bartnes, IIK and SINTEF
Supervisors:	Lars Bodsberg, SINTEF Roy Thomas Selbæk Myhre, TietoEVRY

Abstract

Industrial Control Systems (ICS) are incorporating Information Technology (IT) components, which opens up for remote access possibilities, advanced data analytic, and more. With the increased connectivity, follows the risk of safety now being compromised by a cybersecurity incident. This thesis will focus on current routines for cybersecurity incident management in two different groups from oil companies, IT and Operational Technology (OT). By analyzing how they handle cybersecurity incidents today, the goal is to identify areas where the two groups should align their interest to better face the threats of the future.

To address this, we will first conduct a literature review to get an understanding of the industry and to prepare an interview guide. Semi-structured interviews will be used as the primary data collecting method, and we will interview employees from both IT and OT of several Norwegian oil and gas companies. Results from the interviews show that the industry has a high focus on the period before an incident happens, spending the most resources on preventing an incident from occurring. One reason for this could be that the industry has yet to experience larger cybersecurity incidents. Furthermore, areas that should be considered a focus for the two groups moving forward were identified. These are increased focus on responsibility and role distribution, cooperation, and more training, exercising and awareness. Lastly, the need to define a clear definition of a cybersecurity.

We also want to explore if industries from other critical infrastructure have faced the same challenges and whether the oil and gas industry can learn from their experiences. The same methods will be used to gain insight from two different sectors, one company from the energy sector and one in the transport domain. A centralized environment for IT and OT is highlighted as a possible approach for better cooperation. These interviews show that the challenges they address are similar to those from the oil and gas industry. Therefore, sharing knowledge and experiences across industries should be considered.

Sammendrag

Industrielle kontrollsystemer inkorporerer informasjonsteknologi (IT) komponenter, som åpner opp for muligheter for fjernstyring, avansert dataanalyse og mer. Med økt konnektivitet følger risikoen for at sikkerhet kan kompromitteres av en cybersikkerhetshendelse. Denne oppgaven vil fokusere på nåværende rutiner for hendelseshåntering av cybersikkerhetshendelser for to grupper innenfor oljeselskaper, IT og operasjonsteknologi (OT). Ved å analysere hvordan de håndterer cybersikkerhetshendelser i dag er målet å identifisere områder hvor de to gruppene burde samarbeide for å møte fremtidens trusler.

For å adressere dette, vil vi først gjennomføre et litteraturstudie, for å få forståelse for industrien og forberede en intervjuguide til intervjuene med relevante aktører. Semi-strukturerte intervjuer vil brukes som metode for å samle inn data, og ansatte fra både IT og OT fra flere norske oljeselskaper skal intervjues. Resultatene fra intervjuene viser at industrien har et høyt fokus på perioden før en hendelse skjer, og bruker mest ressurser for å forhindre en hendelse. En grunn til dette kan være at bransjen ikke har opplevd større cybersikkerhetshendelser. Videre ble det identifisert fire områder de to gruppene kan vurdere å fokusere på fremover. Disse er økt fokus på roller og ansvarsfordeling, samarbeid og mer trening, øvelse og cyber bevissthet, i tillegg til en felles definisjon for hva en cybersikkerhetshendelse er for noe.

Vi vil også utforske om andre industrier innenfor kritisk infrastruktur har møtt på de samme utfordringene som olje og gass, og om de kan utveksle erfaringer. De samme metodene vil bli brukt for å få innsyn hos to forskjellige sektorer, et selskap fra transportsektoren og et fra energisektoren. Et sentralisert miljø for både IT og OT blir trukket frem som en mulig tilnærming for økt samarbeid. Disse intervjuene viser at utfordringene ligner for alle selskapene fra de ulike industriene. Derfor burde muligheten for å dele kunnskap og erfaringer på tvers av industrier vurderes.

Preface and Acknowledgements

This thesis is the final requirement for our MSC in Communication Technology at Norwegian University of Science and Technology (NTNU). The research was mainly carried out between January 2020 and June 2020, based on work done in a pre-project delivered the fall before.

A big thanks must be given to our three supervisors: Maria Bartnes, Lars Bodsberg, and Roy Thomas Selbæk Myhre. Your ideas and support were vital for us and the thesis. And also, we want to thank all those of you that set aside time to be interviewed and participate in the study. We would not have been able to complete this thesis without you!

Finally, we would like to thank our family and friends for their support during this last year.

Thea Svenkerud Rydjord
Ingrid Sørdal Volden
Trondheim, June 2020

Contents

List of Figures

List of Tables

List of Acronyms

CERT Computer Emergency Response Team.

CISO Chief Information Security Officer.

CPS Cyber-Physical systems.

CSF Cybersecurity Framework.

CSIRT Computer Security Incident Response Team.

DNVGL-RP-G108 DNV GL Recommended Practice - Cyber security in the oil and gas industry based on IEC 62443.

DSB The Norwegian Directorate for Civil Protection.

HMI Human Machine Interface.

HSE Health, safety and environment.

IACS Industrial Automation and Control Systems.

ICS Industrial Control System.

ICT Information and Communications Technology.

IEC International Electrotechnical Commission.

IoT Internet of Things.

IP Internet Protocol.

ISAC Information Sharing and Analysis Centre.

ISBR Information Security Baseline Requirement.

ISO International Organization for Standardization.

IT Information Technology.

NCS Norwegian Continental Shelf.

NCSC National Cyber Security Centre.

NIST National Institute of Standards and Technology.

NorCERT Norwegian Computer Emergency Response Team.

NOROG104 Norwegian Oil and Gas 104 - Recommended guidelines on information security baseline requirements for process control, safety and support ICT systems.

NSM Nasjonal Sikkerhetsmyndighet.

NTNU Norwegian University of Science and Technology.

NUPI Norwegian Institute of International Affairs.

OT Operational Technology.

PSA Petroleumstilsynet (Petroleum Safety Autority Norway).

SCADA Supervisory Control And Data Acquisition.

SOC Security Operations Center.

Chapter 1
Introduction

The oil and gas industry is vital for the Norwegian economy, alone contributing to 16% of the total Norwegian GDP in 2018 [Pet19b]. So far, only about 47% of the estimated recoverable resources from the Norwegian shelf have been produced and sold [Pet19b], meaning the industry can continue to thrive for many decades to come.

Traditionally, Industrial Control System (ICS) or Operational Technology (OT) systems, were not designed with security in mind [KPCBH15]. But Information Technology (IT) components are now being incorporated into these systems [SFS11], increasing efficiency, but also making the systems more vulnerable to outside attacks [KPCBH15]. Equinor, a Norwegian oil and gas company, alone expected to invest between 1-2 billion NOK in new digital technologies toward 2020 [Equ17a]. The money would be invested to focus on the digitalization of work processes, advanced data analytics, robotics, and remote control [Equ17a]. In November 2017, Equinor opened Valemon, their first platform that is fully controlled from land [Equ17b]. For remote control to be possible, equipment on the platform and the systems on land must communicate. But with the incorporation of IT technology, such as the use of Internet Protocol (IP), new threats arise which need to be managed [AS19].

The petroleum industry has had an extreme focus on safety and security [Equ18]. For safety, a focus on protection is fundamental, particularly protection against technical failure accidents and/or accidents caused by human actions [BHD+18]. Security is defined by the International Electrotechnical Commission (IEC) 62443 standard to be the "prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation or inappropriate

access to confidential information in Industrial Automation and Control Systems (IACS)" [IEC09, p. 7]. Safety can now be compromised by an adversary that targets the systems, meaning the need for securing these systems is more significant than before [SFS11]. An adversary can, for instance, get access to the network and make unauthorized changes to physical equipment [FMG18]. The outcome of such events can be significant: loss of life, environmental damage, or damage to the production [FMG18]. In the worst case, all consequences can coincide.

To combat these new threats, IT employees and OT employees need to be able to handle cybersecurity incidents that affect both systems. However, these groups have traditionally had different priorities, where IT have focused on confidentiality and OT availability [IEC09]. As the systems are more incorporated, the need for cooperation between the two increases.

> While the industry has escaped a major operational catastrophe thus far, this good fortune may not last unless companies expand their cyber security programs. [Del17, p. 2]

1.1 Scope and Research Question

This paper aims to look into the cybersecurity incident management process. IEC 62443 defines cybersecurity as the following: "actions required to preclude unauthorized use of, denial of service to, modification to, disclosure of, loss of revenue form, or destruction of critical systems or information assets" [IEC09, p. 15]. The IEC 62443 standard does not define information security, but International Organization for Standardization (ISO) 27000 uses the following definition: "preservation of confidentiality, integrity and availability of information" [IEC18, p. 4]. In Chapter 2, the term information security is used if the source presented utilizes the expression. While we could lean on both expressions, we have decided only to make use of cybersecurity when presenting our results. Since the term is from a source targeted towards ICS and covers both intentional and unintentional incidents. Exceptions are made if our interview subjects themselves chooses to use the term information security.

Three research questions were formulated to narrow down the scope. These were developed during the pre-report [RV19], and have been subject to some changes for the master thesis. The research questions that will be addressed are the following:

RQ1: How is the current cybersecurity incident management process in industrial ICT systems?

RQ2: How can IT and OT work together to improve their cooperation for the future?

We will look into employees from IT and OT, and explore areas where the two sides have similarities and discrepancies. The goal is to highlight areas where the two sides could work together to better prepare for future cybersecurity incidents.

The challenges related to digitalization may be similar across industries. Other industries can have come further with digitalization than petroleum and might have more experience in the field. We have an opportunity to look at the incident response management of other industries and see if we can learn from their experiences.

RQ3: With a focus on IT and OT, what can the oil and gas industry learn about the cybersecurity incident management process from other critical infrastructures?

1.2 Limitations

Due to time constraints of 23 weeks, only a couple of companies could be included in the thesis. The number of companies interviewed is less than desired to create a recommendation that can be generalized for the entire industry, meaning the conclusion is perhaps not as comprehensive as it could be.

The primary method of collecting data in this thesis was through interviews. A limitation will, therefore, be the interviewers. We have limited experience in conducting interviews, and the lack of practice may affect the interviews and the interpretation of the answers afterward. The limitations of using interviews as a method and of the corresponding results are further described in Section 5.4.

1.3 Contributions

This thesis contributes with an insight into the current cybersecurity incident management process of the oil and gas industry, as well as for two other industries.

By mapping the current cybersecurity management process for IT and OT in oil and gas companies, four main areas are identified as areas where the two groups should focus on moving forward. Especially should the industry set aside time and resources needed for training and exercising.

Challenges and experiences shared by two companies from other critical infrastructures are similar to those shared by the oil and gas industry. This shows that one should share experiences, not just within an industry, but also across the lines of critical infrastructures.

1.4 Outline

This section gives an overview of how the thesis is structured.

Chapter 1 - Introduction: this chapter presents the motivations, objectives, research question, scope, contributions, and limitations.

Chapter 2 - Background: the information needed for the thesis is presented.

Chapter 3 - Methodology: describes the chosen research methods.

Chapter 4 - Results: presents the findings from the conducted interviews.

Chapter 5 - Discussion: this chapter includes the discussion of results for each research question, followed by a discussion around the limitations of the thesis.

Chapter 6 - Conclusion: presents the conclusion.

Chapter 2
Background and Related Work

This chapter presents relevant background material to gain an understanding of cybersecurity incident management and IT and OT in the Norwegian oil and gas industry. In 2.1, relevant standards, frameworks, and guidelines will be introduced and compared to give insight into the incident management process. Further, training and exercise with relevant definitions will be presented in section 2.2. Then, in 2.3, the dependencies between ICSs and IT systems are explained. Lastly, the industry's threat picture and previous attacks are presented in 2.4.

2.1 Standards and Guidelines

2.1.1 Incident Management

The term incident management describes all activities performed when managing information security incidents [IEC18], with activities covering the time before, during, and after an incident occurs [IEC16a]. The main goal of an incident management strategy for many organizations is to prevent or contain the impact of information security incidents such that the direct and indirect injuries to their operations generated by the incident are minimized [IEC16a].

ISO/IEC 27000 defines an information security event and incident in the following way [IEC18, p. 4]:

> **Information security event**: identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.

> **Information security incident**: single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

2.1.2 ISO/IEC 27035

ISO/IEC 27035 introduces an approach for managing information security incidents [IEC16a]. By using ISO/IEC 27035 as a foundation, the organization can develop a strong information security program. The standard is split into two parts. The first, ISO/IEC 27035-1, presents five phases of information security management, basic concepts, and how to improve incident management [IEC16a]. The second, ISO/IEC 27035-2, covers two of the phases of ISO/IEC 27035-1, namely plan and prepare and lessons learned [IEC16b]. It gives guidance on how to plan and prepare for incident response [IEC16b].

2.1.3 IEC 62443

DNV GL has released a report, DNV GL Recommended Practice - Cyber security in the oil and gas industry based on IEC 62443 (DNVGL-RP-G108), that takes the IEC 62443 standard, a global standard targeted towards security in IACS [IEC09], and tailors it to the oil and gas industry [AS17]. IACS, in IEC 62443, includes control systems that are commonly used by organizations that operate in critical infrastructure, which includes the petroleum production and distribution facility [IEC09]. While the standard focuses on *what* to do, the DNV GL report includes recommended practices of *how* to implement the standard [AS17]. Activities described in the next sections are taken from DNVGL-RP-G108, as this thesis has a focus on the oil and gas industry.

DNV GL states, in section 6.5 of the report, that one should have an incident response life-cycle including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities [AS17]. This life-cycle covers the same activities as the phases from ISO/IEC 27035. Requirements for the incident response handling can be found in IEC 62443-2-4 [AS17].

2.1.4 Five Phases of Incident Management

In this thesis, we will use the five phases from ISO/IEC 27035 as a foundation for mapping the timeline before, during, and after an incident. The five phases as

defined in ISO/IEC 27035 are described below, along with similar activities from IEC 62443, if found relevant.

Phase 1 - Planning and Preparing

Planning and preparing for an incident is essential for an effective information security incident management plan to be put into operation [IEC16a]. A plan is valuable as it can document activities and procedures that will help handling information security incidents and communicating them properly [IEC16b]. As a result of fulfilling the activities of phase 1, one should be prepared for and be able to manage an information security incident [IEC16a].

ISO/IEC 27035 [IEC16a]: Activities mentioned in ISO/IEC 27035 are, for instance, to formulate and produce an information security incident management policy and get the top management in the organization to commit to the policy. Other measures that can be taken is to develop an awareness training program and establish and preserve relationships both externally and internally that are involved in information security events.

IEC 62443 [IEC09, AS17]: DNV GL writes that to ensure effective cybersecurity, one must have a clear understanding of the roles and responsibilities [AS17]. It also highlights that while cybersecurity has not been a priority in the project's phase historically, the asset owner or operator should have a cybersecurity management system in place before initiating an oilfield project. The report includes a table, taken from IEC 62443-3-2, describing which roles that should be included and which main activities these roles should perform. For instance, the asset owner should do a high-level risk assessment. Section 4 in the DNV GL report describes good practice for how to complete a security risk assessment.

Both IEC 62443 and DNV GL mentions training, awareness programs, and exercising as a recommended activity, but neither elaborates on how. Nevertheless, DNV GL does mention that one should use previous attacks, such as Stuxnet, and see if one is vulnerable to the same threats [AS17].

Phase 2 - Detecting and Reporting

The second phase is about detecting an incident, vulnerability, or other event and collecting relevant information and reporting occurrences by manual or automatic means [IEC16a].

ISO/IEC 27035 [IEC16a]: Key activities include monitoring and logging network activity and detecting and reporting the occurrence of an information security event or vulnerability. Events in this phase may not yet be classified as information security breaches but can be of interest nonetheless.

IEC 62443 [IEC09, AS17]: As IEC 62443 is more technical, it recommends ways of designing and building the systems to minimize the harm of an attack. For instance, IEC 62443 and DNV GL recommends segregating the systems to minimize the interaction between systems internally. This will also help increase the awareness of information flow and security differences between systems. Other measures are account management, so that users only have access to the services they need, and backup restore, to make sure that data is adequately backed up in case of loss or corruption of data. Also, multi-factor authentication should be used for remote access.

The final section in the report mentions detection and analysis as a part of incident response with activities as to quickly detect signs of an incident, understand the sources and prioritize and analyze incidents listed.

Phase 3 - Assessing and Deciding

The information collected in the previous phase will, in this phase, be used as a foundation for deciding on whether to classify an information security event as an incident or not [IEC16a].

ISO/IEC 27035 [IEC16a]: If an information security event is detected, certain activities should be performed during phase 3 or 4. These activities include: distribute responsibilities internally between employees, provide formal procedures for each of them to follow, and use guidelines for detailed documentation of events and actions that should be taken.

Specifically, in the third phase, key activities include collecting information about the detection of an information security event, carry out an assessment to confirm if the event might be an information security incident or a false alarm.

Phase 4 - Responses

The fourth phase includes responding to the information security incident, putting the activities decided upon in the last phase into action [IEC16a].

ISO/IEC 27035 [IEC16a]: For this phase, key activities include determining if the incident is under control and execute the response, assigning internal resources, identify external resources if needed, and ensure that all parties log all activities for later analysis. Further, a recommended activity is to inform other internal and external employees or organizations of the information security incident. The standard emphasizes that it can be beneficial for other organizations if the information is shared as others can be affected by the same threats and attacks.

IEC 62443 [IEC09, AS17]: Activities mentioned are to isolate affected environments, stop ongoing activities, and restore systems to the original state. Asset owners should have procedures in place for responding so that incidents do not compromise operations and safety.

Phase 5 - Lessons Learned

After the information security incident has been resolved, the goal is to learn from how the incident was handled [IEC16a].

ISO/IEC 27035 [IEC16a]: Activities such as to identify lessons learned, review, identify, and make appropriate improvements to organizations' existing risk assessments are recommended. Further, it is mentioned that organizations should communicate and share the result within a trusted community that can be both external and internal to the organization. More details about the activities for this phase can be found in ISO/IEC 27035-2 [IEC16b].

There should be made regular improvements to the elements of information security as the information security incident management activities are iterative.

IEC 62443 [IEC09, AS17]: It is specified that production and IT should have a greater focus on cooperation and bringing their knowledge together. Finally, the importance of learning and reporting is highlighted in the section about incident response.

2.1.5 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a guide for how organizations can align and prioritize their cybersecurity activities with its business requirements, risk tolerance, and resources [Mus14]. The framework provides a flexible way of addressing cybersecurity, and can be

applied to organizations within the IT, ICS, Cyber-Physical systems (CPS) or Internet of Things (IoT) domain. It needs to be individually tailored, as each organization will have unique risks, but the end goal is to reduce and better manage cybersecurity risk [Mus14].

The framework consists of three parts: the Core, Implementation Tiers, and Profiles. Implementation Tiers is a range of four tiers with different sophistication, in regards to incident handling, for each level [Mus14]. The Framework Profiles consists of two profiles, the current profile and the target profile [Mus14]. For the organization to get from the current to the target profile, a gap must be filled, which can be made possible by utilizing the Framework Core [Mus14]. The Core is a set of activities, desired outcomes, and applicable references that are usually common between critical infrastructures [Mus14]. How to implement, and which parts of the framework to utilize, are up the organization [Mus14].

The Framework Core is divided into five functions: Identify, Protect, Detect, Respond and Recover, as seen in figure 2.1. They are defined in the CSF as follows [Mus14, p. 7–8]:

> **Identify** - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.
>
> **Protect** - Develop and implement appropriate safeguards to ensure delivery of critical services.
>
> **Detect** - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
>
> **Respond** - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
>
> **Recover** - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

In each function, there is a set of key categories and subcategories. These activities have many similarities with the activities described in each phase of the ISO/IEC 27035 standard. Both the standard and the NIST Framework cover the time before, during, and after an incident. For instance, in the Identify Function, a subcategory is to establish and communicate an organizational cybersecurity

policy. This is also mentioned as a key activity in the first ISO/IEC 27035 phase, namely Plan and Prepare. While the phases do not perfectly align, much of the essence stays the same about handling an event.

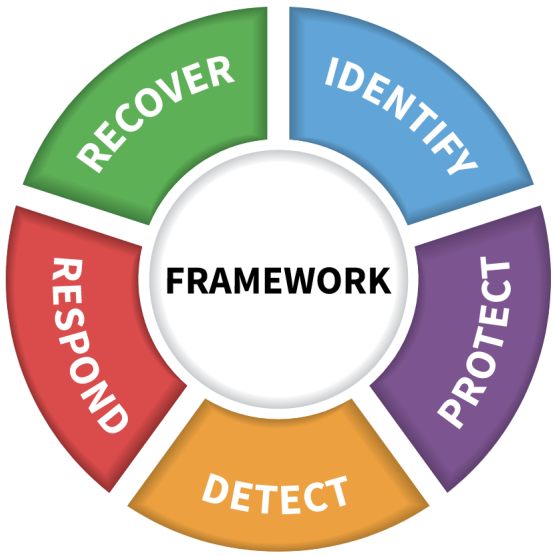


Figure 2.1: NIST Cybersecurity Framework Core. Image taken from [NIS19].

Appendix A, in the NIST CSF, contains a complete list over the recommended activities along with a reference to relevant standards and guidelines, such as ISO/IEC 27001 and IEC 62443.

2.1.6 Norwegian Oil and Gas 104

Norwegian Oil and Gas 104 - Recommended guidelines on information security baseline requirements for process control, safety and support ICT systems (NOROG104) has the goal of increasing the focus on information security in the offshore industry [OA07]. As a result, the safety and consistency of operations on the Norwegian Continental Shelf (NCS) should be enhanced. The guideline consists of a number of Information Security Baseline Requirements (ISBRs) that should be implemented [OA07]. Each ISBR is defined by a control and an

objective, and it is supported by an implementation guidance that is structured equivalently to the different phases of the NIST CSF [OA07].

2.2 Training and Exercising

> Training and exercises help to train the company's emergency preparedness force and contribute to develop skills, competence, risk understanding, and a good safety culture [AS20b, p. 1].

DNV GL, on behalf of Petroleumstilsynet (Petroleum Safety Autority Norway) (PSA), has written a report regarding training and exercise for the industrial Information and Communications Technology (ICT) systems on the NCS [AS20b]. In the report, they have given the terms separate definitions since these are often used interchangeably in Norwegian [AS20b]. The definitions are as follows [AS20b, p. 2]:

> **Training**: Increasing individuals' knowledge, competence and skills which are necessary to fill their given roles in the organization, and for handling an incident/event.
>
> **Exercise**: Developing an organization's ability to handle an incident/event and to reveal whether the current procedures and plans are suitable for the given purpose.

Figure 2.2 shows the sequence of exercises a company can carry out. The commitment needed to plan for an exercise, as well as the training time, increases with the increase in the level of capability [FEMnd].

Exercise
In ISO/IEC 27035-2 it is recommended to test the information security incident management plan through exercises [IEC16b]. Exercising can be of value to validate the incident response plan and procedures, clarify responsibilities, develop a good understanding of roles, and testing and further develop systems, functions, and competence [AS20b]. Activities of an exercise are to define the scope of it and conduct the actual exercise [AS20b]. Further, DNV GL states that follow-up activities such as evaluation of the execution and the suitability of current procedures and contingency plans also are part of an exercise [AS20b].

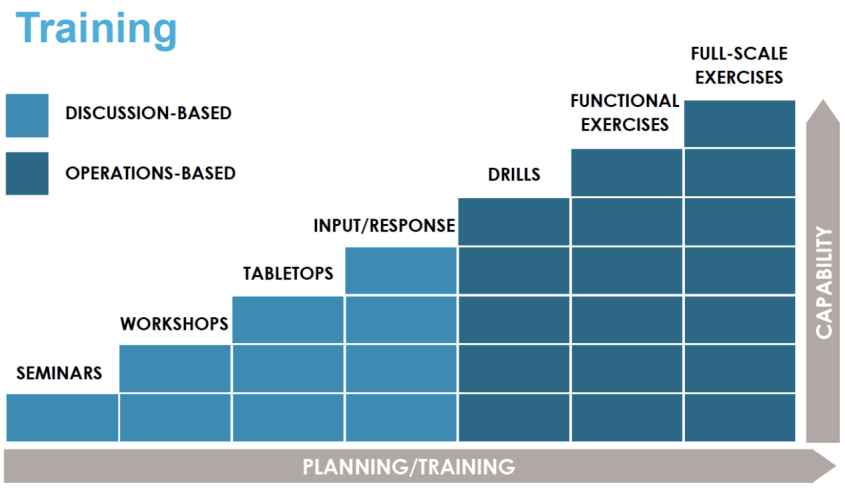


Figure 2.2: Overview of different training and exercises, and their level of difficulty. Image taken from [FEMnd].

An exercise form must be decided upon before it can be further planned. The Norwegian Directorate for Civil Protection (DSB)[1] separates between functional, discussion, game and full-scale exercises [fCP16]. All definitions given and explained below are based on the ones from DSB [fCP16]:

A functional exercise tests an actor's functions. Possible goals can be to test alert plans, such as an emergency response plan, and systems, or the decision-making process within and outside of the organization. A functional exercise is often carried out in a few hours but can take up to a day. They require little time for planning, execution, and evaluation, and can be a good supplement to full-scale or game exercises.

Discussion exercise or a tabletop consists of participants gathering in a shared room were a problem, based on a scenario, is discussed. The discussion of possible ways to handle or solve a scenario in real life, and all other communication during the exercise is to take place in this room. A tabletop can be exploited to test participants coping abilities, prepare for future exercises, or identify possible varying understanding and use of plans. It will typically last from a couple of

[1] https://www.dsb.no/menyartikler/om-dsb/about-dsb/

hours to a maximum of a day. It is recommended by DSB to inform participants beforehand of an exercise to give them time to prepare for it.

A game exercise consists of the trained players and a counterplay. The counterplay operates as the functions or roles that the trained players will only have contact with during the exercise. A game exercise should be handled as if it was a real incident, but no actions are to be taken outside of the game. The exercise scenario can be informed of in advance.

A full-scale exercise consists of trained players, a counterplay, and functions performing a practical job. It is often used when other organizations are invited to participate, such as the police or PSA. These exercises are always carried out in real-time with the regular work equipment and methods. A full-scale is experienced as closer to an actual incident and can be more instructive to the participants as they are tested in situations where they feel pressured in a realistic manner.

All exercises must either be informed of or be kept hidden from the participants in advance and what one chooses will affect the outcomes an exercise can have. ISO/IEC 27035 recommends that all involved parties are informed of that an exercise will take place and that it is not a real incident [IEC16a]. Information is provided to employees to prevent them from triggering actions that can have significant consequences. DNV GL, on the other hand, recommends using red team exercises where personnel is not informed of them beforehand [AS20b]. Such exercises can test how emergency response plans and the organization operates during them [AS20b].

2.3 Operational Technology Influenced by Information Technology

ICSs were traditionally closed-off systems, and as one needed physical access to come near the controls, security was not in focus [KPCBH15]. An ICS typically consists of a combination of components acting together, either fully automated or with human interference through a Human Machine Interface (HMI) to achieve an industrial purpose [SFS11]. Critical infrastructures such as the power grid, water and wastewater, transportation and oil and gas all typically include ICS processes and the infrastructures are often highly interconnected and dependent

on each other [SFS11]. Oil and gas is also an infrastructure with geographically dispersed assets, distributed over an extremely large area [SFS11].

To increase efficiency and reduce the cost, IT components are being incorporated into ICS-systems [SFS11]. This enables the OT systems to be remotely controlled and supervised, but it makes the system more vulnerable to attacks from the outside world [KPCBH15]. The need for securing these systems is greater than before, as safety now can be compromised by an adversary attacking the system [SFS11]. Special precautions must be taken when applying IT solutions for security issues, in the OT environment [SFS11]. Legacy systems, such as many ICSs, have a life span of 10 to 15 years, significantly longer than IT components [SFS11]. Older components were designed at a time when there was no focus on security [AS20a], and may not have the resources to utilize newer security controls, such as cryptography [SFS11]. Security needs to be addressed throughout the whole lifespan of the ICS, and the strategy "defense-in-depth" should be followed, meaning that the security mechanism should be layered [SFS11].

The corporate network should be separated from the ICS network, as segregation is one of the most effective ways an organization can protect its ICSs [SFS11]. The intended use of these two networks is different [SFS11]. While services such as email are allowed on the corporate network, this should not be permitted in the ICS network [SFS11]. However, due to practical considerations, a connection between the two networks is required, which represents a security risk that should be protected [SFS11]. Figure 2.3 shows a possible way of separating the two networks. With a properly configured firewall, the chance of a successful external attack on the control network is significantly reduced [SFS11]. The ICS network can then be segregated into multiple smaller networks, to minimize the access to sensitive information for the people and systems who do not need it [SFS11]. In oil and gas, each facility could have its own ICS network, and then further segregate it internally. This would mean that a cyberattack on one facility, not necessarily affects other facilities [AS17]. Additional security controls that should be implemented are whitelisting, granting access to only known good, network traffic filtering, and the principle of "need-to-know" that limit users' access to systems and data to the minimal amount needed [SFS11].

Traditionally, the focus for OT has been on safety related to, for instance, component failure, but with ICS being cyber-physical systems, an adversary can now compromise safety on a facility [KPCBH15]. Lisova et al. [LSC19] carried out a

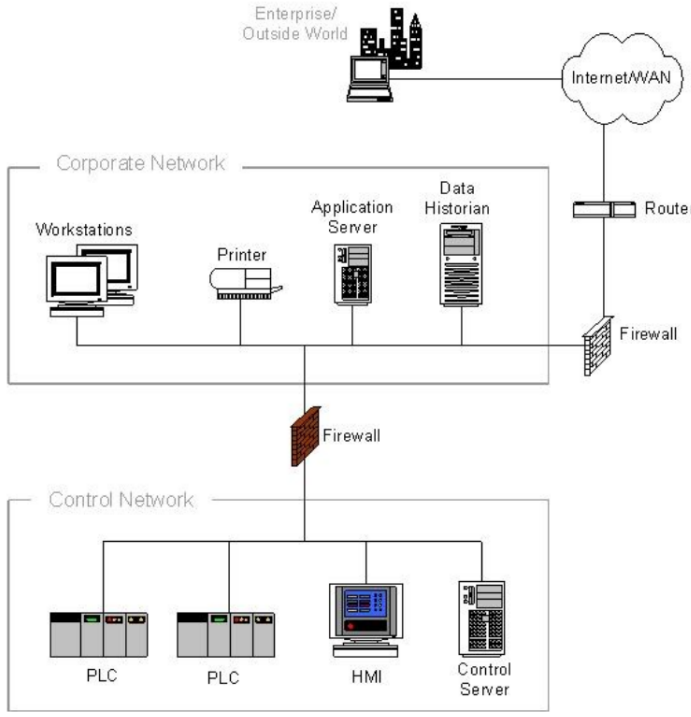


Figure 2.3: Firewall between the corporate and the control network. Image taken from [SFS11].

literature review about how to unite security and safety in system development. As security and safety both can influence each other, one needs to analyze their interdependence. The article does not find a preferred solution, concluding that there is a need for more research into the domain.

> In summary, the operational risk and difference between ICS and IT create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with

> control system operation. IT professionals working with ICS need to understand the reliability impacts of information security technologies before deployment. [SFS11, p. 2-18]

2.4 Threat Picture

The expanded adaptation of digital solutions has led to an increase in the number of cyberattacks [FMG18]. There are several benefits associated with the development of increased use of technologies, such as lower costs, more cooperation, and higher efficiency [FMG18]. However, according to the American company Leidos, the extended use of modern technology has had a negative impact [Lei16]. The usage is leading to new vulnerabilities [Lei16]. The different groups of adversaries can be separated into internal actors, competitors, and external parties [Del17]. According to the Norwegian Government, foreign states are presumably interested in acquiring harmful knowledge about the nation by exploiting ICT-security, which can have significant financial consequences or harm critical infrastructures [oB17]. Countries highlighted as having an interest in attacking and that have carried out the most cyberattacks against Norway's digital systems are China and Russia [FMG18].

The Norwegian Oil and Gas Industry

Critical infrastructures have a vulnerable position in the market as the consequences of an intrusion can be fatal [FMG18]. The Norwegian oil and gas industry was under a cyberattack as early as 2014 [FMG18]. Norwegian Institute of International Affairs (NUPI)s report informs that more than 50 energy and oil companies were influenced by the attack, the primary aim of the attack being the most significant Norwegian oil company, Equinor [FMG18]. In a report published by Dragos in August 2019, they state that the oil and gas industry is mainly exposed and targeted by adversaries due to the use of ICSs [Dra19]. The reasoning for the victimization is the impact the industry has on the economy and politics [Dra19]. Moreover, the number of attacks against ICSs are ever-increasing. Dragos argues that the target of the first major cyber event will be in the oil and gas industry. Both losses of life and equipment damage are mentioned as possible consequences of such an event. Dragos highlights the need for collaboration across private and public companies, the government, and regulatory organizations to increase the safety and security of such systems, reducing the risk of harm [Dra19].

Cooperation

A lack of cooperation within the industry can result in longer reaction times, that more cyberattacks are completed, and significant losses such as human life [FMG18]. The collaboration can be solved in multiple ways and is the focus of a report regarding ICT-security in the petroleum industry conducted by SINTEF [BHD+18]. SINTEF argues that it can be achieved through membership in a Computer Emergency Response Team (CERT). One crucial benefit of gathering companies in a CERT is that information sharing is not voluntary, but mandatory [BHD+18]. Norwegian Computer Emergency Response Team (NorCERT) is a point of contact for reporting of cyber incidents on a national level [NSM19]. Moreover, it monitors members and informs them of events connected to them and others. NorCERT is managed by Nasjonal Sikkerhetsmyndighet (NSM), which is the point of contact for reporting cyber events for Norwegian companies [NSM19]. They are responsible for discovering, handling, and coordination of ICT activities [NSM19].

SINTEF has established that there is no need for a specialized oil CERT at the sectoral level, as Norway has limited ICT security knowledge [BHD+18]. Therefore it is recommended to gather experts from different industries in one joint sector CERT. Oil and gas companies are advised to become participants of KraftCERT[2], which has existed since 2014 [BHD+18]. This specialized CERT was established for the power industry, with the responsibility of supporting the preventive work and incident management of ICT-security attacks [BHD+18]. Another solution, which SINTEF highlights in their report as more desired by companies, is to introduce membership in Information Sharing and Analysis Centres (ISACs) [BHD+18]. ISACs are different meeting areas and forums organized by external actors [BHD+18]. SINTEF does not recommend that oil companies only establish an oil ISAC to improve information sharing within the industry. Instead, the ISAC should strengthen KraftCERT as a means of collaboration on the basis that the energy infrastructure in itself is highly interconnected [BHD+18]. It is worth noting that some companies have internal organizations and CERTs for the management of incidents [BHD+18].

[2]https://www.kraftcert.no/english/om.html

Former Attacks

Several attacks against critical infrastructures have taken place both within and outside the Norwegian borders.

Stuxnet was a foreign cyberattack that occurred in 2010, where the malware was introduced in an Iranian nuclear facility by the use of a USB stick [McA]. As explained by McAfee, the virus spread over Microsoft Windows computers and sent damage-causing instructions to equipment controlled by the machines. As a consequence, centrifuges were injured and burnt out, which lead to an interruption in the production and financial losses [McA]. The attackers were able to send false feedback to the controller, and therefore the attack was not detected before the damage had already been done [McA]. It is believed that Stuxnet could have been a result of disagreements and conflicts between nations, in this case being Iran, and Israel and the US [McA].

The ransomware attack Petya of 2017 was able to take down critical infrastructures in a matter of a few hours. The attack, also known as NotPetya, infected a significant amount of organizations in numerous countries [McAte]. NorSIS informs that ransomware made content on computers unavailable and required a ransom to give employees access [sfi19]. The virus spread via phishing and spam emails from Windows servers and computers to non-vulnerable machines [sfi19].

After a cyberattack took down an electronic distribution system, it was concluded that there is a more significant need for information sharing, explains E-ISAC [RML16]. A Ukrainian Supervisory Control And Data Acquisition (SCADA) system was attacked on December 23 in 2015, which led to a power outage to approximately 225 000 customers [RML16]. According to E-ISAC, this was the first publicly acknowledged occasion a cyberattack has caused a power outage. The blackout affected three different areas of Ukraine and lasted for multiple hours [RML16]. E-ISAC argues that the incident had low impacts, and that the attack was believed to be a test of the malware, based on the time and area of attack [RML16]. The power went out for a few hours during the night [RML16]. Had the event taken place during the day, the consequences could have been more severe. The authors of the white paper recommend information sharing to build more awareness within sectors, which can make it possible to detect attacks earlier [RML16].

Even though there has been an increased focus on security in ICS, Norwegian

Hydro has recently been attacked. In March 2019, the aluminum manufacturer was hit by ransomware [Hyd19]. LockerGoga, as the malware was named, took down parts of the production and the company's website [sfi19]. The amount of lost revenue is assumed to be between NOK 300 to 350 million in the first quarter and NOK 250 to 300 million in the second quarter [AS20b]. It was found praiseworthy by NorSIS that Hydro went out publicly with information about the attack they experienced [sfi19]. NorSIS further emphasizes that such sharing creates an attention around the issue and vulnerabilities and can lead to other companies being able to evaluate their security level and take actions to secure themselves. Such that similar incidents are prevented from occurring.

Summary

Oil and gas companies face several challenges in the fight against cyberattacks. The most pressing problems are assumed to be, for instance, weak information exchange between public and private sector, unclear roles in the companies, varying expectations regarding security standards and supervision, and limited capacity and resources, according to NUPI [FMG18]. If companies are to be in a better position to guard themselves against cyber threats, these challenges should be considered addressed.

Chapter 3
Methodology

This chapter presents the research methodologies utilized in the thesis. Section 3.1 explains the research question and design. We have followed the case study method, which is explained in 3.2. Our main method of collecting data has been through semi-structured interviews, found in section 3.3. How we have processed and analyzed the collected data is then further described in section 3.4. Finally, an evaluation of the study's generalizability, validity and reliability are presented in 3.5 followed by a final section about ethics, 3.6.

3.1 Research Questions and Design

This thesis originates from a pre-project conducted from September to December 2019. The goal of the pre-project was to find an area of focus for the master thesis, which led to identifying a research topic, defining research questions, and narrowing the scope of the thesis. The main focus became the cybersecurity incident response management in the oil and gas industry.

3.1.1 Research Questions

The research questions from the pre-project were slightly altered to fit the study better. A research project's purpose is often either to describe, explore, explain, or reflect [Rob11]. The research questions should be clearly stated, be answerable, and show the purpose of the project [Rob11]. We have chosen to lean on the explanation presented by Blaikie, cited in Real World Research, suggesting the use of "what", "how", "why" [Rob11]. He explains that a question shaped around how expresses an interest in change. Two research questions of this thesis are aimed at exploring the current status of incident management in the oil and gas

industry. For the last question, we want to investigate if the industry can learn anything from other industries.

This leads to the first two research questions:

RQ1: How is the current cyber security incident management process in industrial ICT systems?

RQ2: How can IT and OT work together to improve their cooperation for the future?

The goal of the first question is to identify which standards, frameworks, and processes oil companies use to get a better picture of how the oil and gas industry handles incidents today. This information is necessary to be able to answer the second question, where the goal is to find areas where IT and OT may want to increase their cooperation in the future.

"What" requires a descriptive answer, which is of interest for the comparison for the last question [Rob11]. With the third question, we wanted to explore the following:

RQ3: With a focus on IT and OT, what can the oil and gas industry learn about the cybersecurity incident management process from other critical infrastructures?

The challenges faced by IT and OT in oil and gas can be similar to challenges that other industries have faced. By interviewing employees from other industries, the goal is to explore if any of the lessons they have learned can be transferred to the oil and gas industry.

3.1.2 Research Design

The choice of research design limits every study, where common choices are quantitative research, qualitative research, and mixed-method research [Rob11]. Quantitative research is often associated with measurement, quantification, a focus on behavior, and reliability [Rob11]. In contrast, qualitative focus on, for instance, findings presented verbally, little numerical data, a focus on meanings, little objectivity, and small-scale [Rob11]. Mixed-method research is a combination of the mentioned research types [Rob11].

> A research design is a logical plan for getting from here to there, where here may be defined as the initial set of questions to be answered, and there is some set of conclusions (answers) about these questions. [Yin09, p. 26]

Qualitative research is often a good approach for research based on people's opinions and feelings concerning a topic. Exploiting qualitative research by performing interviews with relevant actors, was selected to be an excellent option to collect relevant data for this study. Furthermore, case studies can be a suitable research method when one wants to study a group or an individual [Rob11], and we had a clear, defined group of interest. Therefore, our final plan for the thesis was to follow the case study strategy and gather qualitative data through semi-structured interviews.

3.2 Case Study

In *Real World Research*, Robson states that case study is a well-established research strategy where the focus is on a situation, for instance, a study of a group [Rob11]. The strategy can involve multiple methods of data collection, where qualitative data are almost invariably collected [Rob11]. The book also mentions studies of events, roles and relationships, and studies of organizations and institutions as possible types of case studies.

> Case study is a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence. [Rob11, p. 136]

Based on theories from [Yin09] and [Rob11], case study was chosen as a suitable research method. We wanted to study employees and their experiences. Our main method of collecting data would be through interviews and a literature review. Interviews were chosen above surveys, as these can give more in-debt information from our subjects through a greater amount of open-ended questions. Our goal was to build theories from the collected data, called inductive research [Oat05].

Figure 3.1 shows the case study research process, which is divided into six phases. During the first phase, Plan, one decides upon the research questions and

determines if one should use the case study method [Yin09]. The phase, therefore, includes the work conducted in our pre-project and the beginning of the thesis work. Initially, in our pre-project, we were not going to use case study. But as the Plan phase continued at the beginning of the thesis, and we were introduced to this by our supervisor, we decided to use this method.

The second phase, Design, is about defining the cases to be studied and developing theory, propositions, and issues underlying the anticipated study [Yin09]. Our research questions can each be seen as two cases, meaning we have a multi-case study. Furthermore, all cases will include several units, meaning each case is an embedded single-case, according to Yin.

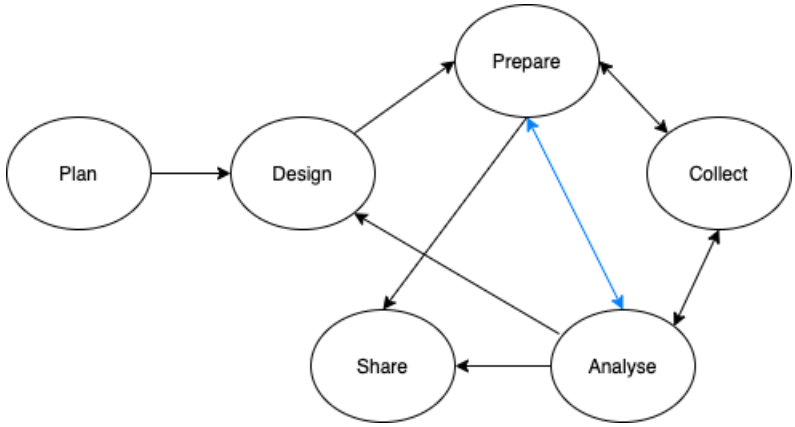


Figure 3.1: Our case study research process. Image inspired by [Yin09].

Prepare is the next phase, which includes getting familiar with the case study method and preparing for the later phases for our cases. The preparation we did for the interviews are included in this phase and is further explained in 3.3.

In the Collect phase, we used both interviews and literature review as our primary sources for collecting data. When all the necessary data have been collected, the phase is followed by two more phases: Analyze and Share. The Analyze phase is further described in 3.4. Lastly, the Share phase was about finalizing this report.

We have added an arrow from Analyze to Prepare, which in figure 3.1 is marked in blue, and is not included in the original figure [Yin09]. This is because we had several cases and gained experience with interviewing and new insight when

working with data from the first case. Our last interview belonged to our second case, where the planning of these interviews was affected by the Analyze phase of the first.

3.3 Semi-Structured Interviews

There are multiple types of interviews, three of them being structured, semi-structured, and unstructured [Rob11]. We chose to use semi-structured interviews as our main research method for collecting data. This type of interviewing is more flexible than the other ones [Rob11].

Semi-structured interviews require that an interview guide is prepared and finalized in advance [Rob11]. The interview guide contains topics to discuss and an ordered list of questions to be asked each subject [Rob11]. During a semi-structured interview, the order of questions from the interview guide can be rearranged and modified to suit each subject better and to achieve a sufficient flow [Rob11]. Follow-up questions can be asked if needed, which gives the opportunity of angling the conversation in a new direction if seen as fitted [Rob11].

In *Kvalitative Forskningsmetoder i Praksis* [Tjo17], Tjora writes that semi-structured interviews are a good method choice in cases where one wants to study the subjects' opinions and experiences. Oil companies might want to minimize the publics' knowledge about how they handle cybersecurity incidents and the weaknesses related to their processes. Therefore, it can be advantageous to angle questions to ask about what the subjects believe, rather than exclusively drawing out how companies operate and their weaknesses. The focus will be on the employees' own experiences and how the company handles situations today.

3.3.1 Interview Guide

An interview guide was essential to give the companies and employees an idea of what to expect and allowing them to prepare for the interview. Further, it was one way of ensuring that the same, desired data is collected from each participant and to give structure to the interviews. The guide was more or less divided into three phases based upon [Tjo17] and shown in figure 3.2.

The first phase, the warm-up phase, included an introduction of us and our thesis, and a couple of questions to warm-up the subject. Questions in this phase should be simple and concrete and are used to set the foundation for the rest of the

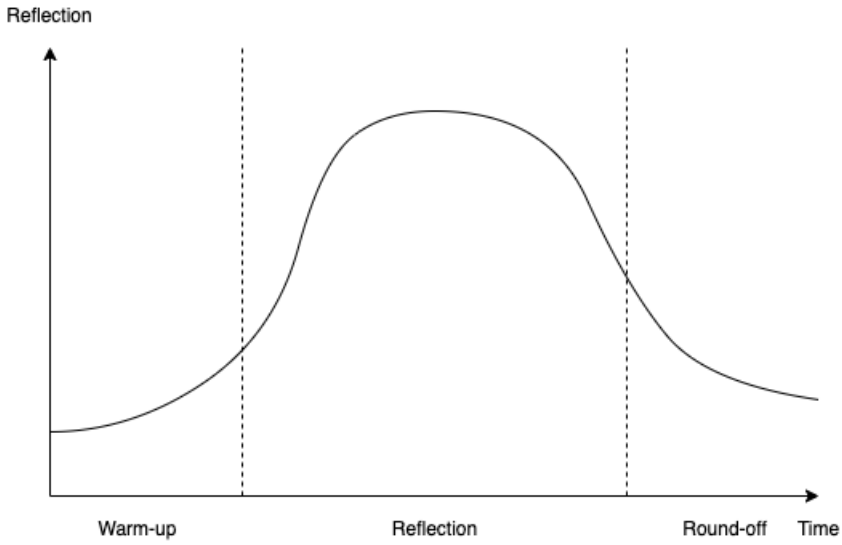


Figure 3.2: Phases of a semi-structured interview. Image taken from [Tjo17].

interview [Tjo17]. We asked questions about the size of the company and the subjects' daily work, before rounding the phase off with an open question about digitalization. This phase usually lasted a couple of minutes, depending on how many details the subject provided.

The main part of the interview belonged to the second phase, called reflection. The questions asked in this phase encourages the subject to reflect on how the company has handled cybersecurity incidents. If the subjects do not have any incidents to reflect on, more general questions about the topic were asked.

Finally, the third phase was used to ask some last, open-ended questions, before rounding off. We asked if the subject had any recommendations for others or otherwise wanted to share something. At the end, we thanked the subject for participating and explained that they would be allowed to read the thesis before publishing and asked if it was possible to send them some follow-up questions if needed. All subjects were willing to be contacted with follow-up questions later.

3.3.2 Planning

An essential part of the early stages of planning was to finalize the interview guide and find companies that could participate in the study. The number of companies should be sufficient to collect enough data, but it must also be limited to avoid the phase being too time-consuming. If the interviews required too much time, we would not be able to set aside enough time to conduct a thorough analysis.

As the main focus of this thesis was to look at differences between employees from the IT and OT side, we needed to get in touch with specific subjects from the companies. We initially wanted to interview workers responsible for the operation of a facility, such as a facility owner or operator. However, due to the Coronavirus, the interviews were pushed further back than planned. As our main priority was to cover the IT and OT side, a decision was made not to pursue interviews with these. Instead, we chose to stick with two subjects from each company.

The recruitment of interview subjects was conducted by utilizing the supervisors' network and participation in CDS-forum[1]. All possible interviewees were contacted through email correspondence. The email contained a description of the study and the positions of interest. If the contacted workers did not have the right knowledge, they were kindly asked to redirect the email to other relevant employees. It was expected that an informative email containing the interview guide would be enough to arouse interest. The respondents were asked to suggest a few time slots where they were available. Some were contacted during the period when the Coronavirus affected Norway. The virus led to most having to work from home, which can be disruptive. It was, therefore, essential for us to give the respondents space and let them answer us in their own time.

3.3.3 Respondents

To increase the diversity of this selection, companies of varying sizes were chosen in the hope of covering a larger part of the industry with our proposal. Size can be an important factor in how companies are organized and operate.

We ended up with five companies that wanted to participate from the oil and gas sector, and two companies from two different industries. They are all Norwegian. Each company has been grouped into small, medium and large based on the number of employees. A company is regarded as small if it contains up to 500

[1] https://www.sintef.no/projectweb/cds-forum/

employees. Companies of medium size have between 501 to 2000 workers, while large companies consist of more than 2000 employees.

From the oil companies, all but one company had both IT and OT employees that wanted to participate. Only OT replied from the last. We decided to include this subject, even though IT was not covered, as this interview would give us a bit more insight into the OT side.

Anonymization was recognized as a requirement for companies to participate. Therefore the oil and gas companies are not further divided. In the next chapters, the reader can notice that the companies have not been given a code name, but that we only refer to one or more companies. Differences between companies have been taken into consideration, and where the size or other factors of a company matters, it is stated.

The two companies from the other industries will be referred to as Industry A and Industry B.

Lastly, the subjects of the interviews are sometimes referred to as "he". This is only to decide upon a single pronoun to use for simplification and is independent of the sex of those who participated.

3.3.4 Implementation

We conducted a total of eleven interviews over several weeks. Each interview with the oil companies lasted approximately one hour, while the ones carried out with Industry A and Industry B lasted one and a half hours each. In advance of each interview, it was decided who was to take the lead and ask the questions. As neither of us has conducted interviews in this context before, we rehearsed by voicing the interview guide out loud. This made us more aware of how we formulated the different questions, and if the intention was clear.

Due to companies' locations, and later the restrictions because of the Coronavirus, all interviews were conducted through Skype and Microsoft Teams. At the time of the Coronavirus, we sat separately but worked together with executing the interviews. In these cases, we communicated to decide upon, for instance, follow-up questions.

After each interview, we set aside half an hour to write down our immediate

thoughts individually before discussing how the interview went. Based on this discussion, some changes could be made for the next interview. For instance, the wording of a question or the order of the questions. However, the version of the interview guide used to interview either OT or IT was also used for the corresponding group in the same company. More significant changes made were implemented for the next company that was to be interviewed. This was done to have the basis of comparison as similar as possible for the two groups in one company.

3.4 Data Analysis

> Unfortunately, qualitative data analysis is not always a straightforward task. There are no hard and fast rules about how to do it. [Oat05, p. 267]

This section describes how we structured and analyzed the data we collected during the interviews. The process is based on and inspired by the step-wise deductive, inductive method from Tjora [Tjo17]. In this approach, one works in several steps to get from raw data to theories or concepts. We have mainly followed the inductive (upward) process.

Figure 3.3 visualizes the process we followed, divided into four steps. These steps describe how we have processed the data to develop theories. Each step is represented by a square, with the outcome of each step represented with rounded corners. The result of one step is brought on to the next, meaning the input to step 4 is the output of all previous steps. Each step is conducted somewhat chronologically for each interview, with some steps in between. Since the interviews were conducted over several weeks, we were working on several steps simultaneously. We could transcribe one interview at the same time as we did analysis work on another. Some steps could affect others. When transcribing an interview, changes could be made in the interview guide, and when writing the discussion, the results in Chapter 4 were checked. These dependencies are shown with arrows in the figure.

Step 1 - Transcribing the Interviews
After each interview was conducted, we started transcribing as soon as possible to keep the experience fresh in memory. One would transcribe parts of, or the whole interview, while the other would listen to the taped recording and double-check

the transcription. When transcribing, we also got increased awareness of our role as interviewers. For instance, we became aware of the need to talk slower and to pause between an answer and the next question in some cases. We further noticed how a few questions were interpreted differently than intended.

Step 2 - Structuring the Data
After each interview was finished transcribed, we went through them and highlighted information of importance. We used several color codes for this: yellow, green, and blue are representing the time before, during, and after an incident, and pink, for other, general information. The IT and OT interviews from one company were then structured in a spreadsheet, where a summary of both sides' answers was written, along with a column for relevant quotes. This way, we had a smaller text-base to work with and could easily compare the two groups' answers within a company. Follow-up questions were either included in the answer to the original question or added as a standalone question.

Step 3 - Qualitative Analysis of the Data
We went through several ways of structuring and analyzing the data, before deciding upon a version of empirical coding [Tjo17]. Since the goal of this thesis is to compare the answers from IT and OT, we decided to use empirical coding to group together the questions from the interview guide and the follow-up questions, not the interviews themselves. We wanted to look at how the two groups answered differently to the same questions, and we believed that some of the differences could be lost if we just coded the interviews as a whole. Therefore, we coded the questions and each follow-up question into groups. The result was 16 different headlines. The data from the interviews, already structured in step 2, were then grouped under each headline and compared. The interview findings are presented in Chapter 4. For the interviews with Industry A and B, the summaries presented in Chapter 4 are structured based on theories developed as the data collected.

Step 4 - Categories for Discussion
This last task was about deciding upon a way of structuring the discussion in Chapter 5. Since we have used an inductive research approach, theories and observations were formed when working with the interviews [Oat05]. For the second and third research questions, focus areas were identified during the analysis of the collected data.

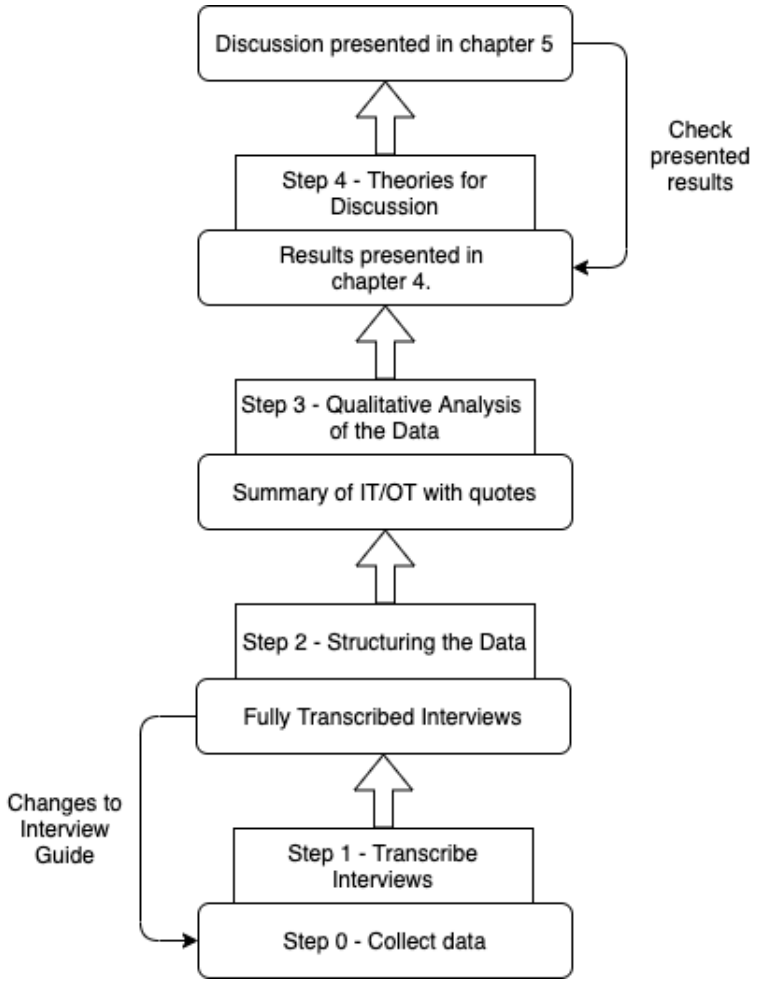


Figure 3.3: Diagram showing the steps of our data analysis process. Inspired by [Tjo17].

3.5 Trustworthiness of the Study

A study built on interviews and human interpretation requires a review and evaluation of the study's generalizability, validity, and reliability, which describes the trustworthiness of a study [Rob11].

3.5.1 Generalizability

> Generalizability refers to the extent to which the findings of the enquiry are more generally applicable outside the specifics of the situation studied [Rob11, p. 77].

To increase the study's generalizability, we wanted to include as many companies as we could manage within the boundaries of our study. Instead of making the study only applicable for the interviewed oil companies, the goal of our thesis was to provide recommendations that can be of use for the entire oil and gas sector, if not also other industries with similar structures. Therefore, achieving a generalizable study was of importance.

In a qualitative study, samples from the target group must be representative and large enough to ensure generalizability. Therefore companies of different sizes, measured in the number of employees, were chosen to participate in the study. We expected these to have different approaches to cybersecurity and would give a representative view of the industry and the proper data needed to generalize the study. Due to time constraints, we were only able to interview five companies from the oil and gas sector and two companies from different industries. As a result, our study is not fully generalizable, but as far as we could get with our available resources.

3.5.2 Reliability

For results to be reliable, they must be replicated and consistent over time, so that the same results can be obtained later [Rob11]. This can be difficult to test in qualitative research. To hopefully achieve reliability, Robson suggests the following:

> This involves not only being thorough, careful, and honest in carrying out the research, but also being able to show others that you have been [Rob11, p. 159].

Reliability can be obtained through an audit trail [Rob11]. All activities from field notes, transcribed interviews, data analysis, etc. were therefore recorded during the study.

Different interviewers will not receive the same answers from the same subject. Even if the questions are asked in the exact same way, it is not possible to ensure that the same answers will be given. A subject will usually make a connection with the interviewer during the process. How the relationship between the two is, can influence the answers given by the subject. The subject might share less with an interviewer, which they do not trust. The mindset of the subjects during the Corona period may also have affected the answers given. Therefore, it is unlikely that another interviewer can recreate our interviews and results.

The subjects' competence of their companies' may vary. All participants in the study were selected by the contacted employees, with the only requirement being that they worked with IT or OT. Therefore there was no way to ensure that the knowledge of the employees was similar. This affects to what extent different answers could be compared and how consistent they are. Comparing results that are not analogous requires an analysis that may not necessarily be replicable.

An essential part of a reliable study is to pursue neutrality. To achieve complete neutrality in a qualitative study is rather impossible, states Tjora [Tjo17]. Being open about the pre-understanding one has about the topic and explain how one's personal engagement can influence the work is necessary to demonstrate one's neutrality, clarifies Tjora. Our limited knowledge in the area of incident management in ICSs can be an indication of neutrality from our point of view. However, we cannot hide the fact that we had a desire to draw conclusions and publish a study of interest and value.

We have tried to clarify what are our personal thoughts and analysis, and what originates from existing literature. However, it can be difficult to treat all literature equally if one has an idea of which conclusions one wishes to draw. For instance, the search for relevant literature can be stopped when we find the data that supports our conclusion, instead of continuing the search and reading all relevant

literature, both that support and disagrees with our conclusion. Such behavior weakens the study and must, therefore, be prevented. Seeking data which is not consistent with our theory is desirable [Rob11]. To hopefully ensure that our recommendations are neutral, they are based on the companies' experiences and relevant literature in the field, both that support and disagrees with our thoughts.

3.5.3 Validity

> Validity is concerned with whether the findings are "really" about what they appear to be about [Rob11, p. 77].

Our minimal experience in conducting interviews can have affected the subjects and, therefore, the answers given. It is not just human relationships that influence what responses we receive. A lack of practice as an interviewer can harm the study. Asking leading questions and not giving a subject sufficient time to digest the question and come up with a deliberated answer are possible outcomes of little experience that can weaken the validity of the results.

Each interview was recorded and transcribed to ensure the accuracy of the data. Using a recorder allowed us to have our focus on the interview and to ask the appropriate questions, instead of having one of us write down the details. Errors may, however, have occurred in the transcribed interviews. Being able to hear differences between similar words in speech can be challenging, especially for the inexperienced.

To provide a valid interpretation of the collected data, it is required that the route leading to the interpretation should be able to trace back [Rob11]. Therefore our interpretations are based on existing research and literature. However, as stated in 3.5.2, the interviews can not be reproduced.

Subjects will be allowed to read through and give feedback on the first draft to assure the validity of the data [Rob11].

3.6 Ethics

Crucial consideration must be taken into account when a project is based on interviews and information gathering from individuals. First and foremost, research should not harm any participants involved [Rob11].

The project had to be approved by the Norwegian Centre for Research Data to secure that appropriate measures have been made to fulfill this. The application can be viewed in Appendix B, while the approval is shown in Appendix C. Each participant had to read through an information sheet, Appendix D, and sign the form it contained if they were willing to participate. The form specified what the study involves and how objects and companies would be made anonymous. If a participant wanted to withdraw their consent, one could send an email and have the participation deleted. Participants were also allowed to ask for the collection of data saved about them.

Chapter 4
Results

Previous chapters have presented relevant background for the thesis and our choice of methods for collecting data. This chapter presents our findings from the semi-structured interviews. Firstly, the results from the interviews with oil and gas companies are presented in 4.1. Then, the findings from interviewing two other industries are presented in 4.2.

Relevant quotes from the interviews are included, and highlighted with a blue background. As the interviews were conducted in Norwegian, each quote is translated from Norwegian to English. All quotes can be found in their original language in Appendix A, along with the complete interview guide in Appendix E.

4.1 Interview Findings - The Oil and Gas Industry

This section is divided into five parts that correspond to the five phases of the ISO/IEC 27035 standard, as described in Chapter 2. Each part is structured equivalently, by presenting answers from both the IT and OT side, to highlight how each group relates to the phases.

4.1.1 Planning and Preparing

Responsibilities:

Factors such as size, history, and resources seem to affect how roles are defined and distributed.

*"People may have different opinions! Even between me and *name* will there be different views about who is, who does what at what time." (1) - OT employee*

One medium-sized company has divided IT and OT into two completely different branches in their organizational structure. The IT employee from this company states that the daily cybersecurity responsibility is placed at the system owner. Furthermore, the subject explains that the operational responsibility for IT cybersecurity is placed with IT and OT cybersecurity at OT. This is confirmed by the OT subject that explains that they have a "IT role" in their OT department. This role is responsible for the IT infrastructure in operations, and cybersecurity on one platform. Other platforms are organized differently. It is pointed out that this is probably due to historical factors, and they have yet to decide upon a general model for role and responsibility distribution. The subject states that a system owner at a platform has less knowledge about cybersecurity than their dedicated IT role. A quote from his answer is included below.

> *"They sit with a lot less, if you compare to a system owner on a platform, for instance, on a control system, then he obviously has less cybersecurity expertise than *name* sitting with the equivalent on *platform*. They may sit with the budgets and the ability to influence, but they do have the right to degrade cybersecurity in relation to control system stuff, so there is an obvious dilemma here." (2)*

Several companies mention that the size of a cybersecurity incident dictates who should be the first point of contact.

One of the larger companies has placed the general information security responsibility at the CIO and his department. This department has the overall responsibility for cybersecurity in the entire organization. Each business area has a point of contact between the business areas and this department. The OT employee from this company describes how he is responsible for delivering cybersecurity from the OT side.

A smaller company has taken another approach for how roles and responsibilities are distributed, differentiating between accountability and responsibility for cybersecurity. The CEO is left with accountability, while the responsibility is placed elsewhere. The OT employee states that OT is left with the responsibility in the process control domain and IT for its domain. This is in contrast to the answers from the IT side, where the subject explained that he is responsible for information security, including ICT security for the whole company. Furthermore, he states that OT is somewhat segmented and that the company has contracts

with different third party suppliers. These are responsible for cybersecurity in the systems they deliver. Lastly, the employee highlights that all employees in the company are responsible for knowing the procedures and rules that the organization has established.

Some OT employees states, when describing their cybersecurity roles, that they are responsible for the OT side and nothing more. One OT employee explains how he has nothing to do with the office networks and applications, nor does he care about these systems.

"IT has the overall responsibility for this to come together, to have a complete picture within cyber. We are responsible for delivering the OT-part (...)" (3) - OT employee

Lastly, some of the companies have access to global resources. These companies explain that the overall responsibility lies on the global teams for cybersecurity and that they get regional demands they need to comply with.

Definition of Cybersecurity Incident:

How a cybersecurity incident is defined varies from company to company. Only one company has corresponding answers between their participating IT and OT employees, where both say that unintentional and intentional actions can be categorized as a cybersecurity incident. IT continues to say that the incident must have a negative impact and affect the company's ability to operate in a good way. At the same time, OT sticks to the definition from the quote below. Throughout the interview, the same OT employee mentions cases, such as a misconfigured server, and that these might not be categorized as incidents after all.

"That is any, either unintentional or intentional, incident that is not a part of the defined use of the system." (4)

The remaining companies answers differ between the IT and OT side. IT from two companies only includes intentional attacks, while OT from one of these mentions that unintentional incidents can also result in damage, and should, therefore, be covered by the definition. This company also categorizes incidents as states, where an undesirable state is a vulnerability of the system that has not yet been exploited. OT from the other company categorizes events as internal or external, as they have a lot of third party vendors.

An event needs to have a consequence to be categorized as an incident in a large company. While they do not differentiate between intentional and unintentional, a virus on a computer in the OT domain would not be reported as an incident, but as an observation and then handled accordingly.

One subject mentions that they base their official definition of the IEC 62443 standard.

Finally, an IT employee specifies that, since we ask for cybersecurity incidents, technology, computers, or networks, must be involved.

Worrying Events:

Both IT and OT employees are worried about events where an external adversary targets their safety systems, change parameters, and prevent them from closing down their facilities securely. The company size does not affect what events they are worried about.

While all IT employees mention attacks towards safety systems in the OT domain as a big concern, not all OT employees have concerns about events that can target the IT systems. Cryptolockers and ransomware are also mentioned as a concern, as this can lead to blackmailing and possibly a long period of downtime in production. The attack against Hydro in mentioned in this context.

> *"(...) there are actually only two attacks that worries me. One is typically what hit Hydro, an intentional attack where the adversary attempts to destroy as much as possible. (...) The other is an attack on a facility where the attacker aims to tamper with the control systems. (...) these are the only ones I would say are a company killer. Any other attacks, the company will survive, but what hit Hydro can kill a company." (5) - IT employee*

The answers of a small company stand out, as OT tells that they are afraid that they themselves, involuntarily through maintenance, do something wrong that will affect the systems. For instance, by bringing untrustworthy computers in or downloading infected files. It is mentioned that they do not scan computers before they are brought to the platforms. The IT employee answers that they are afraid of all events that they do not have the tools to handle, especially since you never know what the outcome of a cybersecurity incident can be.

Finally, one mentions unintentional incidents such as someone bringing a virus onto a platform from a USB-stick or a computer.

"I am not that worried about what we see, that people are inside and disturbs a PC or something similar, we can see that. But those that are invisible, that make changes that alters functionality, making us believe that we are safe, that is the worst." (6) - OT employee

Guidelines, Standards and Frameworks:

Companies follow mainly the same standards. Within a company, the IT and OT side with their distinctive systems, build their work on different standards.

The IEC 62443 series of standards is mentioned by all, even though not everyone bases their work on them. Several highlights that the standard is difficult to understand and heavy to read. Therefore, they have taken DNVGL-RP-G108 into use. This guideline explains how IEC 62443 can be implemented, as explained in Chapter 2. Further, NOROG104 was mentioned.

The NIST Cybersecurity Framework is referred to by three companies and is highlighted as a framework that is easy to communicate.

All IT subjects lists the ISO/IEC 27000-series when asked about which standards they follow, more specifically 27000, 27001, 27002, and 27035. Only one IT employee mention the ISO/IEC 27035 standard, which is used in this thesis to cover the cybersecurity incident management process.

Internal Frameworks and Plans:

Standards and frameworks are used as a foundation to create internal versions that fit each individual company better.

A majority of the companies have plans for the handling of cybersecurity incidents in place. These plans describe how an incident is to be managed, and the contact chain in case of an incident. While the names vary, the essence seems to be the same.

When describing their cybersecurity incident plan, the answers between IT and OT in one company do not correlate. From the OT side, the subject states that there is no direct plan for incident handling. He tells that IT might have one and

that OT contributes when needed. They have not focused on incident handling as a discipline, as the number of incidents in OT are low. IT, on the other hand, explains how they have an emergency response plan for cybersecurity incidents and that it is carefully thought through. It defines roles, responsibility, and authority, along with a process plan of who should do what in which situation. He specifies that the plan is very new, but that they have exercised on it internally and with the emergency response team. He does not specify which internal roles that participated in the exercise.

In one company, the internal standards are developed through a collaboration between IT and OT. In contrast, other companies have put together a group responsible for the internal requirements and contact relevant actors when necessary.

Plans are revised when needed, and it varies how often based on the type of plan. This means every year for some, at least every third year for others and when needed in general. One OT employee does not know if there are any formal requirements for revising their plans.

Training and Exercising:

All companies admit that they have not done enough training and exercising when it comes to handling a cybersecurity event, but states that this is something they want to focus on in the near future.

One company mentions that they have a minimum requirement of cybersecurity knowledge that employees need to know and that this is under development. For everyone that touches an OT system, they need to take a course to gain an understanding of what cybersecurity in OT means.

Two companies, one small and one large, have completed a large, practical exercise where the system parameters where changed, and the plan for managing cybersecurity incidents were tested. Both invited external partners, such as PSA, to observe. Another large company says that they conduct one large exercise yearly, but does not go into more details about the scenarios or who is included.

When planning the exercise, the smaller company chose to have a scenario where someone logged in remote with an unidentified client, got unauthorized access, and changed parameters in the fire and gas safety system. If a fire were to break

out in this scenario, the alarm would not go off. All employees were informed beforehand that an exercise was happening. They chose this scenario as they have many third party suppliers that work for them remotely, making the scenario more likely to occur. These suppliers were not included in the exercises. The Operational Manager initiated this exercise. IT has not had similar exercises but sees it highly relevant to do so. When asked about future IT exercises and the involvement of OT, OT would be included if the scenario includes both sides, as many of the company's systems do not affect OT. The subject underlines the importance of having exercises where both sides can participate. The decision of whether OT would be included or not would be a discussion between the IT manager and the Operational Manager.

One company had an exercise last year where the need for involving OT competence was unraveled. This led to changes in their internal plans, where OT now formally is expected to be included in the case of an incident and help consider the consequences.

"This changed our contingency plans a bit. Now, when something happens, we also have to be there representing the OT side." (7)

One subject mentions that they participate in European Cyber Security Month [1].

Many companies use tabletops as a theoretical, quick way of exercising. Answers about who participates in these vary. For some, if the exercises are offshore, only personnel on the platform is included. One also says that they have tailor-made tabletops towards the top management.

Furthermore, both subjects from one company mention that offshore train and exercise on Health, safety and environment (HSE)-relevant scenarios regularly, and tries to get cybersecurity scenarios included in the existing contingency plan.

"Clearly an oil and gas company has very extensive experience in handling incidents in general. What's new is probably getting cybersecurity incidents into the same category as all other incidents a company like this deals with." (8)

All that have participated in an exercise concludes that this has given them a significant learning outcome.

[1] https://cybersecuritymonth.eu/

4.1.2 Detecting and Reporting

Typical Cybersecurity Incidents:

Most companies state that they experience a large number of cybersecurity incidents every day, where common incidents are phishing and virus. None of the companies have experienced any larger incidents with significant consequences. One IT employee, from a medium-sized company, can concretize the number of events. They detect between 500 and 800 unauthorized logins and up to 100 phishing emails daily. Most OT employees find it difficult to estimate the number of incidents they experience, but numbers point to more yearly events.

The only company that states that they have never experienced a cybersecurity incident does not regard unintentional incidents as part of the definition. The subject believes that this could be explained by the fact that they are a small and not a global actor.

> *"We are a young company and a small company, nonetheless, it will be naive to believe that we are spared and that we are not in the sight of some actors." (9)*

Several mentions that unauthorized logins are another reoccurring event. One subject points out that those systems that are connected to the internet are constantly scanned. The frequency of incidents in IT are completely different from OT. IT from one company specify that due to monitoring and detecting, these attacks rarely succeed.

> *"There are constantly attempts to paralyze our systems." (10)*

None of the companies have experienced external attacks towards their ICSs, at least none that they are aware of. Many have experienced unintentional incidents, for instance, that a computer or USB has been infected. One company shares that they have closed down a platform due to a mistake.

> *"We have actually shut down a platform because someone made a mistake. They sat the security systems out of play, and we were forced to shut down.(...) it is a bit like an exercise, so fortunately no big drama, but it is clear that it takes hours to get a whole platform down and hours to get it back up. (...) And I can promise you, it is not cheap!" (11)*

Two companies have experienced viruses in their offshore facilities. Both had had viruses on a system for years, one believing it had been there for nine years. As it seemed it had no consequences and had been there for so long, the decision was taken to leave it until a planned shutdown of the systems. The OT employee states that IT would not have been able to leave the virus alone.

A subject highlights that he believes an attacker needs a certain amount of resources and knowledge to target their systems. They do not think random attackers can get access.

Political unrest is also mentioned by one company. Norway is an oil nation, and the attacks they experience are planned, targeted, and advanced. They do not believe that random adversaries tare accidentally attacking their systems.

Measures to Protect Against Cybersecurity Incidents:

When it comes to technical measures, all companies answer that they implement these according to industry-specific standards and governmental requirements. All have segregated their networks and systems. Other measures that reoccur are firewall, backup, antivirus, detection, surveillance, logging of network activities, and patching. While some of the companies monitor these technical measures themselves, the rest have outsourced this to third parties. One company informs that their most effective barrier protection, as of today, is the use of antivirus.

Four out of five companies explain that they have remote access to their facilitates. Only two of these go into details of how they manage it, where one has a control room on land where one can log on, and the other states that their suppliers can also work remotely.

More practical measures mentioned are, for instance, a training course for cybersecurity for OT. Anyone working with an OT system needs to take this course, to make sure they understand what cybersecurity in OT represents. Several also work with developing an awareness program to increase the understanding of cybersecurity throughout the organization. Other measures mentioned are phishing-campaigns, e-courses, and pen-testing.

When asked if these measures have prevented cybersecurity incidents, one IT employee answers that the number of end-users that falls for phishing email has decreased.

4.1.3 Assessing and Deciding

Priorities During a Cybersecurity Incident:

The NIST CSF and its five functions is used to describe the priorities in this section.

Today, all companies focus on preventing an incident from occurring. Being preventive and hinder an incident before it can escalate is considered the cheapest solution. Their lack of experience with incidents is the reason for the large focus on Prevent, explains one OT employee. One of the companies belonging to a global organization has been told to only work on prevention, and that the other functions are handled globally.

The importance of Detect is mentioned by a few. If one experiences an incident, then it is essential to try and get control over the situation, tells an OT employee. An overview of the incident is desirable, and third party suppliers have been hired by several companies to log activities in their networks. The companies that are not currently focusing on Detect identifies it as a function their company should have in mind.

Only two companies state that they are working on all functions from Identify to Recover. One of these places most of the effort in Identify, in addition to the functions previously described. The other states that they are spending more resources on Respond and Recover. The IT employee of the second company does not specifically say that they are working in all functions, but rather that they hopefully do, as quote number 12 states below. OT explains that the focus area of his work is on the left side of the bow tie from NIST CSF, especially to prevent a fire from ever occurring on a platform. Further, he emphasizes that the company does focus on the later functions.

"Hopefully, we focus on all phases, but where we, like most other companies, have invested the most throughout the years is on what happens before an attack (...)" (12) - IT employee

A majority of the subjects believe that there should be a greater focus on the lather functions of NIST CSF. Even though most are satisfied with the work conducted on Protect, they see the necessity of being able to handle an incident and reduce the consequences. Should a facility be attacked and the production affected, ensuring the integrity of the facility and restoring the production is

a crucial step. More resources on Detect, Respond, and Recover would an IT employee prioritize moving forward. Spending time on Identify, with its risk assessment and similar activities, is regarded as unnecessary since they often know what the error is. Learning from an incident is a measurement one OT employee suggests.

Safety and availability are always the main focuses of OT. While safety on a facility and for the workers has the highest priority, integrity is also essential to maintain the production. Confidentiality is not a major focus for OT since the ICS systems do not usually carry personal information, separating OT from IT. Different priorities are evident with the example of a virus that has been on a computer for a longer period of time, but that OT chose not to handle it immediately. OT assumes that IT would have fixed the issue instantly.

A majority of the IT subjects explains that their priorities depend on the systems that are exposed, mentioning both IT systems and OT systems. Earlier, the focus was only on confidentiality. Now availability has become more critical in the eyes of IT. The rest highlight confidentiality as being most critical.

Internal Cooperation:

The cooperation between IT and OT is considered to be good by several subjects. The differences in priorities between IT and OT is one of the challenges that affect cooperation. Most companies have plans and procedures which explain how cooperation should be performed.

One OT employee mentions that they are dependent on ITs systems as these are important auxiliary systems. The decision to include OT or not, in case of an IT incidents, are taken on the IT side. There are no guidelines for how to include OT today, but the employee believes that OT should be included in these decisions. He points out that IT is much more vulnerable compared to OT, and that OT does things differently than IT. The quote below is taken from his answer regarding their processes for how to include OT.

"They are mainly only taken on the IT side. There is no systematic approach to involve OT in it." (13) - OT Employee

Cooperation is not seen as a challenge by neither IT or OT of two companies. The small company does not mention any areas of improvement but mentions

that the company has never experienced cybersecurity incidents. A governed process describes how IT and OT is to work together during incidents in this company. They have carried out a larger exercise where both sides participated and contributed. This exercise demonstrated that they are able to cooperate and handle exercises. Further, it is mentioned that IT and OT have daily communication and cooperation meetings where relevant themes are discussed. Through these meetings, they are working towards a common goal. The employees of a medium-sized company tell that their cooperation is good. The company has experienced good collaboration and positivity during incidents where the emergency organization has been contacted and called out. However, as a result of not being properly equipped to handle all types of cybersecurity incidents, they have faced problems with time management, both internally and in collaboration with suppliers. The IT employee means that they are not able to handle such incidents fast enough and that they, therefore, spend more time handling it than they assume they would. Instead, they are built to deliver production efficiently states IT.

OT remarks that terminology should be kept in mind when communicating with people from other environments. For instance, when advising a facility manager about whether to shut down the facility or not, one must be able to communicate clearly. The OT employee emphasizes that training on how to substantiate the different consequences an cybersecurity incident could have, is necessary. Further, OTs focus on availability and production, as described in 4.1.3, influences the cooperation. This challenge is mentioned by a few other OT employees.

IT is the unsatisfied party in companies with disagreements regarding internal cooperation. In a large company, this culminates in the role distribution and responsibilities explained in their plans. Who is to be in charge of an incident is unclear.

Even though OT employees state that the cooperation is good, challenges are located. An OT employee highlights the different focuses and priorities of IT and OT. Furthermore, an unsatisfied OT employee states that there is a fight for the available resources between IT and OT. However, the cooperation is improving, as he stated in the quote below:

"The cooperation is getting better and better, there is no doubt about that. We get more and more respect for each other and we are becoming more and more dependent on each other." (14)

Belonging to a global organization can challenge the cooperation between the local and global teams. To rely on a foreign team to handle local cybersecurity incidents is not easy. Different time zones and the uncertainty of knowing when to involve the global team are challenges. The cooperation is better on a local level. In one of these companies, both IT and OT work from a mutual operation room where they handle smaller incidents together.

Similar to having plans that describe responsibilities, some companies have plans that explain when IT and OT should include each other in the cybersecurity incident management process. Responsibilities and cooperation are often described in the same plans. In a large company, the extent of involvement depends on the type of incident and where it unravels.

"There is no "us" or "them". There is only we." (15)

External Cooperation:

Cooperation with suppliers and sharing experiences with other companies is usual in the industry.

Companies share their own experiences in forums and CERTs. To one company, participation in KraftCERT is of no interest. Instead, they want to gather Norwegian companies of different industries in NorCERT, justified by the fact that Norway is a small country with minimal resources and competence. They do not want to divide competence into smaller environments. One of the companies belonging to a global organization does not participate in a Norwegian CERT, but rather has a global environment. A small company has not yet joined a CERT, but it is under consideration. All participate in CDS-forum[2].

The majority of companies have hired suppliers to handle, for instance, detection and surveillance. The strategy of a small company is to not be experts in all competence areas, but rather outsource many of these areas to third parties. The exact cooperation they have with all suppliers is not described in detail.

[2]https://www.sintef.no/projectweb/cds-forum/

One company faces issues when suppliers must be involved in the handling of an incident, as described in 4.1.3.

Further, companies in the industry cooperate, to some degree, to create and maintain official standards and guidelines.

4.1.4 Responses

Response Time:

" (...), so we will never discover it before something has started to go wrong, before they modify the ICS. Don't think we have any chance of such zero-day type of targeted attacks". (16) - OT employee when asked about how fast they will discover an attack.

Uncertainty is a key factor when it comes to how long the companies believe it will take before they have a response. While none can specify an amount of time needed, some believe that it does not take long from the incident is detected until the right personnel is involved.

Several companies underline that they believe their response time would be completely different should an attack of large scale, like Hydro, occur. Since the incidents they have experienced have not had any severe consequences, they have taken their time to respond and decide upon a course of action. Small incidents, such as a virus, is mentioned by one OT employee to be an incident of minor focus.

""(...) but it would have been a whole different pace if it had been serious." (17) - OT employee about response time.

One company mentions that some of their employees might be hesitant to report a cybersecurity incident, as it can be difficult to know if it is an attack or a mistake.

Consequences of Cybersecurity Incidents:

As most companies have yet to experience a more substantial cybersecurity incident, there have not been any significant consequences. The only consequences that are mentioned are minor data losses, reconstruction of a computer, productive time lost for those involved, and time spent unraveling the incidents.

Contact Chain During an Event:

Who to include and how this process is done, varies from company to company, and is also affected by the size of an incident.

IT and OT will often include each other in the process because of the dependencies they face. One company would previously leave the responsibility of handling an incident with a separate team, even though the team did not have the right competence. Today, the team will instead assist with the analysis, while IT and OT must be able to handle incidents themselves. As a result, the responsibility is more shared, and it is, therefore, paramount that one has the right personnel available at any time.

To a large extent, small incidents are handled locally, implying that offshore personnel is in charge of facilities. As they often have the highest knowledge of how ICSs work, they are capable of making good decisions by themselves. However, this does not mean decision making happens without any help. Remote employees, especially from IT, can advise them and give recommendations for actions that should be taken. The IT employee of a large company can inform that facilities often follow their recommendations.

For global organizations, processes describe how an incident is to be handled both locally and globally. The local company is allowed to handle smaller incidents themselves. However, if an incident is labeled as a major one, the local team is required to contact a global team. This team is responsible for handling such incidents and has the overall authority. Therefore they can take actions they find necessary to gain control.

All companies will scale an incident if there are any signs of it being more serious than initially predicted.

Who is included in the emergency response team is diverse. The team has the mandate to instruct employees to contribute and complete demanded actions in several companies. In a large company the emergency response team consist of a Computer Security Incident Response Team (CSIRT) which includes IT, while OT is left out, but can advise them on practical tasks. Even though OT is not in charge, they are included in a larger extent today than previously. The IT employee states that the right people are centrally placed in this team and point to employees who are to respond to the event, for instance, OT.

One company has separated the emergency response team into a local team on the facility and a management, which takes effect onshore. The onshore team is established to give support to the local team during larger incidents, while smaller incidents will be handled locally as previously described.

The emergency organization in a medium-sized company consists of IT and OT and is lead by the Chief Information Security Officer (CISO). They will collaborate with parties responsible for the systems. The other parties that are included are mentioned in the quote below.

"(...) there is a joint effort with those who are established and have processes towards management, authorities, insurance, national institutions such as PSA, (...) and other parties (...) We also make sure that we have the right expertise to complement those in readiness, because they know nothing about the digital world as much as these do." (18)

4.1.5 Lessons Learned

Major Challenges and Lessons Learned:

The most reoccurring challenge is uncertainty related to cybersecurity incidents. It is not just related to dealing with an incident but also related to not knowing if someone is in your system. One subject states the following:

"One thing is to handle that one has discovered, what one sees, what one knows. But there is a chance that there are a lot more that one has not discovered yet." (19) - OT Employee

Uncertainty is mentioned, along with numerous examples. First of all, as the industry has not had any larger incidents, one points out that their experience base is narrow. Cybersecurity is a field that is rapidly evolving, and new ways of attacking are found all the time, which is especially demanding for a smaller company, as they do not have employees that work 100% of their time with cybersecurity. This same company also mentions that after they have examined an incident, for instance, phishing, they need to come to terms with the fact that they have done what they can, but might not be fully secured.

Even though most companies have few to none incidents to report, they have used cybersecurity incidents that have happened to other companies, as a learning

experience for themselves. One company reports that they had a retrospective after the Hydro incident, brainstorming about how the company would have handled the attack. This resulted in changes made to their plans.

"Because we haven't had so many incidents or carried out that many exercises. We assume a few things." (20)

An IT employee states that due to a lack of structure, a retrospective is not always completed. He has seen a tendency of their structure and processes to disappears when encountering a larger event, and that one is more dependent on individuals knowing their job. This employee believes that training will make a difference in how they tackle larger cybersecurity incidents. OT from the same company addresses that their employees need to go through exercising, but that they are working on defining a minimum competence requirement that all employees must comply with. Another problem that is pointed out is the need to have access to the right competence at all times, not depending too much on individuals. As a result of exercising, this organization realized that they could not depend too much on staff on land. If anything happens, local knowledge and local presence are key to handling the incident, not a security team based on another continent.

Answers from one IT employee stand out, as he does not think the incidents themselves are hard to handle. Working strategically over time, making the right decisions, especially in these times where the Coronavirus has heavily affected the oil prices and the financial years to come, are the challenges he devotes the most time. In relation to a cyber incident, however, he points out the difficulty of remaining calm when discovering an incident. The Identify function is his biggest challenge and mentions getting an overview of the incident, how and when to decide upon what measures that should be taken, and handling top management are all situations he can find difficult.

The need to have a written procedure that describes who is in charge of making a final decision, when to invoke the next step and which consequences it will have, was recognized by one company. They had to make the time period from an incident is detected and how to notify the right personnel clear.

Finally, a small company addresses the challenge of balancing protection and budget. There is always room to get better, but they need to be satisfied with their protection at some point.

"We can probably do everything much, much better, but ... We think that what we do may be good enough, but we don't know." (21)

Recommendations:

A high focus on communication between IT and OT is recommended by the majority of the subjects. Measures that are mentioned to improve communication are sharing knowledge between the two, asking each other questions and building trust, and the importance of human interaction between sides, so that faces are familiar. One company has created a centralized base for both sides to improve the partnership and has only had good experiences with this so far.

To plan and enact a large exercise is strongly recommended by those who have completed one. By conducting an exercise, you have the opportunity to figure out what is not working as it should and find vulnerabilities in plans, processes, or systems. It is therefore strongly recommended by those with experience, to set aside the funds needed, and plan an exercise in the near future. One subject share that they were unsure if conducting a larger exercise was expedient but decided to give it a try. Even though the exercise was not conducted perfectly, they found a lot of areas to improve. And, as pointed out by another, smaller tabletops are also a good way of theoretically going through a scenario.

It is demanding to build up distinct specialist environments for incident handling and detection. An employee from a large, resourceful company recommends small companies to put out the detection function to a reliable third party and keep a small environment for incident handling internally. Unless a company has many workers and a lot of resources, it can be difficult to create a strong environment within the company. However, as pointed out by a subject from a smaller company, keeping a close dialogue with suppliers is extremely important. When a task or responsibility is outsourced to a supplier, one can become too dependent on them. But at the end of the day, if an incident occurs, it is the system owner who has the responsibility.

"So there's one tip I would give: outsource it, but outsource it to someone you trust." (22) - IT employee recommending the use of third parties to smaller companies

One recommendation is to centralize IT and OT internally. Having two separate

environments will most likely not work as it is difficult to find enough people to manage both. Norway has a small academic community when it comes to cybersecurity, especially in ICS, so getting the right people and the right knowledge is difficult. In addition, the employee recommends starting with the smaller exercises and make sure one is able to handle these before moving on to larger and more advanced ones.

Creating a mutual plan for how to handle cybersecurity incidents that applies regardless of which domain you work in has recently been done in one company. As one needs to work together with some incidents, this is recommended. This plan also takes into account the competence from both sides, and how to utilize it in the best possible way.

"Also, I think that those who handle events need to be aware that there is a difference between IT and OT. There are completely different consequences to taking down a system at a facility than it is at the office network." (23) - IT employee on other recommendations

4.2 Interview Findings - Industries A and B

This section presents the findings from interviews with Industry A, a large company from the transportation sector and Industry B, a medium-sized company from the energy sector. Unlike the findings in 4.1, this section will not be separated into the five phases of the ISO/IEC 27035 standard, but are grouped into five main headlines.

Industry B is in the midst of a restructuring, where it today consists of two sections that will be merged. This has affected their answers, for instance, when it comes to their organizational structure, where they do not have a clear answer.

4.2.1 Organizational Structure

Industry A:

The focus on operational security has been increased, as a result of a project that started a few years ago. They identified a number of deficiencies in the organization and management systems, which in return led to more focus on cybersecurity in the OT domain. Here the newly appointed head of department for cybersecurity came in and outlined a new approach with a greater focus on

governance for the company. This resulted in the company being expanded with new roles in the cybersecurity department.

The cybersecurity department of industry A has an interface towards both IT and OT. However, the risk and technical debt of OT systems are greater, where technical debt express that the OT systems are older and more challenging to update. Over a year ago, the information security responsibility was also moved to this department, and a CISO position was created. The CISO has the overall responsibility for information security.

A separate unit handles traditional safety. They are the overall link to preparedness, accidents, environmental events, etc.

Industry B:

This industry, consisting of two sections, has had two different structures in the merging process. These operate separately with their processes and systems. Security is handled by a security organization in one section, while the other has given the responsibility to one role.

4.2.2 Definition

Industry A:

A cybersecurity incident, or digital security incident, can be both an intentional and unintentional incident that affects the security of a system from the outside. However, it is emphasized that the digital security formulation does not require that a threat actor is present, but that the cybersecurity incident definition does. Internal employees committing mistakes, which would be an unintentional incident, is one of the greatest threats:

> *"They do not have to do anything wrong, they can also just not do anything right." (24)*

They believe that all from smaller incidents involving an arbitrary actor and upwards will be taken care of by securing their systems from the larger, intentional attacks constructed by higher-level actors such as foreign states and insiders. Therefore the focus of the definition is mainly on intentional incidents. The insider is an adversary they consider to be of importance. It is highlighted that if you are able to protect your systems from the insider that knows your systems, then you

will, to a large extent, be protected against the employee who made a mistake or acted unaware.

Their definition of a cybersecurity incident is based on other public definitions. The Official Norwegian Reports (NOUs) were relevant to, for instance, establish a distinction between safety and security. Which, as stated, in the Norwegian vocabulary is under the same wording. This was to highlight their focus on security and intentional incidents. While the ISO/IEC framework, such as 27001, is referred to in their control system and gives definitions for information security incidents.

Industry B:

A cybersecurity incident is not clearly defined in industry B. Throughout the interview, terms such as security, information security, and ICT security was mentioned and used, while cybersecurity was rarely brought up. When specifically asked what they put into the concept, it was said that the internet is involved. Nevertheless, it was eventually clarified that both intentional and unintentional incidents should be included.

4.2.3 Responsibility and Experience with Cybersecurity

Industry A:

When this new department was established, a decision was taken to include the word "cyber" in front of all titles. The reasoning behind this is that safety and security are the same words in Norwegian, and they wanted to state their focus area clearly. Their responsibility is, therefore, differentiated from the more traditional safety.

Resisting unwanted, deceptive attacks or establishing measures against attacks is stated to be the cybersecurity department's specialty. The department conducts risk analysis, threat analysis has the responsibility for the Security Operations Center (SOC), and supports other departments with securing their systems.

The company is regularly the victim of attacks, but cannot say how many of these are targeted directly towards them. Typical incidents they deal with are, for instance, internal vulnerabilities as a result of legacy systems, phishing, or administrators that can use the same passwords in several places. An attack that

worries them is that someone will gain access to one of their domains and override the remote control by exploiting unknown holes in their systems.

For Industry A, their main priority is to be able to operate in a safely manner. If there are uncertainties regarding the control, meaning an adversary can have taken over, the unit will be stopped. This is a health and life assessment, and therefore, integrity is highly valued in the industry.

Industry A has not been able to place equal focus on all functions of a cybersecurity incident. It is claimed that this is a result of their lack of experience with major incidents, such as Hydro or Maersk. They believe they have a healthy focus on prevention and preparedness, exercising on relevant cases regularly.

> *"I mean, and will always mean that if you are good on the preventive side, there will be less, and less, and less to do on the incident side." (25)*

Getting an overview of the situation is mentioned as their biggest challenge in relation to cybersecurity incidents, which is key to be able to handle the incident in the most correct manner as possible.

Industry B:

IT and security are placed under one role in the first section. The IT employee with this role suggests that there should be two dedicated roles, one for IT and one for security. He further states that cybersecurity is only a fraction of his role. It is expected that Industry B might have dedicated resources and roles working only in cyber in the long run and that they will rather have a broader approach in the beginning until the team has enough members to distribute roles.

Earlier, the second section had a CEO that was conscious of his ICT security responsibility. The subject highlighted the positive effect of the management being aware of their role, and how the CEO was directly involved and questioned cases such as why all users had admin access.

Phishing and virus are mentioned as incidents they often experience, and ransomware is an event they worry about. The services they have that are connected to the internet are continuously scanned. Whitelisting as services are mentioned as a barrier they want to implement.

The first section has experienced a larger cybersecurity incident triggered by an unintentional incident where someone clicked on a link. It lasted over a longer period, where all employees with a security tag were gathered. It was quickly realized that OT was not affected, only the IT environment, but both were followed up more closely. Suppliers were contacted and assisted in handling the incident. The companies worked well together despite their differences, andIndustry B learned a lot from the incident. The employee from this section opted for a joint evaluation after the incident with both IT, OT, and the external resources. However, the company did not find time to carry it out.

4.2.4 Cooperation

Industry A:

The internal cooperation of Industry A faces a few challenges, and none are in the case of an incident, explains an employee. Getting system owners and service owners to recognize the need to close vulnerabilities is considered a challenge.

There are examples of cases where the cooperation has not been optimal, for instance, the cybersecurity department has not been included to the extent it should. This means that they do not always get to perform their threat analysis. However, it is mentioned that the department's employees might not have adequately advertised their involvement and responsibilities in cybersecurity. An incident in which they were not sufficiently included in is mentioned. It occurred that a component connected to OT systems could be under attack. Instead of informing the cybersecurity department so that they could examine it and verify that the possible attack had not gotten further into the system, the incident was treated as an IT incident and solved as such. They are now working on new routines that will secure better communication in these cases.

A supplier handles the operation of IT systems. In terms of technical resources on the IT side, little is taken care of internally. They are responsible for operating agreements. The communication with suppliers is not where it should be, as shown by the incident above.

Issues are linked to the fact that the cybersecurity department, consisting of both IT and OT, is young. Therefore they do not have the entire organizational structure in place. For instance, routines, for who to contact, and why are not yet ready.

The main challenge between IT and OT is the pace of change, and that the maintenance and opportunities to have downtime are different.

For external cooperation, Industry A is a member of National Cyber Security Centre (NCSC)[3] and has an insurance contract which makes an external party come in and help them during an incident. Further, they have a few industry forums and is a member of a European ISAC. They have no CERT memberships.

Industry B:

IT and OT work separately, and barricades, as he calls them, exist between the environments, stating that it is "us and them". However, the employee in this section says that they must unite forces and competence as they can learn much from one another.

> *"I'm an advocate for tearing down those barricades there and removing those silos. We are in the same boat. And we clearly have different experience, different knowledge, but together we become much stronger (...) Here it is about uniting the forces and the knowledge, for an IT technician, we can call it, has a lot to gain from the OT environment and vice versa. And especially from a security perspective, I think." (26)*

A broader focus on the dependencies between IT and OT in the entire organization is mentioned as important. This must be rooted throughout the organization, especially by those who work with operations daily.

The distinction between IT and OT is said to not be as clear in the second section. A lot of resources are used across the environments.

When asked about the incorporation of IT and OT, one subject stated that he believes the oil and gas industry has come further with the cooperation between the two groups, with the energy sector following behind.

4.2.5 Training

Industry A:

When asked about recommendations for others, they underline the importance of communication, training, and exercising.

[3] https://www.nsm.stat.no/NCSC/NCSS-hendelser/norcert2/norcert-eng/

Industry A has competence requirements for its employees and established a plan where all parties can add relevant courses and competence areas. The head of the department mentions that he is fond of cross-training to learn each other's functions. This type of training opens up for better professional sparring between roles.

"(...) in order to do a good job, you need up-to-date expertise in the area you work with and adjacent areas." (27)

There is also a focus to keep employees continuously updated on the systems they work with. An example can be that if one uses a specific firewall, then courses about this firewall is relevant for all employees with a responsibility in this area.

Exercises are carried out minimum quarterly. An exercise plan has been approved. Industry A has both training of the local emergency response team and also higher up in the division, for instance, with the central communication staff. They have also executed joint exercises and are planning to perform more of these. The scope of an exercise determines what type of exercise should be executed and who to include.

They have conducted a risk analysis to create scenarios for exercises. Scenarios for exercises are only determined if one identifies risk factors during the analysis. This form of creating exercises is appreciated by one employee.

All exercises in Industry A are announced in advance, but the content of them is not always informed of to the employees. They find it necessary to announce future exercises to reserve employees' time such that they will not be disrupted.

Industry A performs both theoretical and larger practical exercises. They prefer game exercises over tabletops as the first is more dynamic and realistic. In the ICT domain, they believe that game and full-scale exercises are almost the same, since the identical group of people, the crisis management, is sitting around the same table with the same equipment.

There are no mentions of whether third party suppliers are included in training and exercises.

Industry B:

Self-study is a form of training that is highlighted by the employees. They attend conferences and such that they find useful. However, there are no requirements for what should be attended and learned on an organizational level.

One of the subjects highlights the importance of continuous awareness and focus in the organization, not just during the security month but throughout the entire year.

> *"(...) some internals believes "that was the year we got to experience an attack". I don't think we can think that way. We must always be prepared for the next." (28)*

about what is happening internally, deviations, and incidents. This is put forward as a good practice, especially to increase awareness in the management. Furthermore, the report was presented at an industry forum, where it was well-received.

The subjects mentioned that they had had tailor-made exercises targeted towards the management group, and the management group with necessary personnel from different areas. An example that is mentioned is one case where they used a third party to create and lead them through the exercise. They have not conducted larger, practical exercises, only simulations.

During the conversation about exercises, it is mentioned that they have hired a service from a third-party provider and gave them two computers with standard user access. The goal was to see how much one could do from the inside, and as stated by the subject, the results were alarming. The company has also participated in a case study where the Office of the Auditor General of Norway[4] tested their systems.

[4]https://www.riksrevisjonen.no/en/

Chapter 5
Discussion

This chapter will discuss the research questions presented in Chapter 1, by using the findings from Chapter 2 and 4. We have divided the chapter into four main sections, one for each of our research questions and then finally one for discussing the limitations of our thesis.

The first section, Section 5.1, will discuss the first question, namely how the current cybersecurity incident management process in industrial ICT systems is. The second section, 5.2, will then discuss how IT and OT can work together to improve their cooperation for the future. Section 5.3 discusses the third research question, what oil and gas can learn from two other industries. Finally, Section 5.4 goes into the limitations of our thesis.

5.1 Research Question 1

How is the current cybersecurity incident management process in industrial ICT systems?

The thesis was targeted towards the cybersecurity incident management process in industrial ICT systems in the Norwegian oil industry, but as OT systems rely heavily on IT components and systems, employees from both sides were included. An attack towards the IT systems can be the first point of entry to the OT systems [AS20c], meaning that the chance is high that they will experience cybersecurity incidents where both sides should be involved. Answers from the IT side are therefore included to get the full picture.

ISO/IEC 27035 was considered the most common standard by IT personnel for

management of cybersecurity incidents, but it was only mentioned by one IT subject during the interviews. However, the majority of those that participated mentioned the NIST CSF, indicating that this is better known to the industry. One subject also mentioned that NIST CSF is easy to communicate. In Chapter 2, the functions of NIST CSF are compared to the phases of ISO/IEC 27035, explaining that while the phases do not perfectly align, much of the essence stays the same. Therefore, when describing the cybersecurity incident management process in the Norwegian oil industry's industrial ICT systems, these five functions of NIST CSF will be used. A description of each of these can be found in Section 2.1.5.

When asked about which phase of an incident companies focus on, referring to before, during, and after an incident occurs, many referred to the bowtie from NOROG104, showed in Figure 5.1. A large portion of the tasks connected to the different functions is not elaborated through our questions or by our subjects' answers. We have only included those activities that are relevant to the answers given.

The bowtie lets subjects state that they did most work on the left side, before an incident occurs, indicating a focus on Identify, Protect, and Detect.

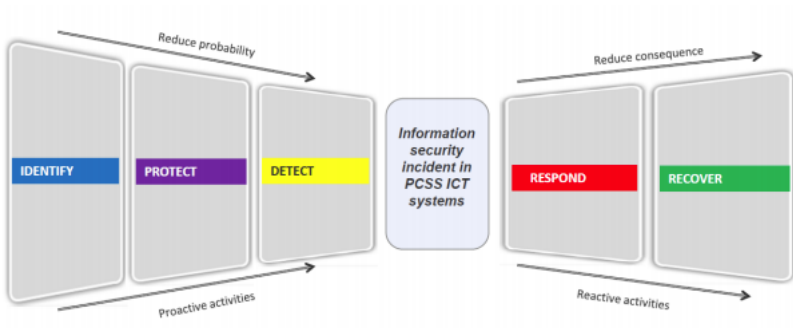


Figure 5.1: Incident management bowtie showing the different functions of NIST CSF and the connection between them. Image taken from [OA07].

Furthermore, the majority believes that more time should be spent on the two last functions, while the rest believes that they are prioritizing the right ones. Table 5.1 shows the participating companies' overall focus, as explained by the subjects.

The fact that few oil and gas companies have been exposed to cybersecurity incidents can affect their attention.

	Priority		
Functions	None	Some	All
Identify		X	
Protect			X
Detect			X
Respond		X	
Recover		X	

Table 5.1: The different functions of NIST CSF and how they are prioritized by the participating companies.

5.1.1 Identify

Activities in Identify, important as they are, are not highlighted as a focal point for the majority of the subjects. During the Identify function, one sets the foundation for managing cybersecurity risk. Many of the activities connected to Identify, can be considered one time activities, which are only revisited when needed. This can also explain why activities belonging to the function are not more specifically mentioned by our subjects, as they are already completed. One employee downgrades Identify, on the basis that he would want fewer resources going to risk assessments and similar task since they often know what's wrong.

Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, partners, customers) are established:
The cybersecurity role and responsibility distribution seem different from company to company, but all subjects explain that they have defined these, as presented in Section 4.1.1. Furthermore, several mentions that they have these written down in internal plans and processes, but not all. However, one subject mentions that their roles might not work as intended in practice.

All companies lean on services from third party suppliers, the smaller companies to a greater extent than the larger ones. Cases like the following are mentioned during the interviews: suppliers that do not participate in exercises, suppliers that take personal computers out to facilities and suppliers that do not always have

the right work permits. In any of the interviews, it is not explicitly addressed how the role and responsibility distribution is solved with suppliers. However, these cases can indicate that there should be a greater focus on clearly defining and coordinating responsibility with suppliers for these companies.

Cyber threat intelligence is receieved from information sharing forums and sources:
All companies have external partners where one can share information about the current cyber threats. The majority mention that they receive reports from NorCERT and that NSM has probes in their networks.

The organizations place in critical infrastructure and its industry sector is identified and communicated:
Norway categorizes oil and gas as a part of their critical infrastructure [fsobD12]. It is mentioned by one subject that the industry may be an attractive target because of the importance for the Norwegian economy.

Summary:
To summarize, Identify does not come out as the highest prioritized function of the three at the left of the bowtie in Figure 5.1. While it seems that activities such as role and responsibility distribution have been conducted, the fact that the roles and responsibilities are not clear for all companies could indicate that these plans should be better rooted in the organization. A poor allocation of roles and responsibility could strike out in later functions.

5.1.2 Protect

Protection is a function companies can spend endless resources on, but the question is how much they should spend on protecting themselves. This is a challenge that is pointed out by one of the smaller actors. Where the line goes for how much a company should spend on protection can depend on the company, size, and how many incidents they face today.

Network integrity is protected (e.g, networks segregation), and other general activities to protect technology, processes and data security:
All companies have a range of measures and barriers to secure the integrity of their networks, which is a requirement from PSA states an employee. One way they maintain integrity is through the segregation of systems. All highlight segregation of technical systems and OT systems. Other specified barriers are

firewalls, backups, logging of traffic, and antivirus. Only one company states that they perform pen-testing of their systems, which DNV GL recommends as a protective measure [AS20b].

Remote access is managed:
Remote access is one of the great benefits of digitization and an opportunity that all exploits. Four companies explain how the access is performed. Not much was mentioned about how companies manage remote access, but as this is a possible point of entry to attack facilities, it should be highly prioritized.

Removable media is protected and its use restricted according to policy:
Removable media should be protected and used according to policy [Mus14], but it has not been guaranteed by all. Three companies have specifically experienced that a supplier has brought with him or her a virus on a USB stick, CD, or laptop to a facility. One company informs that they have procedures in place that controls this access, but that they can easily be bypassed. The fact that companies are unable to prevent these cases goes against the recommendation from NIST CSF.

Response plan are in place and managed, and tested:
The advice of NIST CSF in regards to response plans and recovery plans are not followed by any company to a full degree. Both plans are to be in place, managed, and tested [Mus14]. One company explains that they have both incident response plans and a disaster recovery plan, while another only mentions incident response plans. The rest state that they have plans; however, they do not go into the depth of what they contain. There are different requirements for revisions of internal plans in each company, but none further describes how they manage and test their plans.

Awareness and Training: all users/privileged users/third-party stakeholders (e.g., suppliers, partners, suppliers) etc. understand their roles and responsibilities:
Awareness and training is an essential activity in the Protect function, and all companies perform training and exercising to some extent. This can be everything from courses, seminars, and certifications. There is little to none awareness training for regular employees. Such training may play a role in the amount of unintentional incidents companies experiences. Phishing could be avoided

if employees, especially outside of the technical departments, can discover fake emails and report them. One subject stated that employees are clicking less on links in phishing emails, indicating that the awareness can have improved in this company. It is not mentioned whether suppliers are included in awareness or training. Several mentions that they are working on their cybersecurity awareness, either developing an awareness training program or setting competence requirements.

Even though the training and awareness activities do not explicitly mention exercising, it is considered to be necessary to make sure that employees are "trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements" [Mus14, p. 31]. All companies state that they do not have enough focus on exercising, regarding it as essential, and wishing for more exercises in the future. Only three companies have completed major cybersecurity incident exercises. One of which included one of their suppliers in the exercise. Some companies have performed tabletops. The activity needs more focus from all companies. The majority are planning to execute more extensive, practical exercises. However, they are not more specific in regards to when.

Summary:
The measures that are taken by companies to protect their systems, production, and employees extend far. It is evident that Protect is considered a critical function. It is therefore assumed as the facet for all oil companies, as too little focus can have consequences that violate their requirements and exposing them to dangers they possibly could have prevented. Placing resources in this function seems natural, as it can be easier to see results here. Barrier control appears to be highly prioritized, but the majority should focus more on awareness and training.

5.1.3 Detect

Choices made in Protect regarding measurements, such as firewalls and antivirus, will affect the companies ability to detect an event. Measures have been taken in companies to detect incoming cybersecurity incidents. Both surveillance and monitoring are necessary to get control over the situation and reduce the consequences.

Detected events are analyzed to understand attack targets and methods / the network is monitored to detect potential cybersecurity events:

It is not always evident if a cybersecurity incident is occurring. Especially one company highlights that knowing whether one is facing an event, intentional, unintentional, or not at all, is problematic. Attacks against OT are reasonably new, and knowing what to look for is not entirely clear, possibly making it difficult to detect errors. Having a greater focus on being able to recognize cybersecurity incidents may be necessary to increase the reinforcement of Detect.

All companies rely on SOCs to, for instance, analyze their logs and monitor traffic. These centers are mostly external and delivered by a third party. One company depended mainly on an internal SOC and uses an external one to secure 24/7 monitoring. Another company has a global SOC, which sets requirements, procedures, etc. None of the companies go into detail of how the external SOC handle the analyzed data. It is assumed that they will inform the company affected of an incident such that they can take action.

Impact of an event is determined:
Discovering intentional incidents early is crucial to stop attackers and limiting harm. The impact of an incident is determined in the Detect function [Mus14]. In a few cases, companies have been able to determine that actions should not be taken to manage an incident. When an incident has no alarming consequences, determined through analysis, for instance, a virus can be left for many years without any major fallouts. None of the companies have experienced any attacks that have led to significant consequences, only loss of time and reconstruction of a computer are mentioned. The only event, not a cybersecurity incident, worth mentioning is when one company shut down the facility as a result of a human error.

Summary:
All companies have measures in place to detect cybersecurity incidents. If incidents are discovered, either through detection or failures, the next step of NIST CSF is Respond and Recover.

5.1.4 Respond and Recover

The right-hand side of Figure 5.1, is not mentioned as a top priority by anyone, but two companies mention Respond and Recover as functions they spend resources on. Cybersecurity incident response and recovery plans, which are essential after an incident, vary in name and content; nonetheless, companies seem to have them

in place. Due to the number of incidents being so low, prioritizing many of the activities in the Respond and Recover function can be difficult.

Response plan is executed during or after an incident and incidents are reported consistent with established criteria:
Cybersecurity incident response plans, as explained in 5.1.2, seem to be in place in all companies. These plans vary in content and are important during Respond. One company has very recently finished their plans. One company expresses that they experience difficulties when the incidents are larger, but that smaller incidents are handled well, and plans are followed. Depending on the incident, three companies state that they will take the time they need to properly handle the event if it does not have any large consequences. But, as most point out, knowing how they will react to a larger incident is difficult. One even states that the company feels less confident in that they will be able to handle a Hydro-like incident. This can indicate that more focus should be put in Respond, keeping their response plan up to date and understood. Also, due to differences in answers to what a cybersecurity incident is, reporting incidents with established criteria can be difficult.

Understanding impact of an incident and categorize incidents consistent with response plans:
To know the impact of an incident, and categorizing it, is mentioned as difficult for many. One company with access to a global team states that when they are sure that they are facing with a cybersecurity incident, handling the incident is not the problem. For companies with global resources, smaller incidents are handled, but larger cybersecurity incidents are a source of insecurity.

Personnel knows their role and order of operation when a response is needed:
As written in 5.1.1, indicators suggest that the roles and responsibilities are defined. However, one mentions that their roles and structure seem to disappear when they face larger incidents. Another says that each can have different perceptions about who is responsible for which tasks. This could indicate that this activity should be higher prioritized, at least by these companies. As mentioned in 5.1.2, more focus should be on awareness and training. This will help personnel to know their role and order of operation when a response is needed. Companies that lean on global resources have an advantage, as they have access to a greater pool of knowledge and support.

Response plans incorporate lessons learned and response strategies are updated:
Learning from a cybersecurity incident, and updating plans is important on the right side of the bowtie. Many states that they have a retrospective or lesson-learned activities, but also that they do not conduct these as often as they should. One company used the Hydro incident as an opportunity to learn, while another investigates major incidents, resulting in stricter requirements in the company. Again, the lack of incidents greatly affects these activities, but retrospectives are important to prepare for future incident handling.

Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness:
Which platform to share information on differs according to size and resources, but all companies mention at least one. Only one company is considering membership in KraftCERT, but this is not sought-after for the global or the largest company. Some of these have access to private CERTs. Also, the larger company seems less dependent on external resources, and the ones with access to global resources, lean more on these. The only platform where all is represented appears to be the CDS-forum. How much they share through this channel, and what is not specified by anyone. But, as sharing is a critical activity mentioned in all standards and many relevant sources, such as the DNV GL report about training [AS20b], this activity should be prioritized by all. The company size seems to affect their need to participate in such collaborations.

Public relations are managed and reputations repaired:
As the industry has yet to experience an incident on such a scale as Hydro, activities as managing public relations and repairing the organization's reputation were not brought up. But the companies worry about incidents that result in severe consequences, where public relations and reputation will most likely be affected. As one subject pointed out, a cybersecurity incident such as the attack towards Hydro could be a "company-killer." Having a focus on these activities could, therefore, be essential for increased preparedness.

Summary:
Many of the activities in the Respond and Recover functions do not seem to be prioritized by the industry, probably due to a lack of experience with cybersecurity incidents. It would be natural to expect that companies would regard Recover and Respond as more significant if cybersecurity incidents with greater consequences

were faced regularly.

5.2 Research Question 2

How can IT and OT work together to improve their cooperation for the future?

Our problem description stated that *"Overall, the goal of the thesis is to produce a united process both IT and OT in Norwegian oil and gas companies can utilize."* During the period when we conducted our interviews, we quickly realized that there might be too many differences between the two groups. A complete, united process for them both was not expedient. Variations such as priorities and frequency of attacks, speaks in favor that they also keep different processes. However, areas of improvement in regards to cooperation, responsibilities, and a shared understanding of when to include each other are discussed further in this chapter. The need for a completely united process is no longer a goal, but rather to highlight areas where a lack of cooperation has been identified.

And when an incident occurs, that includes both sides, a common understanding of the way forward needs to be established. For these cases, a united process should be followed. We believe that the first step for further cooperation should be to focus on the areas mentioned in this chapter. When these gaps are addressed, one can further move to look into the united cybersecurity incident management process.

5.2.1 Clear Definition of a Cybersecurity Incident

There were no consistencies in how to define an incident neither between companies or internally with IT and OT, as stated in Section 4.1.1. Only one company had corresponding answers between the IT and OT subjects, where both included intentional and unintentional events as possible cybersecurity incidents. The section includes quote nr. 4, which is the definition given by the OT employee. Later in the interview, examples about cases they have experienced are mentioned, but the subject mention that he would not necessarily call these events a cybersecurity incident, which is a deviation from the definition stated in the beginning. This inconsistency between what employees within a company would call an incident could lead to confusion about who to contact and how to move forward when something occurs later on.

Standards mentioned during the interviews define cybersecurity or information security incidents differently. Of the following standards: ISO/IEC 27000, IEC 62443, DNVGL-RP-G108, ISO/IEC 27035, *Guide to Industrial Control Systems (ICS) Security* and NOROG104, not all specify explicitly that both intentional and unintentional are included, but they do not exclude unintentional either [IEC13, IEC09, AS20c, SFS11, OA07].

Quote 11, in 4.1.2 shows how an unintentional event can have big consequences for production. As this was an unintentional incident, many of the participating companies would not, if they were to follow the definition they stated, categorize this as a cybersecurity incident. However, an incident as large as this, with consequences that went beyond loss of working hours, would probably be handled as such by all companies. Especially since safety is the main priority for all. IEC 62443 defines security as "prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation or inappropriate access to confidential information in IACS" [IEC09, p. 7]. Furthermore, a security violation is defined as an "act or event that disobeys or otherwise breaches security policy through an intrusion or **the actions of a well-meaning insider**" [IEC09, p. 24]. This definition clearly includes the unintentional incidents caused by an employee. DNV GL, which is based on IEC 62443, does not include this aspect in their report when they define cybersecurity and cyber threat.

ISO/IEC 27000 is a standard mainly mentioned by the IT employees we interviewed. Their official definition for an information security event and incident can be found in Section 2.1.1. *Guide to Industrial Control Systems (ICS) Security* has used the same definition for an event, and NOROG104 for an incident. Both these are targeted towards ICSs.

We contacted PSA, and asked them if they had a written definition of what they considered to be a cybersecurity incident. A search on their homepage gave no results. They replied that they do not have a formal definition, but utilize the following definition of when to report to the supervisory authorities: "situations where normal operations of control or safety systems are disrupted by unplanned work (ICT event)" [Pet19a, p. 17]. This is taken from the management regulations, paragraph 29, that the industry needs to comply with, and that PSA is delegated the authority to establish and enforce. As stated in the DNV GL report about training, even though ICT security events are not specifically mentioned, they are still covered by the regulations [AS20b]. While the paragraph does not specifically

mention attacks or unintentional incidents, previous examples have shown that an incident can affect the facility's integrity. As mentioned above, most of the standards also do not differentiate between intentional and unintentional but includes a definition that can cover both.

DNV GL writes that actors of the industry view PSA regulations as relevant only for OT [AS20c]. However, the trend is that the industry is taking a more holistic perspective of ICT security, which includes both IT and OT [AS20c]. We suggest that PSA should consider establishing a clear definition of what a cybersecurity incident is that the industry can utilize.

Without a clear understanding of what a cybersecurity incident is, how does a company keep a toll on how many incidents they experience? Some of the subjects stated that they had never experienced a cybersecurity incident at the OT side. The learning phase can be just as important after an intentional incident as an unintentional. Especially if a company does not encounter any attacks, they should work to learn from their internal experiences. As the employees are reluctant to define an event as a cybersecurity incident, they might also not use these as a learning opportunity.

Reaching a shared understanding of what a cybersecurity incident is, both within and possibly between companies, could increase awareness and make it easier for employees to categorize events. Two companies had their own way of categorizing, and whatever one chooses, it should be the same for both sides. With this definition in place, following plans and procedures could be easier. Some of the subjects we interviewed were almost afraid of adding more events to the category, saying that they did not really believe that this was an actual incident. But what is the harm in adding another event to the statistics? We believe that an open policy of what an event is and how many one experiences, might increase the company's overall awareness, and in the long run, could make the total number of events decrease.

5.2.2 Cybersecurity Roles and Responsibility

How cybersecurity responsibility is distributed differs between companies with access to global resources and those that are fully based on Norwegian soil. Role distribution seems to be quite similar for all and is mostly based on standard recruiting.

DNVGL-RP-G108 states that it is important to have a clear understanding of roles and responsibilities in order to ensure effective cybersecurity [AS17]. Furthermore, ISO/IEC 27035 and NIST CSF both include activities that covers the importance of defining roles and responsibility, and that users understand the roles and responsibilities they have [IEC16a, Mus14]. A clear understanding of who is responsible for the cybersecurity in what domain will benefit the organization in case of an incident. A written document that distributes responsibility is of no use if these roles are not properly followed.

There seems to be a miscommunication when it comes to the responsibility distribution in several companies, which should be solved as soon as possible. As written in Section 5.1.1, even though the written plans seem to be in place, the distribution is not as clear in practice. One company loses its roles and structure when they deal with larger incidents. Another has different answers from their two subjects. The IT employee states that he is responsible for information security in the whole company, and that OT is somewhat segmented, but that suppliers are responsible for delivering cybersecurity in their systems. While the OT employee states that he is left with the cybersecurity responsibility for the OT side. Responsibility should be clear to all, and these companies should, therefore, work on clarifying this internally. IT and OT should have a common understanding of each other's areas, and work together to ensure efficient cybersecurity, as recommended by DNVGL-RP-G108 [AS17].

Cybersecurity in OT is relatively new, while it has long been a focus for IT, meaning they have more experience and knowledge about the area. We do note, however, that some OT employees are quick to highlight that they have nothing to do with the IT domain. OT should make use of the knowledge of IT, and not increase the gap by looking at IT in this manner. Even though this is a relatively new field for OT, it has come to stay, and will just have increased focus for the years to come.

For those companies that have a global team to support them, they have national and regional roles, but as soon as an incident occurs, the global teams are notified. This gives them access to global knowledge of cybersecurity, which can be a significant advantage. But as one of them pointed out, one can easily rely too much on these global teams. This same company changed their roles to have more regional responsibility and highlights the need for local knowledge. The Norwegian cybersecurity in the ICS community is small, and sharing and participating in

these, even though one is backed up by a larger global community, will have a positive impact on the entire industry. The importance of sharing one's experiences is a key activity in all standards mentioned in Chapter 2, and is also recommended in the DNV GL report about training and exercise [AS20b].

One way of improving the clarity of roles and responsibilities is to increase the focus on training and exercising. DNV GL writes that "clarified responsibilities, good role understanding and well thought out routines are created through practical experience, exercises and reflection on one's own and others practices" [AS20b, p. 28]. Section 5.2.4 specifies how the industry should focus on training and exercising.

5.2.3 Cooperation

The majority of our subjects state that they do not have problems with the cooperation internally, but later examples might indicate otherwise. Cooperation exists in many different contexts and groups within a company, and it occurs in departments and across them to work towards a common goal. External cooperation is essential to keep up to date on what is going on elsewhere.

Answers from global companies can be affected by having a global team with a lot of the responsibility for handling larger cybersecurity incidents. When answering how the cooperation is between IT and OT, they may have based the response on global cooperation, meaning it can be satisfactory on a local level in Norway. However, this did not emerge from the interviews.

Internal Cooperation

The differences in prioritization affect the cooperation between IT and OT. All companies except one mention in some manner that challenges can be connected to the fact that the sides have different thoughts about the handling of a cybersecurity incident. The fact that they have different opinions on how to handle an incident is not that strange as the systems of IT and OT are different. One reason for why their priorities and background play a part in the cooperation is that IT and OT often have different environments and therefore have little to do with one another in daily life. As a result, there are few arenas where they can meet, discuss, and come to an agreement on issues. It is highlighted by one company that proper communication is essential as this makes employees aware of who they are and the responsibility they have. For companies where IT and are located internally,

establishing a centralized environment responsible for cybersecurity, could be a solution. This is mentioned as a positive way of working together, for instance, by industry A, see Section 4.2.1.

A common cybersecurity environment can encourage more sharing of knowledge between IT and OT. IT has a lot of domain knowledge, while OT is more recent in the field. By gathering them on common scenes, one promotes to learn and exploit one another's knowledge. Then IT can gain more understanding of OT, and vice versa.

Establishing a setting, such as joint meetings, were IT and OT can build human relations, ask questions, and discuss issues is recommended by a company where both employees are satisfied with the cooperation. For smaller companies that have put out parts of the handling or large parts of IT, joint meetings can be an option. These recommendations should not change the focuses of IT and OT. However, they can make it easier to cooperate and find mutual goals.

The emergency organization or team should include both IT and OT [AS20b]. Measure 4 in the DNV GL training and exercise report describes the need to have an emergency organization containing an ICT security team with both IT and industrial ICT resources [AS20b]. The measure implies that the IT and OT resources should be a part of the emergency organization, indicating that these should have more precise guidelines and be included to a more significant extent. An OT employee stated that he would like to be included in evaluations to the same degree that IT is when asked about the matter. In another case, a company gave OT more responsibility because they witnessed a need for their knowledge during an incident. DNV GL highlights that by fulfilling the measure, one will secure quick access to resources and strengthen the competence within the area [AS20b]. OT employees know the industrial control systems best, and IT the office systems. IT and OT have different priorities, to secure that the integrity of a facility is maintained and the other way around, both should have a place in the emergency organization. Therefore, we recommend that the next step is to include them both in the emergency organization and have them take part in the process from the beginning. This is a recommendation which also applies to companies that use suppliers for IT or OT, and global companies.

Since not all companies have experienced a lot of incidents, especially intentional, it is not easy to know how the collaboration will be. Therefore, performing

exercises should be considered necessary, as stated in the quote translated from Norwegian:

> Exercises are crucial to becoming good at crisis communication [AS20b, p. 28].

External Cooperation

"Fostering cooperation between private companies and between the public and private sectors is often mentioned as a silver-bullet solution for cybersecurity" [FMG18, p. 51]. When using suppliers a plan for cooperation is needed. The amount of cases where suppliers do not behave according to guidelines could indicate that the cooperation is not optimal. NIST CSF states that one can achieve a broader cybersecurity awareness by sharing information with external stakeholders, which includes customers, partners, and suppliers [Mus14]. It is easy to lean on suppliers to handle all their tasks and responsibilities for them without any involvement states one company. If an incidents occurs, the responsibility will lie at the system owner, not the supplier. Another issue is that suppliers may promise more than they keep. Therefore, to follow up and communicate with all suppliers is necessary. We find that creating a medium for communication, just as between IT and OT, with regular meetings could be a possible solution.

Sharing experiences with other companies and the authorities can have great value, which can be accomplished through membership in CERT or CSIRT or other available forums [AS20b]. DNV GL states that companies are exposed to many of the same threats and therefore need the same resources and support functions [AS20b]. Cooperation is appropriate and cost-effective through sharing knowledge and resources [AS20b]. Through membership in a CERT or CSIRT, companies can receive support in, for instance, surveillance, detection, and exercises [AS20b]. SINTEF recommends participation in CERT, specifically KraftCERT, which can be strengthened by establishing an oil ISAC as mentioned in 2.4, to gather knowledge [BHD+18]. As only one company stated that they have a CSIRT, it will not be furthered discussed. The interviews revealed that some companies rather have private CERTs or both participate in a public CERT and have a private. Companies that prioritize private ones are rather members of forums to cooperate with other companies.Gathering all at one CERT implies that companies that have internal ones also share their experiences and help others in the fight against cybersecurity attacks. There exists various CERTs. NUPI

informs that companies interviewed were not satisfied with the capabilities of NorCERT [FMG18]. Therefore, participating in KraftCERT, along with other industries, can be the best solution.

Summary

To establish strong cooperation both internally and externally, it is essential to secure the processes of companies. There exist areas of improvement in both. Creating a shared environment for IT and OT to cooperate more in the cybersecurity domain, making both participate in the emergency organization, communicating with suppliers, and participating in a common CERT, are all recommendations. We highlight that minimal experience in handling cybersecurity incidents can lead to uncertainties regarding communication that will not be fully adjusted with these. Knowing who to contact in various cases and such can be challenging. Exercising has been highlighted as a means to improve the cooperation both internally and externally, as in the quote below. This is further discussed in the next section.

> Stakeholders interviewed vary considerably in their perceptions of the cybersecurity challenges in their sector. However, all agree that exercises are essential for improving systems and cooperation to face the challenges and weaknesses involved in securing the petroleum sector [FMG18, p. 40].

5.2.4 Training and Exercises

Even though all companies stated that they do not exercise enough and that it will be a priority in the near future, few have a more specific timeline than "hopefully within the year." This can indicate that the companies do not have a plan for when to exercise. Only three of the companies interviewed have completed a large practical exercise that included all roles from the contingency plan. Standards such as IEC 62443 and ISO/IEC 27035 mention training as a key activity, but neither goes into detail of how one should train and how often. A report from the Norwegian Ministry of Justice and Public Security, *Risk in a Safe and Secure Society*, states the following:

> "Good decision making in a crisis requires experience, expertise and preparation in a wide range of areas. When the incident is major, it is

> important that lines of responsibility are clear, roles are understood and procedures are fully thought out. Such clarity comes from practical experience, training, exercises and reflection on our own practices and those of others. A crisis can present surprises and challenges that prove highly demanding. Another important quality is therefore mental preparedness, including an attitude in which the actors are conscious of and, as far as possible, prepared for the unknown and the unmanageable." [oJS16, p. 29]

DNV GL addresses how training and exercises are applied in safeguarding the ICT systems for the petroleum industry on the NCS [AS20b]. Furthermore, the report goes more into the depth of how the industry trains and exercises today and defines clear recommendations that should be followed for good practice. As stated in the quote above, experience is an essential factor in handling events later in the best possible way. None of the companies we interviewed have had intentional attacks towards their facilities that have resulted in any severe consequences. Unintentional attacks that have resulted in more significant consequences are barely mentioned. Training and exercises might be the industry's most important tool to prepare for future incidents, and therefore should be prioritized by the industry moving forward, as can be seen from the above quote by the Norwegian Ministry of Justice and Public Security.

Company-wide Awareness:

Awareness of cybersecurity is an important factor mentioned in many standards and frameworks, among them IEC 62443 and NIST CSF [IEC09, Mus14]. Increasing employees' awareness can be done in many ways. During the interviews, measures such as phishing campaigns, awareness campaigns, and participating in European Cyber Security Month are mentioned. These actions are company-wide and will have a positive impact. As these are measures that target all employees, it should be tailored to fit the different roles in the organizations in the best possible way [AS20b]. Both employees that work with the more administrative IT systems and the ICT systems should be included [AS20b]. One company mentioned that they are working on a course to cover cybersecurity in OT. Everyone in touch with an OT system will be required to take this course, to increase the awareness about cybersecurity in OT systems. One should consider extending this requirement to relevant IT personnel. NOROG104 has an ISBR concerning user training and awareness, which states that all personnel intending to access ICT systems must

receive training and be made aware of the possible threats [OA07]. We believe that giving such awareness training not only to OT, but also the relevant IT employees, can contribute to closing the gap between the two sides.

When asked about training, one company described in detail their onboarding process with two new employees. However, there was no mention of any further training than an introduction program over the first few months. It was explained that the employees are senior personnel with a lot of experience from before. As both systems and attacks are under constant development, one should have continuous awareness training also for key IT and OT personnel [OA07]. It is possible to divide up these programs based on experience, but the experience should not be used as an excuse for not prioritizing continuous training. Some companies mention that they have a document describing each role and the corresponding workflow. These documents could include how each employee is expected to incorporate training in their work routine.

Tabletops:

Tabletops are a more theoretical way of training, that can be cost-saving compared to a full-on, practical exercise, all while still being effective [RD15]. All companies mention tabletops as a type of theoretical exercise they have executed.

DNV GL points out that tabletops are a great way of training, but that all parts of the contingency plan need to be included [AS20b]. While both IT and OT can conduct individual tabletops, it could be hugely beneficial to plan one that includes both. They may need to cooperate in the event of an incident and should be familiar with each other beforehand. Also mentioned in the DNV GL report is the importance of working with the top management to increase awareness in all stages, for instance, by using tabletops. Only one of the participating companies stated that they have carried out such tabletops.

Furthermore, some of the subjects mentioned that they had used real-life attacks as an opportunity to learn. Hydro is mentioned as an example by one, where they sat down and discussed questions such as "how would we have handled this?" and "do we need to make any changes to be able to handle similar attacks in the future?". Adjustments were made to their plans accordingly. These attacks can be an excellent opportunity to have a tabletop where you can save time planning a scenario. However, it is essential to not focus too much on these attacks, but also focus on scenarios tailor-made to your own company. Industry A conducts risk

analysis, and then use this to create a scenario, a solution they are satisfied with. One smaller company has contracts with several third party suppliers. For this company, tabletop scenarios, including suppliers, might be more relevant than the Hydro attack.

How often these tabletops are conducted were not specified, except for one subject that believes they do it every other month. DNV GL writes in their report that between three to five exercises should be performed yearly, with different themes and personnel included in each [AS20b]. The time needed to plan an exercise can vary between days and months. It is essential to set aside the correct amount of resources and time required, especially to work needed for evaluating and implementing changes in the aftermath [fCP16]. It is our opinion that a carefully planned exercise can give more to the organization than two that are not sufficiently followed up. Furthermore, to cover all functions of the NIST CSF, one should set aside the time needed to have a minimum of three exercises, such as tabletops each year. Exercises target towards top management and similar groups should be outside of these three.

Practical Exercises:

The benefits of carrying out an actual exercise, both small and large, should not be underestimated. As stated by the Ministry of Justice and Public Security, a crisis can lead to stress, be full of surprises, and not least be demanding for the employees [oJS16]. Theoretical exercises can locate areas that should be improved. However, it is the practical exercises that require mental preparedness and allocates deficiencies that would otherwise not be discovered before it is too late [oJS16]. The results of a tabletop can give input to what type of practical exercises should be carried out. Companies can perform both large and small exercises as these can have different areas of application.

Smaller exercises provide the opportunity to focus on specific parts of the emergency response, which have been identified as essential to master real cybersecurity incidents [RD15]. By limiting the extent of an exercise, it is possible to reduce the number of resources utilized since only the relevant personnel will be asked to contribute. These smaller exercises could especially be valuable for companies with limited resources. There exist many versions of small exercises that can be of interest. Field exercises are proposed by the Norwegian Water Resources and Energy Directorate [RD15]. An example of a field exercise, as one company stated,

is to test that it is possible to get the critical systems back up. The assurance is accomplished by personnel at the facility by testing the relevant systems. Further, several subjects stated that they have backups in place as a part of the Protect function in Section 5.1. With this in mind, it seems that companies have realized the opportunities for performing small exercises.

When asked about recommendations for other companies in the sector, one subject expressed the value of focusing on building up exercises. He believes one should gain control of the smaller exercises, and as you become more confident in managing the smaller ones, you can expand. Working in this manner, one can possibly secure that the communication is maintained at all levels and that the structure does not regress.

To gain control over the whole process, larger exercises, including all relevant parties, are essential to complete yearly [AS20b], even though not all companies have carried out such exercises. One subject emphasized that they carried out a large exercise, although some felt the company was not quite ready for such an extensive exercise. It turned out to locate several areas of improvement. The exercise was not conducted perfectly, but as it is only an exercise, it is not meant to be either. The main goal is to discover misconceptions about, for instance, the plans and other discrepancies between plans and actions. The appropriate changes can then be made so that the organization is better prepared than they were before exercising. Based on this, a recommendation from us is that companies perform exercises even if they do not feel completely ready. Further, it is not possible to prepare for all incidents, but executing enough exercises can influence the final result.

It is not to be expected that companies have neither the time nor the opportunity to perform more than one larger exercise per year since larger exercises can require 6 to 18 months of planning [fCP16]. To not complete more than one yearly goes against the recommendation of PSA [AS20b]. The fact that two companies have not carried out such large exercises demonstrate that these exercises have not been a focus for the time being.

Independent of the amount and size of exercises companies carry out, IT has had a broader focus on exercises than OT. Several companies highlight that IT has completed more exercises. A natural reason for this may be that IT, as previously mentioned, has worked with cybersecurity for a longer period than OT and,

therefore, may have had more time to prepare for and execute exercises. Further, it can be related to the roles included in the emergency response organization since they are, to a large extent, responsible for planning and executing exercises.

An essential task of exercising is planning for it. When planing an exercise, one needs to decide on specific goals [AS20b]. These should define why the exercise will be conducted and set up the scenario. It is important to determine the most critical scenarios and practice parts of the scenarios [AS20b]. Relevant actors must be informed and given the opportunity to prepare [fCP16].

It is mentioned by several OT employees that they are only invited to participate in the execution of exercises, not necessarily the planning. If one is to carry out larger exercises, it can be essential to involve OT personnel in the planning and goal setting in advance. OT has control over its systems, employees, and may have insight that goes beyond that of IT and the emergency response team.

All exercises that have been carried out by our subjects was informed of ahead of time. This can be advantageous since they allow personnel to prepare, such that all know their roles and tasks [AS20b]. The next stage, after a few large exercises, can be to carry out red team exercises. In these cases, personnel is not informed of the exercise beforehand, which affects the execution and result [AS20b]. By keeping the exercise hidden, one will observe the employees in a more real-life situation [AS20b]. Red team exercises can test the efficiency of preparedness processes and the personnel connected to them [AS20b]. Keeping exercises hidden and letting employees believe they are under attack can be a valuable next stage of performing exercises when one has gained control over regular, larger exercises. DNV GL recommends that red team exercises are conducted [AS20b].

General Recommendations:

It is important to follow up on both exercises and incidents and change plans and documents according to the experiences. Most companies point out that they should get better at implementing changes as a result of an exercise or incident. This retrospective should include both IT and OT, as one OT employee pointed out, they should be included more. The decision if OT is to be included or not, is described by several organizations as it is taken by either the IT side or by the emergency response teams. Not all of these teams have a representative from the OT side.

As one company states, one needs to set aside the necessary time and money and really put training and exercises on the agenda. DNV GL recommends making a plan for the next two to three years, with a complete overview of the exercises and training that the company will cover [AS20b]. This can help those in charge to get a full picture of which exercises to plan and to whom.

Those companies that explain the exercises they have had, also mention that they invited PSA. The available resources such as PSA, NSM and similar, should be included when deemed necessary. Other relevant resources are specified in the DNV GL report [AS20b]. While organizations in the same industry compete in the same market, sharing experiences about how to train and exercise can result in a positive outcome for all, particularly since all organizations face similar threats from outside attackers [AS20b].

5.3 Research Question 3

With a focus on IT and OT, what can the oil and gas industry learn about the cybersecurity incident management process from other critical infrastructures?

The two interviews with Industry A and B, shows that the challenges they are facing are similar to those from the oil and gas industry. Getting an overview and understanding of the cybersecurity incident one is facing is mentioned as the main challenge for Industry A and most oil and gas companies. While Industry B struggles to define what a cybersecurity incident is clearly.

Industry A seems to have come further than the rest, with a higher focus on training, exercises, and a centralized unit that includes both IT and OT. These areas stand out relative to the oil and gas industry and will be discussed below.

5.3.1 Centralized IT and OT Environment

Industry A has a centralized environment, consisting of both IT and OT, in charge of cybersecurity, and is satisfied with their joint department. Further, they seem to be overall gathered in their opinions. For instance, they have a mutual understanding of what a cybersecurity incident is. Industry B is a different case; they do not have a joint or composite environment for handling cybersecurity incidents. Further, there is less cooperation between IT and OT, and no common definition of cybersecurity incidents, as we see it. As mentioned at the beginning of Chapter 4, the industry is under reconstruction. As a result, their cybersecurity

structure, among other things, may change. However, both industries find more cooperation between IT and OT to be practical and worth investing in. As stated by one of the subjects from Industry A, IT and OT will become much stronger if they work together. It can be deduced from a DNV GL report that the separate environments should pool their resources and competence [AS20b].

Creating a united environment for IT and OT is also supported by one OT employee from the oil industry. The employee recommends that all companies, that have internal resources and roles for both IT and OT, should centralize the environments. One reason is that it is difficult to find enough resources to have two separate environments. These arguments, together with the good experience of Industry A, could indicate that this is an approach the oil and gas industry should explore. Therefore, we will recommend that companies look at the possibility of establishing a centralized environment consisting of IT and OT.

5.3.2 Awareness, Training, and Exercises

Both Industry A and B seems to have a high focus on training, along with self-study with free reigns and continuous work to keep employees updated on the latest technology. This is in contrast to one of the oil companies, who mostly had training for new employees. While Industry B does not have any requirements for what should be learned and attended, they seem to have an open environment for employees to explore and learn. The cross-training that Industry A favors, can help the IT and OT to work better as a whole.

Industry A has done a lot more extensive training than both Industry B and the oil and gas companies. They have a clear plan for when to exercise and includes relevant roles when necessary. In contrast to the oil and gas industry, which do regard training as an important factor, but does not seem to have a plan in place.

In Industry B, they had a CEO that was conscious of the importance of cybersecurity. Awareness at the top management level is an important activity in, for instance ISO/IEC 27035 [IEC16a], and the subject expresses that their section really benefited from the CEOs awareness. A higher focus on cybersecurity awareness at the top management level is therefore recommended by us.

The importance of continuous awareness is highlighted by Industry B, where focus during one month is not seen as enough to carry throughout the year. This is especially clear as they experienced an incident that was a result of a possible

phishing-mail. As can be seen in quote 28, their employees did not believe they would experience another similar incident. This incident lasted over a longer period of time, and our interview subject wanted to do a retrospective session in the aftermath. This was not completed, and as our subject pointed out, it should be prioritized after the next incident. Many standards highlight the importance of learning from an incident, among them the ISO/IEC 27035 and NIST CSF. Both Industry B and the oil and, as companies, should prioritize this moving forward.

5.3.3 Summary

To summarize, these two industries share a lot of common factors with the oil and gas industry. Being a possible candidate for cooperation actually enlarges the pool of resources that is available. As the cybersecurity environment in Norway is small, one should be positive to cooperate across critical infrastructures.

Before interviewing the last industries, we believed that the oil and gas industry was not in the front line when it comes to IT/OT incorporation, but that the energy sector was. Since the company we included in this thesis, is in the midst of a reconstruction, a generalized conclusion cannot be drawn about the industry. But our interviews indicate that Industry A has come the furthest, with the rest following behind.

5.4 Limitations

As this thesis was restricted to a narrow time frame, this influences our overall results. Several factors may have affected our finished results.

We have little experience with interviewing. Small differences in wording, and the fact that we shared the responsibility for the interviews, can have affected the acquired results. We wanted to both gain experience with interviewing and tried to stay aware of how our behaviors were.

Even though we felt that we covered a lot of ground with our interview guide, the participants have their own interpretation of the questions asked. This will affect the finished results. For instance: a question that asks about internal plans will receive different answers from each subject, as they will reply with what they remember. As a result, even though one subject might not mention having a disaster recovery plan in place, it does not necessarily mean the company does not have one. However, we have chosen to include the answers we were given and not

speculate if the answers do not cover everything an organization has implemented. If only two companies mention having a specific plan, whether or not the three others have a similar one are not relevant.

As stated many times by our subjects, few, larger cybersecurity incidents have hit the oil and gas industry in Norway up to this point. Therefore, as the subjects do not have a lot of experience in the field, some of their thoughts are based on assumptions. Nonetheless, those that work in the industry and with cybersecurity in these areas are in the best position to tell how they would handle future incidents, meaning their assumptions are still of interest. Sharing experience across companies and industries is nevertheless an essential part of learning, as highlighted many times by our sources and us throughout this thesis.

Our interviews were conducted in Norwegian, which was natural since both us and our subjects have this as our first language. But the thesis is written in English. All quotes are therefore translated to the best of our abilities. Misinterpretations from both us, and by the translation, can have affected the results. When choosing which quotes to include, we re-listened to the audiotapes again, to make sure the wording was correct. This was done to minimize the possibilities of misinterpretation, but it cannot be removed completely.

The interview between IT and OT of one company had several weeks in between. A lot seems to have happened in the company between these two interviews, but we chose to include both nonetheless. We believed that the relationship between IT and OT would probably not have been drastically changed over those weeks, even though some plans had been established and changes were made from the first to the second interview.

Chapter 6
Conclusion

In this thesis, we have examined how five oil and gas companies of various sizes handle cybersecurity incident management today, focusing on two groups: IT and OT. We have also studied the processes of two companies from different industries to find areas the oil and gas industry can learn from. This chapter will provide a conclusion for the thesis and our research questions.

RQ1: How is the current cybersecurity incident management process in industrial ICT systems?

For the first research question, our interviews show that all companies focus mainly on the functions before a cybersecurity incident occurs and implementing preventative measures. Few companies invest in the functions belonging to after an incident. As the industry has yet to experience cybersecurity incidents of a larger scale, this may be a natural progression. However, a couple sees the need for more investment in the later functions, meaning Respond and Recover will most likely have a broader focus moving forward.

RQ2: How can IT and OT work together to improve their cooperation for the future?

Chapter 5 has four subsections that we believe should be of focus for IT and OT moving forward. This includes a clearer definition of a cybersecurity incident (5.2.1), defined responsibilities (5.2.2), more focus on cooperation (5.2.3) and lastly, a greater focus on training and exercises, (5.2.4). IT and OT are two different groups with different priorities. OT expresses that ICSs have rarely been targeted and experienced incidents as of today. Since the potential outcome

of a cybersecurity incident could be fatal, they need to increase their focus on larger exercises and be better prepared. The two groups should have a common cybersecurity incident plan for incidents that touch both areas. OT should also include IT in their plans, as they have knowledge that should be utilized.

RQ3: With a focus on IT and OT, what can the oil and gas industry learn about the cybersecurity incident management process from other critical infrastructures?

Finally, for the third research question, similarities in experiences show that oil and gas companies have the opportunity to learn from other companies in critical infrastructure. The industries we included had positive experiences related to a centralized IT and OT environment. One of them has had a higher focus on training and highlights the importance of the lessons learned phase. All participating companies can be related to critical infrastructure, and as they have expressed a lot of similar challenges and goals, oil and gas companies should take the opportunity to share experiences across critical infrastructures.

To summarize, this paper discusses how oil and gas companies should prioritize to better face the threats of the future. Additionally, our research shows that the area of IT and OT can be further explored in many ways. How the recommendations of this paper will affect the industry's preparedness, along with a higher focus on cooperation and a common environment, are areas that could be of interest to research further.

References

[AS17] DNV GL AS. Cyber security in the oil and gas industry based on iec 62443. Available at: http://rules.dnvgl.com/docs/pdf/DNVGL/RP/2017-09/DNVGL-RP-G108.pdf, 2017. Accessed: 10 March 2020.

[AS19] DNV GL AS. A test of resilience - the outlook for the oil and gas industry in 2019. Available at: https://industryoutlook.dnvgl.com/2019, 22 January 2019. Accessed: 8 November 2019.

[AS20a] DNV GL AS. Cyber security sus og egensikre komponenter, kommunikasjonsprotokoller. Available at: https://www.ptil.no/contentassets/fbde8c6d6b9d4ff7afb8188aadb96a62/dnv-gl---cyber-security-sis.pdf, 2020. Accessed: 18 March 2020.

[AS20b] DNV GL AS. Ikt-sikkerhet - robusthet i petroleumssektoren. trening og Øvelse. Available at: https://www.ptil.no/contentassets/fbde8c6d6b9d4ff7afb8188aadb96a62/dnv-gl---trening-og-ovelse.pdf, 2020. Accessed: 18 March 2020.

[AS20c] DNV GL AS. Regelverk og tilsynsmetodikk. Available at: https://www.ptil.no/contentassets/fbde8c6d6b9d4ff7afb8188aadb96a62/dnv-gl---regelverk-og-tilsynsmetodikk.pdf, 24 February 2020. Accessed: 19 March 2020.

[BHD+18] L. Bodsberg, B. Hale, Ø. Dahl, T. O. Grøtan, M. G. Jaatun, M. Moe, and T. Onshus. Kunnskapsprosjekt ikt-sikkerhet; industrielle kontroll- og sikkerhets- systemer i petroleumsvirksomheten. Available at: https://www.ptil.no/contentassets/d67ffa5187c846fe9a074d1e68f2ce1c/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf, 29 May 2018. Accessed: 13 October 2019.

[Del17] Deloitte. An integrated approach to combat cyber risk: Securing industrial operations in oil and gas. Available at: https:

//www2.deloitte.com/global/en/pages/energy-and-resources/articles/integrated-approach-combat-cyber-risk-energy.html, 2017. Accessed: December 19 2019.

[Dra19] Dragos. Global oil and gas cyber threat perspective: Assessing the threats, risks, and activity groups affecting the global oil and gas industry. Available at: https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf, August 2019. Accessed: 28 September 2019.

[Equ17a] Equinor. Digitalisation driving value creation. Available at: https://www.equinor.com/en/news/digitalisation-driving-value-creation.html, 22 May 2017. Accessed: 8 November 2019.

[Equ17b] Equinor. Norway's first platform to be remotely-operated from land. Available at: https://www.equinor.com/en/news/09nov2017-valemon-remote.html, 9 November 2017. Accessed: 8 November 2019.

[Equ18] Equinor. The equinor book. Available at: https://www.equinor.com/en/how-and-why/health--safety-and-security.html, 2018. Accessed: 8 November 2019.

[fCP16] The Norwegian Directorate for Civil Protection. Veileder i planlegging, gjennomføring og evaluering av øvelser - grunnbok. Available at: https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/grunnbok_oving.pdf, 2016. Accessed: 4 May 2020.

[FEMnd] Homeland Secuirty FEMA. Is-870 - dams sector: Crisis management overview course. Available at: https://emilms.fema.gov/IS870/DCM01summary.htm, n.d. Accessed: 31 May 2020.

[FMG18] Karsten Friis, Lilly Pijnenburg Muller, and Lars Gjesvik. Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector. *NUPI Report*, 2018.

[fsobD12] Direktoratet for samfunnssikkerhet og beredskap (DSB). Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring. Available at: https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf, 2012. Accessed: 11 June 2020.

[Hyd19] Norsk Hydro. Cyber-attack on hydro. Available at: https://www.hydro.com/en/media/on-the-agenda/cyber-attack/, 14 November 2019. Accessed: 13 February 2020.

[IEC09] IEC. Iec 62443: Industrial communication networks - network and system security - part 1-1: Terminology, concepts and models. 2009.

[IEC13] IEC. Iec 62443: Industrial communication networks - network and system security - part 3-3: System security requirements and security levels. 2013.

[IEC16a] IEC. Iec 27035: Information technology - security techniques - information security incident management - part 1: Principles of incident management. 2016.

[IEC16b] IEC. Iec 27035: Information technology - security techniques - information security incident management - part 2: Guidelines to plan and prepare for incident response. 2016.

[IEC18] IEC. Iec 27000: Information technology - security techniques - information security management systems - overview and vocabulary. 2018.

[KPCBH15] Siwar Kriaa, Ludovic Pietre-Cambacedes, Marc Bouissou, and Yoran Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety*, 139:156–178, 2015.

[Lei16] Leidos. Definitive guide to cybersecurity for the oil gas industry. Available at: https://www.ciosummits.com/Online_Assets_Leidos_Definitive_Guide_to_Cyber_for_Oil_and_Gas_eBook.pdf, 2016. Accessed: 10 February 2020.

[LSC19] Elena Lisova, Irfan Sljivo, and Aida Causevic. Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal*, 13(3):2189–2200, Sep. 2019.

[McA] McAfee. What is stuxnet? Available at: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html. Accessed: 20 October 2019.

[McAte] McAfee. What is petya and notpetya ransomware? Available at: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/petya.html, no date. Accessed: 14 February 2020.

[Mus14] S. Mustard. The nist cybersecurity framework. *InTech*, 61(1-2), 2014.

[NIS19] NIST. Nist cybersecurity framework resources. Available at: https://www.nist.gov/cyberframework/resources, 2019. Accessed: 23 May 2020.

[NSM19] NSM. Nsm norcert. Available at: https://www.nsm.stat.no/om-nsm/tjenester/nasjonalt-cybersikkerhetssenter-ncsc/nsm-norcert/, 23 August 2019. Accessed: 4 March 2020.

[OA07] Norwegian Oil and Gas Association. 104 – norwegian oil and gas recommended guidelines on information security baseline requirements for process control, safety and support ict systems. 2007.

[Oat05] Briony J Oates. *Researching information systems and computing*. Sage, 2005.

[oB17] Det Kongelige Justis og Beredskapsdepartement. Meld. st. 38(2016 –2017) ikt-sikkerhet: Et felles ansvar. Available at: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf, 22 June 2017. Accessed: 13 October 2019.

[oJS16] Norwegian Ministry of Justice and Public Security. Meld. st. 10 (2016–2017). report to the storting (white paper). risk in a safe and secure society. Available at: https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/en-gb/sved/stm201620170010000engpdfs.pdf, 2016. Accessed: 3 May 2020.

[Pet19a] Petroleumstilsynet. Guideline regaring the management regulations. Available at: https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_veiledning20_e.pdf, 18 December 2019. Accessed: 29 April 2020.

[Pet19b] Petroleumstilsynet. The government's revenues. Available at: https://www.norskpetroleum.no/en/economy/governments-revenues/, 2019. Accessed: 26 September 2019.

[RD15] The Norwegian Water Resources and Energy Directorate. Øvelser - en veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen. Available at: http://publikasjoner.nve.no/rapport/2015/rapport2015_39.pdf, 2015. Accessed: 4 May 2020.

[RML16] Tim Conway Robert M. Lee, Michael J. Assante. Analysis of the cyber attack on the ukrainian power grid defense use case. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, 2016. Accessed: 10 February 2020.

[Rob11] Colin Robson. *Real World Research*. John Wiley & Sons, 3th ed. edition, 2011.

[RV19] Thea Svenkerud Rydjord and Ingrid Sørdal Volden. Cyber security incident management process in industrial ict systems. Project report in TTM4502, Department of Information Security and Communication Technology, NTNU – Norwegian University of Science and Technology, Dec. 2019.

[sfi19] Norsk senter for informasjonsskring. Alle kan rammes av løsepengevirus. Available at: https://norsis.no/jhfkjsdhfkjhsdkfjhskhfk/, 1 April 2019. Accessed: 13 February 2020.

[SFS11] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[Tjo17] Aksel Hagen Tjora. *Kvalitative forskningsmetoder i praksis*. Gyldendal akademisk, Oslo, 3th ed. edition, 2017.

[Yin09] Robert K. Yin. *Case study research : design and methods*, volume vol. 5 of *Applied social research methods series*. Sage, Thousand Oaks, Calif, 4th ed. edition, 2009.

Appendix A
Quotes from the Interviews

This table shows all quotes included in the thesis in its original language. Each quote has been given a number, that corresponds to the number in a parenthesis behind the quote in the thesis.

# Quote nr.	Quote
1	“Folk kan ha forskjellig oppfatning da! Til og med mellom meg og *navn* vil det være forskjellig oppfatning om hvem som er, hvem som gjør hva til hvilken tid.”
2	"De sitter jo med mye mindre, hvis du sammenligner med en sånn systemeier på et, på en plattform for eksempel, på kontrollsystem, så har jo han åpenbart mye mindre cybersikkerhetskompetanse enn *navn* som sitter med det tilsvarende på *plattform*. De sitter kanskje med budsjettene og muligheten til å påvirke ting, men de sitter jo og med retten til å nedprioritere cybersikkerhet i forhold til kontrollsystem ting, så det er jo et åpenbart dilemma her."
3	"Det er IT som har det overordnede ansvaret for å sy dette i hop, sånn at man presenterer et totalbilde innen forbi cyber. Så er det vi som leverer, skal sørge for at det blir levert inn fra OT-biten(...)."
4	"Ja, det er vel egentlig enhver, enten tilsiktet eller utilsiktet hendelse som ikke er en del av det som er avtalt bruk av systemet."

5	“(...) det er egentlig bare to angrep som bekymrer meg. Det ene er typisk det som traff Hydro, målrettet angrep der angriperen forsøker å ødelegge så mye som mulig. (...) Den andre er angrep på anlegg, der angriperen har som mål å tukle med kontrollsystemer. (...) er at de er de eneste som jeg vil si er en “company-killer”. Absolutt alle andre angrep klarer vi å overleve selskapet, men det som traff Hydro kan jo ta livet av et selskap.”
6	"Jeg er ikke så bekymret for det vi ser, at folk er inne og forstyrrer en PC eller noe sånt noe, det ser vi. Og da har likevel kontroll. Men de som er usynlige, som gjør endringer som gjør at det endrer funksjonalitet, som gjør at vi tror vi er trygge, det er det verste."
7	"Det endret litt på beredskapsplanene våre. Nå er det sånn at når det skjer noe så skal vi også stille opp fra OT siden."
8	"Det er klart at et olje og gass selskap har veldig lang erfaring i håndtering av hendelser generelt. Det som er nytt er nok det å få cyber security hendelser inn i samme fold som alle andre hendelser som et sånt selskap jobber med."
9	"Vi er et ungt selskap og et lite selskap, allikevel så vil det være naivt å tro at vi er skånt og at vi ikke er i siktet hos enkelte aktører. "
10	"Det er hele tiden forsøk på å lamme våre systemer."
11	"Vi har faktisks stengt ned en plattform ved at noen gjorde en feil. Da satte dem sikkerhetssystemene ut av spill og vi var nødt til å stenge ned. (...) det blir litt som en øvelse, så heldigvis ingen stor dramatikk, men det er klart at det går timevis å få en hel plattform ned og timevis å få den opp igjen. (...) Og det er ikke billig kan jeg love deg!"
12	“Forhåpentligvis fokuserer vi på alle fasene, men der vi som de fleste andre selskaper har investert mest opp igjennom er på det som skjer før et angrep (...).”

13	“De tas i utgangspunktet bare på IT siden. Det er ikke noe systematikk for å involvere OT i det.”
14	"Samarbeidet blir bedre og bedre, det er det ikke noen som helst tvil om. Vi får mer og mer respekt for hverandre og vi blir mer og mer avhengig av hverandre."
15	"Så det er ikke noe “oss” og “dem”. Det er bare vi. "
16	“ (...) så vil vi jo aldri oppdage det før noe hadde begynt å gå galt, før de begynte å modifisere kontrollsystemet. Skal ikke tro vi har noe sjans på sånne zero-day type målrettede angrep.”
17	"(...) men det hadde vært et helt annet tempo hvis det hadde vært alvor."
18	"Og da er det en felles innsats med de som er etablert og har prosesser ut mot ledelse, myndigheter, forsikringer, nasjonale institusjoner som Petroleumstilsynet, (...) og andre parter(...) Også sørger vi for at vi har rett kompetanse som stiller opp for å komplementere de som sitter i beredskap, for de kan ikke noe om den digitale verden sånn som de kan. "
19	"En ting er å håndtere det en har oppdaget, det en ser, det en vet. Men det er jo sannsynlig at det er mye annet rundt som en ikke har oppdaget helt ennå."
20	“For vi har jo ikke hatt så mye hendelser eller gjort så mye øvinger. Vi antar en del ting.”
21	"Vi kan jo gjøre alt mulig sikkert mye, mye bedre, men... Vi tror jo at det vi gjør er kanskje godt nok, men det vet vi jo ikke."
22	"Så det er et tips jeg ville gitt: outsource det, men outsource det til noen du stoler på."
23	“Også tror jeg at de som håndterer hendelser må være klar over at det er forskjell på IT og OT. Det er helt andre konsekvenser å ta ned et system på et anlegg enn det er på kontornettet.”

24	"De trenger jo ikke å gjøre noe galt, de kan også bare ikke gjøre noe riktig."
25	"Jeg mener, og kommer alltid til å mene at hvis du er god på forebyggende side, så vil det være mindre og mindre og mindre å gjøre på hendelsessiden."
26	"Jeg er en forkjemper for å rive ned de barrikadene der og fjerne de siloene. Vi sitter i samme båt. Og vi har klart forskjellige erfaring, forskjellig kunnskap, men sammen så blir vi mye sterkere (...) Her handler det om å forene krefter og kunnskapen, for en IT-teknolog, kan vi kalle det, har mye å hente fra OT-miljøet og omvendt. Og spesielt i sikkerhetsperspektiv tenker jeg."
27	"(...) for å få til å gjøre en god jobb så trenger du oppdatert kompetanse på det området du jobber med og tilstøtende områder."
28	"(...) noen internt som tror at “det var det året vi fikk oppleve et angrep”. Jeg tror ikke vi kan tenke sånn. Vi må hele tiden være forberedt på neste."

Appendix B
Research Application

Following is the research application sent to NSD.

NSD NORSK SENTER FOR FORSKNINGSDATA

Meldeskjema 132414

Sist oppdatert

12.02.2020

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Type opplysninger

Du har svart ja til at du skal behandle bakgrunnsopplysninger, beskriv hvilke

Vi har behov for å vite arbeidssted og stillingen til hvert intervjuobjekt.

Skal du behandle særlige kategorier personopplysninger eller personopplysninger om straffedommer eller lovovertredelser?

Nei

Prosjektinformasjon

Prosjekttittel

Cyber Security Incident Management in Industrial ICT-Systems

Begrunn behovet for å behandle personopplysningene

For å følge opp de ulike intervjuobjektene trenger vi å lagre navn og e-postadresse til alle intervjuene er fullført. Vi ønsker å lagre telefonnummer for å enklere komme i kontakt med hvert enkelt intervjuobjekt. Informasjon om hvilke stillinger objektene har er nødvendig da vi skal skille på de ulike ansvarsområdene og vil intervjue flere personer med ulike stillinger fra samme bedrift. Bedriftene og personene vil bli anonymisert i oppgaven. All data vil bli sletted ved prosjektslutt.

Ekstern finansiering

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Thea Svenkerud Rydjord, [redacted]

Behandlingsansvar

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet NTNU / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Maria Bartnes, [redacted]

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?

Nei

Utvalg 1

Beskriv utvalget

IT-sikkerhetsansvarlig innenfor et utvalg oljeselskaper og en annen bransje.

Rekruttering eller trekking av utvalget

Rekrutteringen vil skje ved at en av våre veiledere vil kontakte de relevante selskapene og spørre om de ønsker å delta i studien. Dersom de som kontaktes ikke har stillingene vi ser etter, vil vi be om å bli satt i kontakt med de som har de konkrete stillingene, eller tilsvarende. Personene som vil bli kontaktet vil i utgangspunktet tilhøre veilederne sine nettverk, men det kan hende vi blir nødt til å kontakte noen selv. Vi vil i såfall sende mail til bedrifter vi er interessert i å intervjue.

Alder

18 - 67

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Utvalg 2

Beskriv utvalget

Kontrollromsoperatør innenfor et utvalg oljeselskaper og en annen bransje.

Rekruttering eller trekking av utvalget

Rekrutteringen vil skje ved at en av våre veiledere vil kontakte de relevante selskapene og spørre om de ønsker å delta i studien. Dersom de som kontaktes ikke har stillingene vi ser etter, vil vi be om å bli satt i kontakt med de som har de konkrete stillingene, eller tilsvarende. Personene som vil bli kontaktet vil i utgangspunktet tilhøre veilederne sine nettverk, men det kan hende vi blir nødt til å kontakte noen selv. Vi vil i såfall sende mail til bedrifter vi er interessert i å intervjue.

Alder

18 - 67

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 2

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 2?

Personlig intervju

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Informasjon for utvalg 2

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Utvalg 3

Beskriv utvalget

Systemansvarlig innenfor et utvalg oljeselskaper og en annen bransje.

Rekruttering eller trekking av utvalget

Rekrutteringen vil skje ved at en av våre veiledere vil kontakte de relevante selskapene og spørre om de ønsker å delta i studien. Dersom de som kontaktes ikke har stillingene vi ser etter, vil vi be om å bli satt i kontakt med de som har de konkrete stillingene, eller tilsvarende. Personene som vil bli kontaktet vil i utgangspunktet tilhøre veilederne sine nettverk, men det kan hende vi blir nødt til å kontakte noen selv. Vi vil i såfall sende mail til bedrifter vi er interessert i å intervjue.

Alder

18 - 67

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 3

- Navn (også ved signatur/samtykke)
- Adresse eller telefonnummer
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 3?

Personlig intervju

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Informasjon for utvalg 3

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?

Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Manuelt (papir)
- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Ved å ta kontakt på mail eller via telefon og spesifisere at man ønsker å trekke seg.

Hvordan kan de registrerte få innsyn, rettet eller slettet opplysninger om seg selv?

Etter å ha transkribert intervjuene vil vi sende de over til intervjuobjektene. De vil da få mulighet til å gå over og samtykke, eventuelt rette eller slette opplysninger om seg selv.

Totalt antall registrerte i prosjektet

1-99

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?

Behandling

Hvor behandles opplysningene?

- Maskinvare tilhørende behandlingsansvarlig institusjon
- Mobile enheter tilhørende behandlingsansvarlig institusjon

Hvem behandler/har tilgang til opplysningene?

- Student (studentprosjekt)
- Prosjektansvarlig
- Databehandler
- Eksterne medarbeidere/samarbeidspartnere innenfor EU/EØS

Hvilken databehandler har tilgang til opplysningene?

NTNU Onedrive.

Tilgjengeliggjøres opplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?

Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (kodenøkkel)?

Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Opplysningene anonymiseres
- opplysningene krypteres under lagring

Varighet

Prosjektperiode

15.01.2020 - 10.06.2020

Skal data med personopplysninger oppbevares utover prosjektperioden?

Nei, data vil bli oppbevart uten personopplysninger (anonymisering)

Hvilke anonymiseringstiltak vil bli foretatt?

- Lyd- eller bildeopptak slettes
- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?

Nei

Tilleggsopplysninger

Appendix C
Research Approval

NSD approved our application to begin our study and collect sensitive data as long as the requirements we planned to implement were followed. The answer to the application presented in Appendix B is shown below.

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Cyber Security Incident Management in Industrial ICT-Systems

Referansenummer

132414

Registrert

04.02.2020 av Thea Svenkerud Rydjord [redacted]

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet NTNU / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Maria Bartnes, [redacted]

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Thea Svenkerud Rydjord [redacted]

Prosjektperiode

15.01.2020 - 10.06.2020

Status

13.02.2020 - Vurdert

Vurdering (1)

13.02.2020 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet den 13.02.2020 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:
https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 10.06.2020.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).
NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Microsoft OneDrive er databehandler i prosjektet. NSD legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Kontaktperson hos NSD: Simon Gogl
Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Appendix D
Information Sheet

In this appendix the information sheet that was sent out to each of the participants is presented. It is written in Norwegian as all participating workers were Norwegian.

Vil du delta i forskningsprosjektet

”Cyber Security Incident Management in Industrial ICT-Systems”?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge hvordan oljebransjen håndterer cybersikkerhetshendelser og legge frem et forslag til en forent prosess for hendelseshåndtering. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Dette er en masteroppgave som utføres av to studenter fra Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU. I masteroppgaven vil vi kartlegge hvordan to grupper ansatte, en som driver med IT-sikkerhet (IT) og en som er ansvarlig for operasjonell sikkerhet (OT), håndterer cybersikkerhetshendelser. Kartleggingen vil foregå gjennom å intervjue ansatte innenfor de to gruppene. Målet er å foreslå en forent prosess for hendelseshåndtering som kan tas i bruk av begge grupper. Gjennom intervjuer vil vi også undersøke en annen bransje med likhetstrekk innenfor integrert bruk av IT-komponenter i kontrollsystemer og et fokus på sikkerhet. Målet er å se om oljebransjen kan lære noe av en denne bransjes erfaringer.

Studien vil bygge på forskningsspørsmålene:

- Hvordan håndteres sikkerhetsbrudd i industrielle kontrollsystemer, og hvordan kan prosesser innenfor IT og OT forenes?
- Med fokus på å forene prosesser for IT og OT, hva kan olje- og gassindustrien lære av andre bransjer som har vært gjennom en periode med digitalisering og møtt på lignende utfordringer?

Det første forskningsspørsmålet vil vi forsøke å besvare gjennom intervjuer med ansatte i olje- og gassindustrien og ett litteraturstudie. Det andre forskningsspørsmålet vil vi svare på gjennom intervjuer med ansatte i en annen bransje som allerede har vært gjennom en tilsvarende periode med digitalisering, slik den olje- og gassbransjen opplever. Basert på de svarene vi innhenter vil vi forsøke å legge frem et forslag til en forent prosess som kan være av nytte for både OT og IT for håndtering av cybersikkerhetshendelser.

Hvem er ansvarlig for forskningsprosjektet?
NTNU er ansvarlig for prosjektet og veiledes av SINTEF.

Hvorfor får du spørsmål om å delta?
For å samle inn nok data om hvordan bedrifter, håndterer cybersikkerhetsangrep i dag trenger vi at ansatte innenfor bransjene deltar i studien, og deler sine erfaringer og vurderinger innenfor feltet. Vi ønsker å intervjue ca. 3 ansatte fra 4 ulike bedrifter, 3 bedrifter innenfor oljeindustrien og den siste innenfor en annen bransje.

Hva innebærer det for deg å delta?
Dersom du velger å delta i studien, vil dette innebære deltakelse gjennom et til to intervjuer. Intervjuet vil vare i ca. 1 time. Opplysninger vi er interessert i til det første intervjuet omhandler stilling, arbeidsoppgaver og tilknytning til cybersikkerhetsmiljøet. Videre vil vi stille noen generelle spørsmål om hvordan bedriften arbeider med cybersikkerhet og dine erfaringer. Det andre intervjuet vil være fokusert rundt å hente inn tilbakemeldinger fra deg om forslaget vi legger frem.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Det er masterstudentene, Thea Svenkerud Rydjord og Ingrid Sørdal Volden, som vil gjennomføre intervjuene og ha tilgang til all data. Deler kan likevel bli diskutert ansvarlig professor Maria Bartnes, førsteamanuensis II ved NTNU og Forskningssjef i SINTEF Digital og veilederne Lars Bodsberg, Senior Research Scientist i SINTEF og Roy Thomas Selbæk Myhre, Avdelingsleder Network & Security i TietoEVRY. Vi vil registrere din stilling og arbeidsoppgaver, personidentifiserende data vil bli lagret i form av lydopptak. Opptak, notater og eventuelle andre dokumenter som inneholder sensitive opplysninger vil bli oppbevart og behandlet konfidensielt på NTNU. For å anonymisere deg vil du, og bedriften du tilhører, bli registrert med et anonymt identifikasjonsnummer.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes 10. juni. Lydopptak og anonymisert data tilknyttet intervjuene vil bli permanent slettet ved prosjektslutt.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU og SINTEF har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
- NTNU – Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved
  - Maria Bartnes, faglærer og tilhører NTNU og SINTEF [redacted]
  - Thea Svenkerud Rydjord [redacted]
  - Ingrid Sørdal Volden [redacted]
- Vårt personvernombud: Thomas Helgesen [redacted]
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlige

Maria Bartnes Thea Svenkerud Rydjord Ingrid Sørdal Volden

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet Cyber Security Incident Management in Industrial ICT-Systems og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju der lydopptaker benyttes.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 10. juni.

(Signert av prosjektdeltaker, dato)

Appendix E
Interview Guide

Here follows the interview guide.

Intervjuguide

Cyber Security Incident Management Response in Industrial ICT-Systems

Thea Svenkerud Rydjord og Ingrid Sørdal Volden

I forbindelse med vår masteroppgave, vil vi kartlegge hvordan to grupper ansatte i oljebransjen har håndtert sikkerhetshendelser, men tanke på integrert bruk av IT-komponenter i tradisjonelle kontrollsystemer. Målet er å kartlegge hvordan de ulike gruppene gjør det, for å kunne foreslå en forent prosess begge grupper kan bruke. Vi skal skrive en masteroppgave basert på denne datainnsamlingen. Intervjuene vil gjennomføres ansikt-til-ansikt eller via videokonferanse. Alle svar behandles med full fortrolighet og vil anonymiseres. Resultatene skal ikke være sporbare tilbake til enkeltpersoner eller bedrifter som deltar, og all data vil slettes når oppgaven leveres.

Forskningsspørsmål:
Gjennom masteroppgaven håper vi å kunne svare på følgende forskningsspørsmål:

- Hvordan håndteres sikkerhetshendelser i industrielle kontrollsystemer, og hvordan kan IT forenes med OT?

Intervjuobjekter:
Vi håper på å intervjue rundt tre ulike roller, fra tre ulike bedrifter:

- IT-sikkerhetsansvarlig
- Kontrollromsoperatør
- Systemansvarlig

Meldeplikt:
Vi ønsker å ta lydopptak av intervjuene, og må derfor melde denne studien til Norsk Samfunnsvitenskapelig Datatjeneste - NSD.

Intro til intervju
Takk for at du vil delta i denne intervjuprosessen. Vi håper at resultatene vil være til nytte for deg og din arbeidsgiver.

Hvem er vi:

- To masterstudenter fra Kommunikasjonsteknologi, NTNU i Trondheim.

Hvilke type sikkerhetshendelser vi er interessert i (cyber)

- I denne studien er vi kun interessert i cyber-sikkerhetshendelser.

Mål:
Målet vårt med intervjuprosessen er å kartlegge hvordan cyber-sikkerhetshendelser blir håndtert i dag innenfor både OT og IT sektoren. Derfor vil vi intervjue ansatte med ansvarsområde innenfor disse to. Intervjuene vil bli analysert og resultatet vil bli brukt til å legge frem et forslag til en samlet prosess for hendelseshåndtering.

Spørsmål

Innledning

1. Hvor mange ansatte er det i selskapet?
2. Kan du fortelle litt om din stilling og hva du jobber med/arbeidsoppgaver?
    a. Hva en din rolle i forbindelse med cyber sikkerhet?
    b. Hvor lenge har du hatt denne stillingen?
3. Har økt bruk av ny teknologi endret din arbeidshverdag?
    a. Hva slags endringer har dette medført for deg og selskapet?

Hoveddel

1. Hvem er ansvarlig for cybersikkerhet? (roller)
    a. Hvordan blir disse rollene utdelt?
    b. Får de ansvarlige opplæring? Hva slags?
2. Hva legger du i ordet cyber sikkerhetshendelser?
    a. Hvor ofte blir dere utsatt for cyber sikkerhetshendelser?
    b. Hva er en typisk cyber sikkerhetshendelser?
    c. Hvis sjeldent/aldri:
        i. Hva tror du er grunnen til det?
3. Hvilke cyber sikkerhetshendelser er dere bekymret for?
    a. Er IT- og OT-avdelingene oppmerksom på hvordan tilgang/uautorisert tilgang i motsatt system kan påvirke egne systemer? F.eks: tilgang til kontrollsystemene, gjennom IT-systemene.
4. En hendelse har et tidsperspektiv som kan deles inn i før, under og etter at hendelsen har skjedd. Hvilken fase fokuserer dere på og hvorfor?
    a. Hvor mener du at fokuset burde ligge?
5. Har du selv opplevd en cyber sikkerhetshendelse?
    a. Har dere opplevd både målrettet og vilkårlige angrep?
    b. Dersom ja målrettet:

        i. Hvilke systemer var angrepet rettet mot?
    c. Dersom ja vilkårlig:
        i. Gå videre til Ja under.

Hvis Ja på spm 4:

d. Hvordan oppdaget dere hendelsen?
e. Hva var konsekvensene av hendelsen?
f.
    i. Hvor fort oppdaget man den? Hvor fort reagerte dere?
g. Hva ville du gjort annerledes i dag? (Forbedringsområder)
h. Har denne hendelsen endret måten dere jobber på?

Hvis ”Nei” på spm 4:

6. Hvilke planer har dere for hvordan dere håndterer sikkerhetshendelser?
    a. Hvor ofte revideres planen deres?
7. Hvilke tiltak har dere gjort for å beskytte dere mot cyber sikkerhetshendelser?
    a. Hvorfor har dere valgt akkurat disse tiltakene?
    b. Har dere trent på dette? Hvordan? Hvor ofte?
        i. Hvem inkluderes i treningen?
    c. Har dere hindret sikkerhetshendelser ved hjelp tiltakene deres?
8. Hvilke forsvarsmekanismer har dere for å oppdage hendelser? (IDS, logger, overvåkning, osv)
    a. Følger dere med på disse mekanismene?
    b. Har dere oppdaget/stanset sikkerhetshendelser ved hjelp av disse forsvarsmekanismene?
9. Man må anta at noen er istand til å komme gjennom barrierekontrollen. Hva gjør dere når dere **oppdager** sikkerhetshendelser? (rett etter)
    a. Hvor lang tid går det før dere har en respons på plass?
    b. Hvilke prioriteringer gjør dere? (availability vs confidentiality)
    c. Hvem er ansvarlig for hendelsesløpet i etterkant?
    d. Har dere trent på dette scenarioet?

Generelt:

10. Opplever dere utfordringer med samarbeidet internt i forbindelse med sikkerhetshendelser?
    a. Hva slags utfordringer opplever dere? (terminologi, kunnskap, bakgrunn, osv)
11. Hva gjør dere i etterkant av et sikkerhetshendelser? (i senere tid)
    a. Hva slags samarbeid har dere med eksterne/interne? (bransjeforum, CERT)
    b. Hvordan bruker dere erfaringene fra en hendelse videre?
    c. Gjør dere noen forskjell i arbeidet i etterkant, basert på om dere har håndtert en hendelse bra eller dårlig? Hvilke forskjeller er dette?
12. Følger dere noen rammeverk/standarder?
    a. I så fall, hvilke?
    b. Hvor lenge har dere brukt de?
    c. Hvis interne rammeverk

i. Hvem utvikler de?
ii. Hva er de basert på?
iii. Hvor ofte revideres de?

Forbedringsområder og samarbeid:

1. Har dere noen gode rutiner du vil anbefale til andre? Kan du fortelle oss litt om disse?
2. Hva synes du er vanskeligst når det kommer til å håndtere sikkerhetshendelser?
3. Finnes det forbedringsmuligheter til hvordan dere håndterer sikkerhetshendelser?

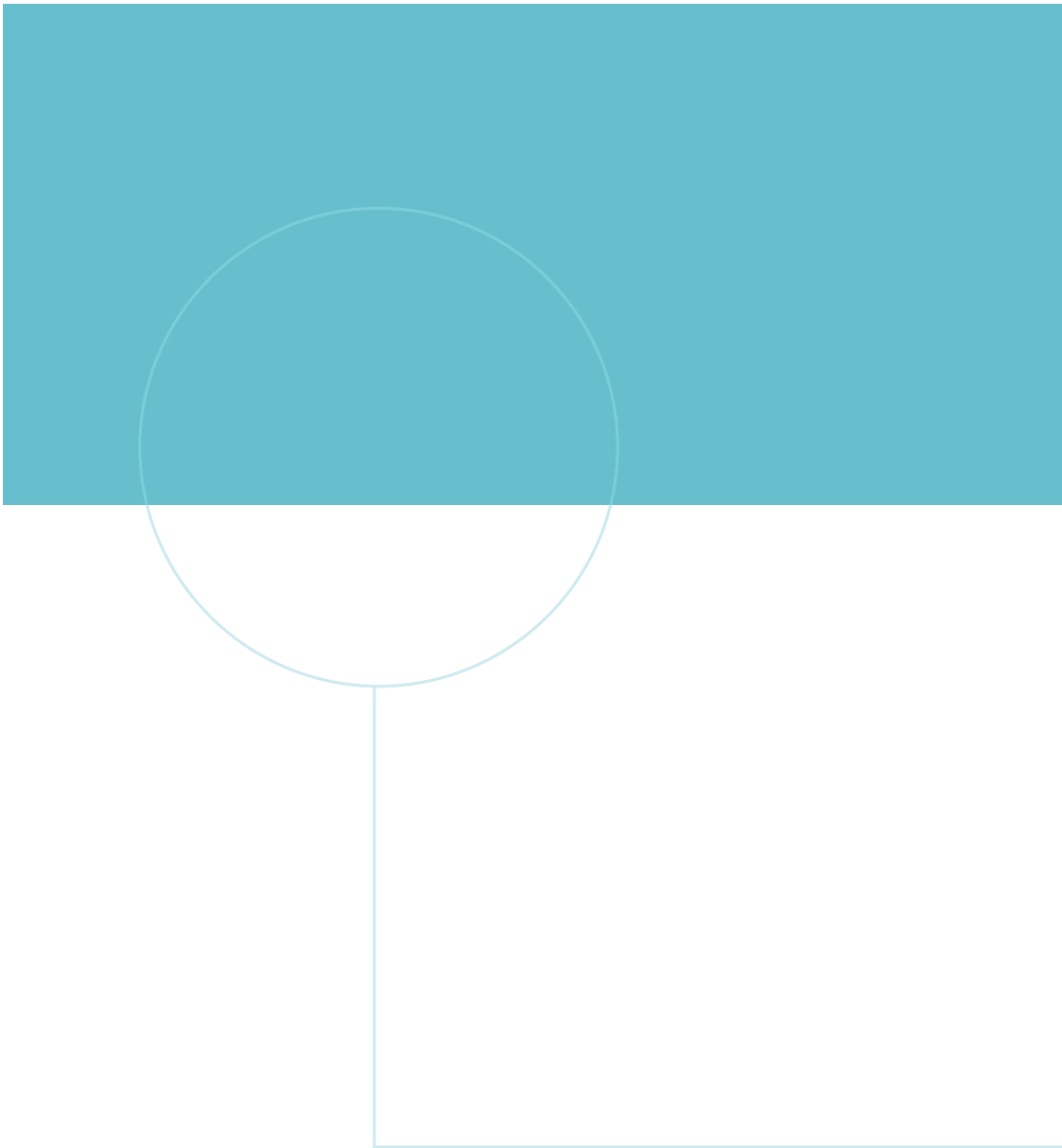
Avslutning:

1. Er det noe du selv ønsker å tilføye?

Takker for deltagelse og spør om det er greit at vi kommer med oppfølgingsspørsmål i etterkant.

Notis til intervju:

Be om forklaring av ord og uttrykk som brukes for å sikre at alle intervjuobjektene og vi har samme forståelse.



NTNU

Norwegian University of
Science and Technology