University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/Specialization: MSc Societal safety	Spring semester, 2021 Open
Writer: Mathiassen, Caroline Midtlien	…………………………………………… (Writer's signature)

Faculty supervisor:
Petersen, Karen Lund

Thesis title:

"A study of the organizational aspects of cyber threat management in an ICT-company"

Credits (ECTS): 30

Key words: Societal safety, societal security, critical infrastructure, ICT-infrastructure, ICT-security, cyber threats, wicked problems, networking, knowledge sharing, resilience, high reliability organisations, awareness culture, information and communication technology	**Pages:** 120 **+ enclosures:** 4 Stavanger, 15/06/2021

MSc Societal safety
Department of Safety, Economics and Planning
Faculty of Science and Technology
University of Stavanger

"A study of the organizational aspects of cyber threat management in an ICT-company"

By: Caroline Midtlien Mathiassen

June 2021

Abstract

This master thesis is an explorative study of organizational aspects of cyber threat management in a private ICT-company. The study has sought to address the theoretical concepts of critical infrastructure, wicked problems and resilience in order to answer the problem statement: *"How do private ICT-suppliers perceive and define their role in protecting critical infrastructure?"*

I have studied a single case, a private ICT-company entitled XX, to answer the chosen problem statement. The chosen method was a qualitative method with the use of data triangulation of interviews, survey and document analysis. The purpose was to understand organisational aspects of cyber threat management. My role was to understand what was meaningful for the actors at the blunt end (top-level management) and the sharp end (employees at technical and operational level). The application of abductive logic was chosen to answer the research questions of this thesis. The actor's "world" was interpreted by me based on their knowledge and understanding of how things are, which is applicable to the epistemological constructionism approach. Analysis was conducted using themed questions for coding purposes.

The main analytical take away is that in the case of XX, they perceive and define their role as being a critical supplier of cyber security to their customers. Making sure their customers can operate fully, XX perceives themselves as a contributing factor to national security. Still, the company is not prioritizing protection of national security in their company strategies.

I conclude that, in the case of XX, they are having a broad and traditional understanding of cyber threats which results in a few internal misunderstandings on how to manage the cyber threats. How the company perceive their societal responsibility is reflected internally on how they organise their own security. Based on the main contradictions, the company inhabits different types of uncertainty that needs to be managed for the company to be more resilient and to fully be able to be perceived as a high reliability organisation. They also need to prioritize the use of networking societies and knowledge sharing to broaden how the internal organisation perceive cyber threats.

In the case of XX, they construct themselves as a private company with a traditional risk-adaptation. But show instead a combination of risk- and uncertainty-adaptation, which illustrate that the company in practice have a resilience management approach. With the

existing focus of uncertainty on operational and tactical level, in the case of XX, they should be able to measure resilience. This is something the company need to pinpoint in the organisation and the adaptation needs to be strategically incorporated at top-level management. A resilience-adaptation is dependent on how the top-level management will go about to measure accurate resilience and uncertainty in the organisation.

Table of contents

Tables of figures and tables

Figures

Tables

Terminology

Term	Definition
Societal security	*"…to look ahead and develop and operate systems and activities that will avoid accidents and meet the functional requirements that have been set"* (Njå, Sommer, Rake, & Braut, 2020, p. 136)
Critical infrastructure	*"Social structures and technical systems and facilities that are necessary to maintain or restore societies critical functions"* (Njå, Sommer, Rake, & Braut, 2020, p. 140) or *"… technological systems that deliver solutions and services of great importance to society"* (2016, p. 138).
Information Communication Technology	*"…Critical infrastructures that rely wholly or in part on Information technology"* (Jaatun, 2015, p. 28)
Technology	*"…material objects, techniques and knowledge that give us humans opportunities to change and control the material world"* (Engen, et al., 2016, p. 138)
Digital security	*"…protection of "all" that is vulnerable because it is connected with or dependent of information- and communication technology (ICT)"* (Bergsjø, Windvik, & Øverlier, 2020, p. 1)
Wicked problems	*"…poorly formulated, boundary-spanning, ill-structured issues with numerous stakeholders who bring different perspectives to the definitions and potential resolution of the issue or problem. […] each issue can be seen as a symptom of others, each issue is unique, no definitive solutions are possible, and there is no "stopping rule" that determines the problem's end or is likely to satisfy all the stakeholders"* (Waddock, Meszoely, Waddell, & Dentoni, 2015, p. 996)
Uncertainty	*"…the possibility of occurrence (uncertainty)"* (Renn, 2008, p. 2)
Crisis	*"…something bad threatens a person, group, organization, culture, society, or, when we think really big, the world at large. Something must be done, urgently, to make sure that this threat will not materialize"* (Boin, Hart, Stern, & Sundelius, 2016, p. 3)
Creeping crisis	*"…a threat to widely shared societal values or life-sustaining systems that evolves over time and space, is foreshadowed by precursor events, subject to varying degrees of political and/or societal attention, and impartially or insufficiently addressed by authorities"* (Boin, Ekengren, & Rhinard, 2020, p. 10)
Vulnerabilities	*"…the conditions under which operational disruptions with negative consequences or serious incidents may occur"* (Engen, et al., 2016, p. 139)
Tight coupling	*"…is a mechanical term meaning there is no slack or buffer or give between two items. What happens in one directly affects what happens in the other"* (Perrow, 1999, p. 90).

Networking society	*"…high degree of dynamics and border crossing activities so that the existing institutional frameworks are unable to handle or may even limit the handling of societal problems that spring from this. In addition to the nature and the solutions of problems becoming more difficult to determine, the complexity of how the problems is handled is also a result of the inevitable involvement of other parties and the complexity of the involved institutional arrangements"* (Koppenjan & Klijn, 2004, pp. 10-11)
Complex interactions	*"…unknown sequences, or non-planned or unexpected sequences, that are either non-visible or not possible to understand"* (Njå, Sommer, Rake, & Braut, 2020, p. 131).
Resilience	*"…to focus on the capacity of systems to adapt, reorganize and recover from disruption and disturbance"* (Zio, 2018a, September, p. 20)
High Reliability Organisation	*"…a perspective and approach that describes characteristics of organisations with high complexity and tight couplings that experience extraordinarily few accidents, despite the assumption that such systems […] cannot be satisfactorily controlled in the long run"* (Haavik, Antonsen, Rosness, & Hale, 2019, p. 481).

Abbreviations

ICT	*Information Communication Technology*
GDPR	*General Data Protection Regulation*
HSEQ	*Health (Safety, Environment), Security, Ethics & Quality*
NSM	*Norwegian National Security Authority*
NCSC (previously NorCert)	*Norwegian National Cyber Security Centre*
Cert	*Cyber Emergency Response Team*
ISMS	*Information Security Management System*
ISO	*International Standard Organization*
KPI	*Key Performance Indicators*
OWASP	*Open Web Application Security Project*
HRO	*High Reliability Organisation*
CAB	*Change Advisory Board*
SAB	*Security Advisory Board*

Preface

This thesis marks the completion of a post-graduate degree in Societal Safety at the University of Stavanger. I decided in 2017 to study one of my personal interests: Societal Safety and Security. While working in a fulltime job I managed to finish after four busy years. It has been a long journey, but so fulfilling and worth it.

…To my dear supervisor, Karen Lund Petersen, who kept me motivated from day one and provided me with valuable feedback until the last minute.

…To my employer who let me write about them.

…To the interview and survey participants who provided insight and valuable knowledge about the company.

…To my beloved husband for supporting me through thick and thin.

…To my dog, Pax, for keeping me with company.

Thank you so much for your contributions!

Caroline Midtlien Mathiassen
Sandnes, June 2021

1. Introduction

We constantly hear about new cyber-attacks conducted by foreign states or non-state actors against critical infrastructure, by exploiting vulnerabilities in information- and communication technology (ICT). As the world gets increasingly more digital, critical infrastructure rely on digital security and the requirements and expectations increase for those who protect the systems and business critical information.

According to the Norwegian Security Authority (NSM, 2019), software, hardware, protocols, algorithms, value chains, organizations, routines and the people involved, all have vulnerabilities. As the work intensifies to identify and eliminate deviations and vulnerabilities, new threats appear and assets are at stake. The following sectors are especially exposed to cyber threats: defence, space, maritime, medical research, oil, gas, and energy. In addition to gather business critical information and espionage, foreign states also seek to influence decision processes in state ownership, cooperation, and trade (NSM, 2019, p. 15).

Cybercrime can, according to the Norwegian Directorate for Societal Safety (DSB), be defined as *"criminal offenses committed in the exploitation of information technology"* (DSB, 2015). Cyber-attacks are intentional malicious events conducted with the purpose to cause harm, information-gathering or to create a launchpad for a future cyber-attack. In the annual National Crisis scenario analysis conducted by DSB (2019) , cyber-attacks are considered to be on the list of the biggest threats against our society today. A challenge applicable to all sectors is that digital vulnerabilities are difficult to identify and manage. Value chains are long and complicated, and deviations in one part of the chain can cause immediate and critical consequences in other parts of the value chain. DSB pinpoints that it is necessary to not only protect business critical information, but to protect the systems itself and by this ensure the protection of national security (DSB, 2019).

In December 2015 successful cyber-attacks infiltrated three Ukrainian energy companies causing physical damage to electrical grids resulting in loss of power for over two hundred thousand citizens. The malicious actors used emails as an entry point into the control systems. They disabled communication channels and changed security measures which prevented the energy companies from addressing the blackout to the general population. This resulted in panic and a weakened level of trust towards public infrastructure and the government's ability to protect their citizens. One year later a second cyber-attack infiltrated a power station causing power outage of one fifth of Kiev’s electrical power. This time over one hundred thousand citizens lost their power (Newbill, 2019, p. 773) (Fischer & Lehnhoff, 2019).

Most of the cyberattacks conducted is network based and exploit how computer systems are linked in a global network (DSB, 2019, p. 197). There are especially two recent examples to illustrate this statement:

In December 2020 it was reported that SolarWinds, a large US based ICT-company, was a victim of a cyberattack in as early as January 2020. The cyberattack was not detected until several months later and by that time the threat had already spread to their customers. This included the US Government (Pentagon and different departments), Microsoft, Cisco, Intel and Deloitte. The four latter is well known suppliers of ICT-services to other ICT-companies and critical infrastructures. The intention seemed to be espionage on private companies and the US government. The hackers added malicious code to SolarWinds software system “Orion” and when an automatic update was sent to their customers the malicious code was included. The code made it possible to breach companies’ ICT-systems through a backdoor so that they could install even more malware used for spying and stealing of information (Jibilian & Canales, 2021). This attack also affected the Norwegian Oil fund and NCSC have additionally indicated that several governmental and private companies was affected (Langved & Kibar, 2021).

The most recent cyberattack was made possible through a security hole affecting over hundreds of thousands of Microsoft Exchange servers worldwide (Gundersen & Grut, 2021). Those affected had local email servers, or their ICT-supplier did not utilise a cloud solution for the email servers (Sterud, 2021). In Norway, the Microsoft Exchange hackers breached the Norwegian Parliament, a municipality, university college and public transportation companies (Sterud, 2021).

The increase in sophisticated hacking groups increases the possibility that other vulnerable institutions can be attacked, such as small organizations and companies, schools and local governments. It is argued that this cyber-attack and hacking campaign was greater in the number of victims than the cyberattack of SolarWinds (O'Neill, 2021) (Sterud, 2021). This illustrates that malicious threat agents are increasingly more sophisticated and resourceful and that their networks are expanding aggressively and rapidly. Which further poses an increased threat to the protection of national security.

1.1 Problem statement and research questions

Digital services and products used by the public sector, along with its critical digital security, is mainly developed, owned and operated by private companies. This is supported in the Norwegian National cyber security strategy where it is stated that *"... decisions related to the development of - and security in – cyberspace is made by commercial, non-state actors, i.e., outside the conventional intergovernmental arenas. As a result, the role of the authorities in the development of cyberspace is limited, which in turn calls for an extensive public-private partnership"* (Norwegian Ministeries, 2019, p. 9). The private sectors engagement in the protection of our critical infrastructure is considered crucial to national security. It would be interesting to find out how the private companies, especially ICT-companies, understands their role and their responsibility towards protection of critical infrastructure.

The problem statement of this thesis is as follows:

> *"How do private ICT-suppliers perceive and define their role in protecting critical infrastructure?"*

With the aim of answering the problem statement of this thesis, the following research questions are raised:

1. How are ICT-suppliers affected by cyber threats?
2. How does ICT-suppliers perceive their societal responsibility in the protection of national security?
3. Does ICT-suppliers have a conscious relationship towards resilience in their work to protect ICT-infrastructure and manage wicked problems?

1.2 Disposition

The next chapter of this thesis will consist of an elaboration of the chosen theoretical aspects and introduce previous research relevant to answer my research questions. The three key aspects of this thesis are *critical infrastructure*, *wicked problems* and *networking*, as well as *resilience*. Chapter 3 will be used to explain the methodological choices and assessments for data collection, in addition to analytical tools and techniques used to interpret collected data. In chapter 4 the empirical data and empirical results will be presented. The empirical results will be analysed in chapter 5 up against the chosen key theoretical aspects. This thesis will end with a short summary and a concluding comment in chapter 6.

2. Theory - Problem statement strategy

This chapter identifies key theoretical aspects necessary to answer the chosen problem statement. Based on the research questions, this thesis seeks to elaborate the chosen theoretical aspects and introduce previous research relevant to answer them. The chosen main theoretical aspects in this thesis relates to academic debates about critical infrastructures, wicked problems and resilience.

First, I will introduce the theoretical aspects and previous research on *critical infrastructure*. It is especially important to address the debate related to the different use of terms within this theoretical aspect. Theoreticians have different opinions related to the use of the term *critical infrastructures* and how it can be applied, this debate is highlighted in the second section. It is necessary to narrow down the topic as critical infrastructure can consist of several different functions, systems and components. I have chosen to focus mainly on *Information Communication Technology (ICT)* infrastructures, which are crucial for several critical infrastructures to operate continuously (DSB, 2016, p. 110).

To narrow down the topic of critical infrastructures and ICT, a view on one of the biggest malicious type of threats towards ICT-infrastructures is essential. I perceive cyber threats as a type of *wicked problem.* I will elaborate on the theory related to wicked problems and how *networking and knowledge sharing* can be a solution for private companies to manage these problems. Previous research and ongoing debate on the theoretical concepts of wicked problems and networking and knowledge sharing will be put in relation to ICT-infrastructure and cyber threats.

Finally, an elaboration of previous and current theoretical debates related to *resilience* and *resilience management.* I perceive these concepts as a strategy to manage wicked problems. Theoretical aspects of *High Reliability Organisations (HROs)* are elaborated. The theoretical debate will be put in relation to private companies who operate and/or supply ICT-services.

The elaboration of the theoretical concepts mentioned above will be used as a problem statement strategy and the theoretical disposition as illustrated on the next page, in figure 1.

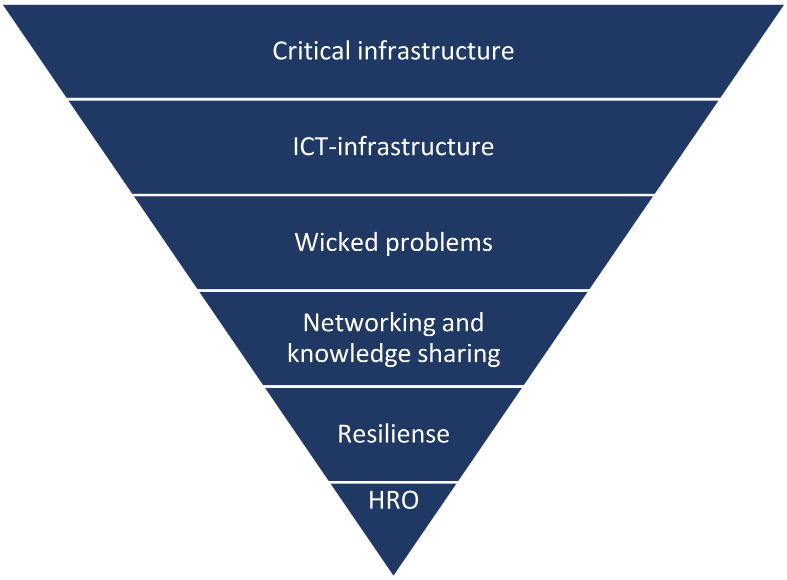

Figure 1 Theoretical disposition

I will begin by introducing the chosen theory of this thesis, followed by an elaboration of the theoretical concepts.

2.1 Choice of theory

Research about *critical infrastructures* is extensive and demands the need of limitation to what is relevant to answer the problem statement of the thesis. I mainly emphasise theoretical aspects presented in the academic books by Njå et. Al (2020) and Engen et. Al (2016) in the section about critical infrastructure. Insight from Colleen Newbill (2019) and Enrico Zio (2018a, September) is used to provide additional perspective of critical infrastructure. As there is a broad variety of what types of infrastructures is viewed as critical. There are also different views on what critical infrastructure means and involves. This is addressed by Weick, Sutcliffe and Obstfeld’s (2008) adaptation of Perrow’s (1999) Normal Accident Theory and the use of complex interactions and tight coupling in High Reliability Organization theory.

Research about *ICT-infrastructure* is mainly about protection of power grids, development of smart cities and political strategies. I mainly emphasise Martin G. Jaatun (2015), Engen et. Al (2016), Julian Jang-Jaccard and Surya Nepal (2014) in regards to ICT-infrastructure, digital security and different types of threats. N. MacDonnell Ulsch (2014), Enrico Zio (2018a, September), Bergsjø et. Al (2020), Goessling-Reisemann and Thier (2019) and Sissel H. Jore

(2019) provide additional context to the concepts addressed. Research about *cyber threats* is consists mainly of technical research and computer science. There is available research in the field, but this is limited to organisations usually defined as HROs, like sectors operating within petroleum, aviation and nuclear power.

There is limited availability on research about organizational management of cyber threats as *wicked problems* in private ICT-companies that own, supply and operate ICT-infrastructure. While there is extensive amount of research on wicked problems. I mainly emphasize Engen et. Al (2016), Waddock et. Al (2015) and Koppenjan and Klijn (2004) on the concept of wicked problems. Boin et. Al (2020) provides knowledge on the concepts of *crisis*, *creeping crisis* and *crisis management*. Rittel and Webber (1973), Renn (2008), Newbill (2019), Ulsch (2014) and Fischer and Lehnhoff (2019) provides additional context to the concepts addressed.

The amount of research about *networking and knowledge sharing* to manage wicked problems is increasing in academia. Especially in areas such as crisis management of transboundary and wicked problems. I emphasize the aspects on networking societies as addressed by Koppenjan and Klijn (2004) and Alastair Stark (2014). Waddock et. Al (2015) address the importance of collaboration between organization and being part of something bigger than themselves. Olsen and Kruke (2011) introduces the concepts of the blunt and sharp end in organizations, which are terms I use to describe management and employees in this thesis. Lægreid and Rykkja (2019) address networking in relation to wicked problems. Boin et. Al (2020), Engen et. Al (2016) and Newbill (2019) provide additional context.

Academic literature on *resilience* is dominated by research on typical HROs such as the oil and gas, aviation and nuclear power. Goessling-Reisemann (2016) and co-authors w/Thier (2019), w/Ruth (2019) address resilience as an approach to manage complex systems and problems. Shaw and Maythorne (2013) emphasize the use of resilience as a planning approach and provides a *resilience discourse*. Supported by Colding, Barthel and Sörqvist (2019). The concept of HRO is briefly introduced in the section about critical infrastructure, but it will be fully introduced in the last section about resilience and HRO. There is limited research on ICT-companies as HROs, but it is possible to draw similarities to other sectors. I emphasize the theoretical view of *HRO* by Haavik et. Al (2019), Engen et. Al (2016), Boin et. Al's (2016) crisis management perspective and Weick (2001), co-authors w/Sutcliffe (2015) and w/Sutcliffe and Obstfeld (2008) perspective on HRO. These academics provide additional context to the concepts: Njå et. Al (2020), Lægreid and Rykkja (2019), Waddock et. Al (2015), Reason (1997), Zio (2018a, September) and Stephen Flynn (2018b, September).

The literature review shows that there is extensive research on the terms alone, but limited research about some of the chosen main theoretical concepts in relation to each other. The theoretical concepts will be elaborated in the following sections.

2.2 Critical infrastructure

This section offers an introduction to academic research and theories about critical infrastructures. I will first introduce the term *critical infrastructure* and the academic debates related to the use of the term and how critical infrastructures are defined differently. The role of critical infrastructures in the aspect of *societal safety* will be presented. Followed by the debate about critical infrastructure systems as increasingly dependent, complex and coupled. Secondly, I will focus mainly on the role of ICT-infrastructure in critical infrastructures in today's digital and technological society. I will address different types of threats, where cyber threats are perceived as the main threat. Academic research about ICT-infrastructure is characterized by being mainly quantitative, but I have chosen to focus mainly on qualitative research to reflect the chosen research questions of this thesis.

We could say that the term *critical infrastructure* conceptualises the relationship between the governmental responsibility and the prioritization of national security, as well as the importance of private companies' involvement. Njå, Sommer, Rake & Braut (2020) provides a social definition of critical infrastructure as *"social structures and technical systems and facilities that are necessary to maintain or restore societies critical functions*" (p. 140). While Engen et. Al (2016, p. 138) defines critical infrastructure as *"... technological systems that deliver solutions and services of great importance to society"*. This definition points out to a greater extent how important technology is and how important of a role it plays as a critical infrastructure. But according to the definition by Njå et. Al (2020, p. 140) critical infrastructure is not synonymous with technology, here one can argue that technology rather constitutes technical systems or facilities that are necessary to maintain and restore critical infrastructure in the event of an incident or breach. In Norwegian academia, The Norwegian Directorate for Civil Protection (DSB) have played an important role in defining terms within societal safety theory and is frequently referred to in Norwegian societal safety literature. I seek to expand the theoretical view and try to limit the use of definitions and references to governmental sources. Their definitions are mainly on a national level and have the purpose of setting boundaries for political reasons, but also regarding regulation of different infrastructures and the companies who operates them. These definitions do not necessarily reflect which functions actually are critical to ensure reliable operations of critical infrastructure locally, regional, national and/or international (Njå et. Al, 2020, p. 16). The purpose of this thesis is to analyse how a private company who operate and/or supply ICT-services are important in ensuring a reliable operation of critical infrastructure. Hence, if they can be perceived as critical themselves.

Njå et. Al (2020, p. 16) questions what it means to have a title as a critical infrastructure. Should these functions have a certain status, be subject to a special type of control and regulation, or if the organizations owning and operating these functions should be provided with additional state funded resources to serve their purpose. Colleen Newbill (2019, p. 778) sees the term *critical infrastructure* used loosely and that the definitions can vary greatly. According to Enrico Zio (2018a, September, p. 10) can critical infrastructure consist of, and be categorized into, the following organizational sectors: power supply, communication, transportation, natural gas and oil, water supply, banking and finance, emergency services and government services. While Newbill (2019, p. 778) argues that there are differences between nation-states on how they define their critical infrastructure. Some nation-states have a long list and other nation-states have a shorter list with just a few critical infrastructures. This makes it difficult to apply a global definition of the term critical infrastructure, there are differences in definitions and in prioritization on the importance of what is considered as critical and needs protection. Protection of critical infrastructure, services and activities is by Njå et al. (2020, p. 17) called *societal safety. Societal safety* is to *"... look ahead and develop and operate systems and activities that will avoid accidents and meet the functional requirements that have been set"* (Njå et. Al, 2020, p.136). This perception of societal safety could be argued to have a proactive approach towards accidents as something caused by unintentional human-, technological- or organizational error, not intentional and malicious threats. Still, if we perceive critical infrastructure as consisting of systems, then this definition can substantiate the need for a system approach towards critical infrastructure. This is supported by Njå et. Al (2020, p. 17) who address the immediate assumption that societal safety is about complex systems, not a system as standalone but as a system context consisting of different societal functions. Njå et. Al (2020) continue to state that *"As soon as* *we talk about societal safety, it is assumed that we work with complex systems. Which [...] must be placed in its context with other systems and societal functions"* (p. 17). This approach is not only about the "system", but the ability to view one system as a part of something bigger and within its context and function towards other systems. According to Nystuen (2020) are ICT-systems playing an increasingly important role in physical infrastructure: *"Infrastructure security is less about physical linear structures, but instead about physical structures that are increasingly controlled by ICT-based control and management systems"* (p. 9). Critical infrastructure systems can be an overview of participating elements within the system, or it can be a system within a system, an information system to process information, or tools to understand structure and dynamics of a technological system. Newbill (2019) state that *"... components of one infrastructure can differ markedly in their criticality to the survival of the overall system; thus, non-essential systems are incorporated into the critical infrastructure while excluding some vital sectors"* (p. 768). Njå et al. (2020, p. 118) emphasize that critical infrastructure consist of several different systems, and management of these systems are characterized by complex interactions and high degree of dependency, hence they are tight coupled systems. The terms *coupling* and *complexity* originates from Perrows' *Normal Accident Theory*. But it is, according to the chapter about "Organizing for High Reliability: Processes of Collective Mindfulness" written by Weick, Sutcliffe and Obstfeld (2008), possible to adapt the use of this concept to *resilience* theory which I will elaborate on later (cf. 2.4). Today industries are more dependent on technologies, governments and supply/demand, which shifts industries like ICT-companies towards a more complex and tightly coupled state (Weick et. Al, 2008, p. 34). Complexity is a characteristic of the interactions in critical infrastructures. Njå et. Al (2020) defines *complex interactions*, based on Perrow (1999), as *"unknown sequences, or non-planned or unexpected sequences, that are either non-visible or not possible to understand"* (p. 131). Njå et. Al (2020, p. 132) address four types of complex interactions: 1) *interactive complexity* as interactions between system components, 2) *dynamic complexity* as interactions changing over time, 3) *decompositional complexity* as structured and functional non-consistent decompositions, and 4) *non-linear complexity* as no direct or obvious coupling between cause and effect. Complex systems consist of many different systems and services supplied by different organizations and sectors. The civilian population represents the users of critical infrastructures, but as there are complex value chains, the users are usually not in direct contact with the supplier of the function or service (Nystuen, 2020, p. 5). Tight coupled systems are defined by Perrow (1999) as *"...a mechanical term meaning there is no slack or buffer or give between two items. What* *happens in one [system] directly affects what happens in the other"* (p. 90). This approach to dependencies between systems increases the vulnerability of the society, but on the other side Weick et. Al (2008, p. 34) argue suggest that complexity and tight coupling might actually increase reliability in organizations. Dependencies related to time, continuity, processes and other activities can make it difficult and possibly disastrous if operations are disrupted (Njå et. Al, 2020, p. 117). This is supported by Engen et. Al (2016) who argues that:

> *"… loss or significant changes in critical infrastructures such as data traffic or transport can have major consequences and life and health may be at stake. Loss or disruption of an organization can also create unforeseen interactions for others, depending on how closely organizations and sectors are linked"* (p. 139).

On the other hand, Weick et. Al (2008) state that: *"Complexity and tight coupling motivate designers to create more redundancy in a system, inspire operators to customize centralized decision premises, favor the development of multiple theories of system functioning, and encourage learning and discourage complacency"* (p. 34).

Compared to previous research conducted in the field of critical infrastructure, this thesis will provide a different and essential aspect. Critical infrastructure has in the mentioned academic debate mainly been perceived as a nation-state and governmental responsibility. The debate is characterized by the need to define a global definition of what critical infrastructure should be. In comparison, this thesis will instead focus on the role of ICT-infrastructure in critical infrastructures and the role private companies plays in the involvement in protecting these functions.

2.2.1 ICT-Infrastructures and threats

Most of the ICT-infrastructure theory is focused on building technical designs, development of detection software and coupling of technical systems. There are mainly private companies that develop digital- and technological services and products used by the public sector, and they own and operate services supplied to critical infrastructure. The private sectors engagement in the protection of our critical infrastructure is considered as crucial to national security. Employees working with critical infrastructures should understand how it is complex and coupled from beginning of the process to the end (Njå et. Al, 2020, p.18).

Martin Jaatun (2015) defines ICT-infrastructure as *"critical infrastructures that rely wholly or in part on Information technology"* (p. 28). Jaatun (2015) continue to explain that *"… any* *hardware or software product might find itself as a component of a critical infrastructure system, whether it was designed with this in mind or not"* (p. 28). This means that while some components have a defined purpose and function, there are also components supporting these functions and being just as important to ensure continuous performance. I perceive ICT-infrastructure as having a key role within critical infrastructure systems, but also as something that should be characterized as *critical*. If we look back at Njå et. Al's (2020) definition of critical infrastructure and societal safety, here critical infrastructures as technical systems and facilities are necessary to ensure continuous and reliable performance or to restore societies critical functions. Which is also supported by the definition by Engen et. Al (2016), where technology is in fact defined as critical infrastructure.

I have previously elaborated on the complexity of ICT-infrastructure playing a key role in the continuous and reliable performance of critical infrastructure, this can also be a cause for concern. Technology provides us with services and functions such as electricity, internet, smart devices, smart houses, communication- and information technology, protection, weather-, map- and tracking services, it also provides disadvantages in case of severe catastrophes if these systems are disrupted (Engen, et al., 2016, p. 139). MacDonnell Ulsch (2014) points out that a fundamental issue about critical infrastructure is that it is *"... comprised of a number of sectors necessary for the country to operate under reasonably normal conditions. [...] Most critical infrastructure operations are connected to the Internet. They are therefore vulnerable"* (p. 87). Bergsjø et. Al (2020) defines digital security as *"... protection of "all" that is vulnerable because it is connected with or dependent of information- and communication technology (ICT)"* (p. 18). Based on the previous discussed interdependencies of critical infrastructure, Ulschs (2014) statement can defend the view of digital security as something that is or should be fundamental to protect critical infrastructure. Ulsch (2014) continue to state that *"what does matter is the vulnerability of virtually every industry built upon an Internet-enabled foundation. That means that it is accessible by anyone with the will and the talent to break into it"* (p. 68). Vulnerability is defined as *"...the conditions under which operational disruptions with negative consequences or serious incidents may occur"* (Engen, et al., 2016, p. 139). Societal security is the ability to look forward and plan, adapt and operate systems and activities to, in this thesis, avoid cyber-attacks and meet stakeholder requirements that have been set (Njå et. Al, 2020, p. 136). Jang-Jaccard & Nepal (2014, p. 984) argues that societal and digital security is aimed at reducing vulnerability in critical infrastructure structures and systems and highlights especially five areas of threats:

1. *Cyber warfare:* Political motivated hacking initiated by nation-states for the purpose of espionage and sabotage towards other nations causing damage and disruption of critical infrastructure
2. *Terrorism:* where a single actor or groups are deliberately attacking critical infrastructure for political agenda or gain. According to Engen et. Al (2016, p. 155) cyberattacks can also be perceived as terrorist attacks, which are difficult to predict and prevent as the threat actors adapts their strategies to the existing mitigative efforts and security measures.
3. *Sabotage:* deliberate actions from a single actor (ex-employee, insider, unwilling participant), political groups or environmental groups.
4. *Information warfare:* Private single actors hacking for personal gain or agenda, or other nations initiating attacks towards other nations to damage a country's infrastructure or influence elections.
5. *Natural disasters:* earthquakes, flood, landslides, or other natural events causing damage to ICT-infrastructure.

Threats and consequences can be difficult to predict due to *"… unknown probability of occurrence (frequency), unknown probability of extent and duration of stressor, unknown impact on system, and unknown system state or interdependence with other systems"* (Gößling-Reisemann & Thier, 2019, p. 118). For critical infrastructure not all risks are unknown either (Engen, et al., 2016, p. 154). The threats against critical infrastructures such as cyber threats have become well known in European societies in recent years, which have increased the demand of research on how to manage these threats and protect critical infrastructures (Jore, 2019, p. 158). Based on this I would argue that threats such as cyber threats are known threats and there is an extensive amount of information about the concept. The role of information in managing wicked problems towards critical infrastructures will be further elaborated in the next section about wicked problems. In recent years, the technological and operational improved measures towards known threats have increased the level of security. Security in this context is the ability to handle both the known and unknown threats by technological development together with organizational, both systematic and local, adaptations (Engen, et al., 2016, p. 155). Known threats are natural hazards, technical failures, system aging, known unknown, human errors, terrorist attacks and cyber-attacks (Zio, 2018a, September, p. 13). Cyber threats are a well-known challenge in today's society. There is uncertainty related to what extent the consequences of a cyberattack will affect critical infrastructure now or in the future. Threat actors with malicious intentions are constantly trying to succeed in breaching private companies, governmental institutions, nation-states and critical infrastructures. However, we do not know where, what or which vulnerabilities can and will be exploited next. Goessling-Reisemann (2016, p. 74) categorizes threats towards critical infrastructure based on their dynamics and knowledge about the nature of these threats in four categories:

1. *Known threats* that has already been experienced in the past and where predictions of future occurrence exist.
2. Threats that has never or rarely occurred and where predictions for future occurrences do not exist, are *unknown threats*.
3. *Creeping threats* develop slowly and possibly undetected for some time.
4. *Sudden threats* develop and occur without warning.

Based on the theory mentioned in this section, this thesis will further investigate academic theories related to cyber threats as wicked problems. Compared to previous research conducted in the field of ICT-infrastructure, this thesis will provide an essential aspect on how private companies owning, supplying and managing ICT-infrastructure can manage wicked problems by using networking and network societies. This will be elaborated in the next section about wicked problems.

2.3 Wicked problems

This section elaborates on the debate related to *wicked problems* and the perception of cyber threats as a new emerging wicked problem. As previously mentioned, critical infrastructure consists of complex interactions and tight coupled ICT-systems (cf. 2.2). These complex and coupled systems and the increasing digital and technological world we live in provides new problems, wicked problems. The debate in this section also introduces the perception that the evolving technological and complex society can arguably contribute to the rise of wicked problems towards ICT-infrastructure. This section will further elaborate on the use of *networking and knowledge sharing* as a solution to manage cyber threats as wicked problems. Actors working with critical infrastructure both in public and private sector will have different perceptions of problems and view them from different angles and interpret the available information differently.

Waddock et. Al (2015, p. 998) characterises wicked problems as unique, complex and interactive problems, this is supported by Rittel and Webber (1973, p. 164) who characterizes wicked problems as unique and challenging to define and categorize. These factors makes wicked problems unsolvable and potential solutions to these problems might be problematic in their nature (Engen, et al., 2016, p. 276). Waddock et. Al (2015) also presents a broader definition of wicked problems as *"... poorly formulated, boundary-spanning, ill-structured issues with numerous stakeholders who bring different perspectives to the definitions and potential resolution of the issue or problem. [...] each issue can be seen as a symptom of others, each issue is unique, no definitive solutions are possible, and there is no "stopping rule" that determines the problem's end or is likely to satisfy all the stakeholders"* (p. 996). Wicked problems are, from a change perspective, defined by "… *dynamic, interconnected issues that influence and are influenced by complex systems in which institutions, such as nations, oil companies, and utilities, are important actors"* (Waddock et. Al, 2015, p. 997). I have previously elaborated the meaning of the term *critical infrastructure*. Complex and tight coupled critical infrastructures are applicable to the concept of wicked problems in their nature as critical. As they are highly dependent on other infrastructures, defined by their dynamic interactions and complex systems.

Before we look closer on the term *wicked problems* in relation to critical infrastructures, it is necessary to look at a situation where critical infrastructure is threatened, which is called a *crisis*. According to Boin et. Al (2016) is a *crisis* defined as more of a social term where *"... something bad threatens a person, group, organization, culture, society, or, when we think really big, the world at large. Something must be done, urgently, to make sure that this threat will not materialize"* (p. 3). Boin et. Al (2020) has interpreted the definition of the term *crisis* in a modern society as *"…when political-administrative elites perceive a threat to the core values of a society and/or life-sustaining systems in that society that must be addressed urgently under conditions of deep uncertainty"* (p. 6). Wicked problems are compared to the term *creeping crisis* due to the characteristics of being a new problem, high degree of uncertainty, could potentially mobilize whole societies as it can potentially due harm to people or their values (Boin et. Al, 2020, p. 10). Boin et. Al's (2020) definition of a creeping crisis is *"... a threat to widely shared societal values or life-sustaining systems that evolves over time and space, is foreshadowed by precursor events, subject to varying degrees of* *political and/or societal attention, and impartially or insufficiently addressed by authorities"* (p. 7). Key characteristics is the lack of attention and exposure of limitations of governance. A crisis can also be considered as a real threat of objective nature, for example a cyberattack, which is measurable and have observable effects and consequences. This perception of the term crisis is according to Boin et. Al (2020, p.6) perhaps the most influential in disaster and critical infrastructure literature.

The perception of a crisis occurs when actors perceive a threat as urgent to address, hence it might be a crisis in its nature, but not perceived as one by the actors (Boin et. Al, 2020). It is when the actors involved perceive uncertainty differently, when there are large differences between how actors perceive the severity of the threats differently that a certain type of problems arise. Uncertainty is difficult to define, but can be describes as our perception of the *possibility of occurrence* (Renn, 2008, p. 2). Koppenjan and Klijn (2004) state that these complex problems are *wicked* due to three factors: 1) *"involved parties disagree not only about the solution, but also about the nature of the problem",* 2) *they cut across the traditional jurisdictions of organizations and cross the traditional borders between the private and public sector"*, and 3) *"Governments, businesses and civil society are unable to tackle these issues by themselves"* (p. 7). A crisis can also, according to Boin et. Al (2016), in academic discourse represent a *"... phase of disorder in the development of [..] an organization, [...] a business sector, or a polity"* (p. 5). Organizations can choose different approaches in managing wicked problems and Waddock et. Al (2015) address that these differences can *"influence the dynamics in interactive and complex ways that generate unpredictable outcomes"* (p. 1000). Which can turn out to be either negative or positive, or both, depending on how the situation is perceived and managed. If the solution to a wicked problem demands organizational and structural changes in government agencies and ministries, this can in fact cause a wicked problem too. Many structures are law binding and regulated, or changes can cause a shift in the balance of power and either centralize or decentralise the decision making (Engen, et al., 2016, p. 374). When wicked problems need transboundary involvement and management then new problems arise. New vulnerabilities for national security can emerge as well as cripple nation-states sovereignty when there are different perception of criticality and importance of protection of different critical infrastructures. Newbill (2019) support this by stating that*"... what is critical to a nation-state's survival vary between different nation-states, and these discrepancies could lead to confusion or conflict regarding what critical infrastructure sectors warrant international* *protection"* (p. 771). As ICT-companies deliver to customer all over the world, means they need to comply to also need to follow various laws, regulations and policies. If they operate in several countries, they can also experience a conflict in inequalities and demands. An example could be the General Data Protection Regulation (GDPR) in the EU which demand that companies operating in the EU, even if not located in the EU, has to follow the new regulations (European Commission, n/a).

Cyber threats, like natural disasters or terrorist attacks, can cause serious consequences for critical infrastructures and the systems that are dependent on them (Engen, et al., 2016, p. 155). One event in one part of the system will influence other parts of the system and easily have consequences throughout the system. This is supported by Boin et. Al (2020, p. 12) who argues that a minor technological incident or error can travel and spread unnoticed and cause a variety of consequences within a complex system which can accelerate a crisis. This is what makes cyber threats towards ICT-infrastructure problematic. Cyberattacks are:

> *"…continuous experience, and the identity of the attacker isn't always obvious. The constant probe attacks, in the form of cyber probes against critical infrastructure, could come from cyber criminals, nation-states intent on stealing information, or from hostile military forces. Such attacks may come from independent, unaffiliated hacker groups. Unless an attack originates with a known cyber terrorist group, or unless a terrorist group takes credit for an attack, reliable identification is complex and not always possible"* (Ulsch, 2014, p. 67).

This view is shared by Newbill (2019) who addresses the possibility of an exploitation where:

> *"Many of these cyberattacks on infrastructure systems are thought to be testing grounds for experimenting with new methods of attacking vulnerable targets and seeing how a nation-state will respond. These attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitred, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker"* (p. 773).

This means that attackers can roam freely and that a cyberattack can spread to millions of businesses and people worldwide without being noticed until after the damage is done. An example of this is the cyberattacks on the energy companies in Ukraine in the period 2014-2016 as previously mentioned (cf. 1). Based on previous events of cyber-attacks, it is possible to argue that there is a constant battle between sophisticated actor's resources and knowledge and the development of security mechanisms and implementation of proactive protection of critical infrastructure. It seems that critical infrastructure is too late in detecting breaches. The reason for this might be that governments have had a lack of focus on the importance of proactive security. The lack of regulations and governmental prioritizations reduce incentives for private companies to increase digital security. Change takes time and it is important to consider the complex characteristics of critical infrastructures and their vulnerability to wicked problems. As time goes by it is necessary to show willingness to constantly evolve and adapt to the development of new technological solutions with continuous innovation and reflection. This can also enhance the overwhelming perception as organizations need to address changes beyond their experience (Waddock et. Al, 2015, pp. 1005-1006).

The academic research on cyber threats as wicked problems towards ICT-infrastructure is growing but mainly conducted by governmental institutions. Compared to previous research, this thesis will gather the terms ICT-infrastructure, cyber threats, and wicked problems together with the aim to clarify the relationship between the terms. While critical infrastructure is more about politics and prioritizing societal functions as critical, wicked problems is more about the organizational interpretation and understanding of issues towards critical infrastructure and how to manage them. So, how can private companies participate in being a part of the solution to these complex and wicked problems? To mitigate wicked problems, it is necessary to seek experience and knowledge elsewhere. This takes us to the next section about *networking and knowledge sharing*.

2.3.1 Networking and knowledge sharing

The academic debate elaborated on in this section highlights both negative and positive sides of using networks and knowledge sharing. Theories promote the use of networking and knowledge sharing to manage wicked problems, but this is also not without problems. Networking societies are dependent on how information is interpreted and utilized, within their own organization and externally between the networking actors. The dynamic between the networking actors are affected by their own organizational features, which may cause an increased amount of uncertainty. Networking alone as a solution to dealing with wicked problems will likely not be sufficient if the use of networks is not part of a strategic and well-defined organizational plan.

Private companies are forced to seek knowledge and experience outside of their organization to be able to manage wicked problems. Olsen and Kruke (2011, p. 4) address knowledge as created out of interpretation of information and that *knowledge* is something that employees *possess*, compared to hardware which can store data and information. Companies and organisations want and need information from each other to provide their customers with goods and services. These interactions are called networks and a web of networks constitutes a networking society (Koppenjan & Klijn, 2004, p. 9). Koppenjan and Klijn (2004, pp. 10-11) characterizes networking societies with the purpose to manage wicked problems as environments with complex dynamics and border crossing activities, where individual organizational frameworks alone are not enough to manage wicked problems. The nature of the problem and the potential solutions are difficult to identify, the complexity of how networking societies are managing wicked problems are also a result of the dynamic between the actors and their own organisational arrangements. Based on this we could say that the involvement of different actors in a network would pose as an issue itself in handling wicked problems. Lægreid and Rykkja (2019) argues that the nature of wicked problems involves "*… multi-level and multi-sectoral actors, and create challenges as well as opportunities for political actors and public servants"* (p. 3). But the cooperation between different actors will be affected by uncertainty, unclear goals, different priorities and their perception of solutions. This is supported by Boin et. Al (2016, p. 50) who states that when a crisis occurs there is often the need for a coordinated network response on regional, national and global level. Private companies, public sectors and nation-states need to work together, but this is not without problems. Global, national and regional agendas and differences in jurisdictions and interests, political coalitions and parties, professional fields, organizational routines and policies can cause problems when trying to find common ground for responding to a crisis. A more positive approach is presented by Waddock et. Al (2015), they state that if private companies are able to appreciate and contribute to a broader system, then they are *"... more likely to engage in networks and collaborations of organizations: creating resources and competencies beyond those of a single organization are required"* (p. 1003). Waddock et. Al is not alone in perceiving use of networks as a resource when managing crises. Alastair Stark (2014, p. 693) explains how scholars have examined how networking societies can build bridges in collaborative and hierarchical crisis management. This is possible by creating:

> *"...flexibility through command structures. [...] If [networks] can develop collaborative interpersonal skills [...], if they can get the mix between hierarchy and*

> *collaboration correct within their network management […], and if they implement appropriate organizational procedures to supplement their modes of governance […], then structure and flexibility can coexist successfully"* (Stark, 2014, p. 693).

Rather than focusing on using networking societies and collaboration as crisis management response, this thesis focuses instead on how networking societies and knowledge sharing can be used to prepare for or manage wicked problems. Private companies develop technological and digital services and products used by the public sector and they own and operate ICT-infrastructure. The digital value chain consist of an environment of consumers, buyers, suppliers, supporting companies and organizations, interest organizations, governments who imposes laws, regulations and policies, consumer organizations, social interests groups, who all have demands regarding products, services and methods of production and operations (Koppenjan & Klijn, 2004, p. 8). The intertwined digital value chains can be illustrated in six main characteristic traits of the developing networking society as specified by Koppenjan and Klijn (2004, pp. 9-11). These characteristics have an important impact on how to manage wicked problems with the use of network and knowledge sharing:

1. *Increasing intertwinement:* Organizations dependency of each other, the need of specialization and dynamics in knowledge and product development. Creation of strategic alliances to share cost and to spread risks. Governments needs other parties to achieve their policy goals. These factors intensify the relations between governments and between governments and private companies.
2. *Deterritorialization and globalisation:* Private companies increasingly operate in a worldwide theatre, and economic investments and developments are less influenced by nation states.
3. *Turbulent environments:* Governments have always been a focus of societal attempts at influencing and it is impossible for governments to withdraw from these societal influences.
4. *Value pluralism:* Networking societies and subcultures have their own value systems. Diverging and competing values and demands towards public and private organizations that change over time.
5. *Horizontal relations:* Increased market driven and calculated relations between governments and companies, citizens and other governmental levels. Private companies and target groups are involved in governmental policy making.

6. *Development of knowledge and technology:* new technological inventions create new possibilities but also new uncertainties and risks. This demands an increased knowledge about complexities and development in specializations due to new knowledge and methods.

To organize with the purpose to ensure sufficient protection and security of critical infrastructure can also be perceived as a wicked problem. Especially when it is necessary to coordinate different actors and organizations in governmental and private sector, all with different responsibilities and agendas. As the world is increasingly getting more technological and new demands emerge, private companies also need to ensure they have the resources and knowledge to meet these new demands. Waddock et. Al (2015) state that:

> *"… bringing together the relevant stakeholders to a given problem, in many cases including stakeholders from multiple sectors, is crucial to any potential for what we can call a good enough solution […] where right answers or scientific certainty are unlikely"* (p. 1000).

This statement reinforces the value of using networking societies when faced with wicked problems where an unproblematic solution is virtually impossible to achieve. This view is essential for this thesis, and it would be interesting to research further how private companies benefit from such a relationship.

As previously mentioned, networking societies face increased intertwinement between governments, dependency towards other organizations, globalization, governments with different political agendas, a market driven landscape and the need for more knowledge to meet new risk and uncertainties of modern technology. Private companies and organizations will have different laws and regulations to consider depending on which countries they operate in or supply to. Due to this, I wish to briefly mention the need for a global set of rules between nation-states. Newbill (2019, pp. 763-764) highlights the proposed *Digital Geneva Convention*, a set of global rules between nation-states, which could be necessary to achieve international action towards cyber threats. A convention like this will not come without issues. It is therefore difficult to state that the purpose of networking will solve wicked problems alone. Instead, a set of rules which is open to interpretation may prove to be more helpful when operating with networking societies. It is also important to include not only nation-states and governments, but private companies as developers and suppliers of infrastructures. On the other side, Lægreid and Rykkja (2019, p. 3) states that achieving a global perception of wicked problems is difficult as there will be a distinction between perception of information and the importance of managing wicked problems.

An important aspect to consider when talking about networking and knowledge sharing as solutions to wicked problems, is the aspect of the previously mentioned term *uncertainty*. Koppenjan and Klijn (2004, pp. 12-13) addresses three types of uncertainty which concerns the complex institutional context of wicked problems:

1. *Substantive uncertainty related to the nature of wicked problems and availability of information:* More information does not necessarily lead to less uncertainty and solve the uncertainty of wicked problems, it might in fact lead to more uncertainty. In addition to this, the meaning of information is another source of uncertainty.
2. *Strategic uncertainty related to strategic choices actors make to manage wicked problems:* Actors base their decisions on perceptions that other actors do not acknowledge or know of. Complex issues can cause a broad variety of different strategies among actors in network societies. Unexpected strategic turns and complex interactions characterize wicked problems. Based on these characteristics, strategic uncertainty is difficult to reduce and cannot be eliminated.
3. *Institutional uncertainty related to actors having different institutional background:* There are diverging institutional frameworks within and between organizations, administrations, and networks, hence the involved actors will likely have different perceptions, regulations, tools, opinions, culture and language to base their choices on. This increases the institutional uncertainty of how interactions develop and takes place between the actors involved.

An important aspect of institutional uncertainty is knowledge sharing in an organization, including training and staying up to date. This can, according to Olsen and Kruke (2011), be different in the sharp end and the blunt end. Their research is based on mainly relief and humanitarian organizations crisis management. But I think the concept is applicable to private companies managing wicked problems in complex infrastructure, systems and value chains. In this thesis, I view the sharp end to represent the employees at operational and technical level working closer to the customers, systems and products. On the opposite side, there is the blunt end, representing the strategic level with executive management, top-level management and middle management. The blunt end has a strategic perspective on politics, economy and governance, while the sharp end is more involved in the day-to-day performance and threats.

Based on previous research, this thesis will further investigate the application of networking and knowledge sharing to manage wicked problems. The difference compared to previous research is that this thesis will put wicked problems and networking in a resilience context. Which brings us to the next section about resilience and High reliability Organizations.

2.4 Resilience

This section elaborates the debate on *resilience*, *resilience management* and the application of *High reliability organisations (HROs),* as solutions to manage wicked problems for private companies. Where the debate previously was about the character of the problem with private companies' management of cyber threats, resilience is now considered a solution to the complexity of the problems and to manage the related uncertainty. It is necessary with more academic research on how private companies can organize, manage and evaluate how to manage threats and wicked problems. This is supported by Lægreid and Rykkja (2019, p. 1) who states that there is a growing, but limited, amount of research on how to design, manage and evaluate organisations mitigative efforts to protect societies and critical infrastructure against crisis and wicked problems. In addition to this there can be vulnerable system designs and lack of priorities in politics and leadership (Engen, et al., 2016, p. 155). The existing academic literature is mainly about risk management, but another theory that can be related to management of wicked problems and cyber threats in organizations is *resilience*. Wicked problems require a complex response to a changing context and this is where the concepts of resilience and adaptive abilities is emphasized (Waddock et. Al, 2015, p.1007). In recent years the focus on resilience management of critical infrastructure have been evolving. Enrico Zio (2018a, September) expands the term *resilience* to involve more than only the ability to adapt but as a "*focus on the capacity of systems to adapt, reorganize and recover from disruption and disturbance"* (p. 20). This contrasts with the more traditional risk approach where *"risk analysis focuses on achieving reliability, absolute protection and the control of system change"* (Gößling-Reisemann & Thier, 2019, p. 121). Traditional risk management cannot adequately capture the *"… failures in interdependent critical infrastructures […] connected to ICT networks [and] differs from risk management in some key points: the type and characteristics of stressors assessed, the level and uncertainty of quantification of impacts and the typically addressed systems"* (Gößling-Reisemann & Thier, 2019, p. 118). In contrast to risk management, is resilience management an approach to manage complex systems and problems that are difficult to detect, with low probability and potentially catastrophic consequences in complex and tight coupled systems (Gößling-Reisemann & Thier, 2019, p. 118). These characteristics is used to describe critical infrastructures (cf. 2.2.1). Based on the debate elaborated in this section, resilience in context of managing wicked problems could potentially be a paradigm shift for the academic literature.

Terrorism can also involve cyberattacks (cf. 2.2.1). Stephen Flynn (2018b, September, p. 30) state that the resilience approach can be used to manage risks as it can decrease the risk of terrorism by weakening threats. Threat is a result of intentions and capability. Reduced vulnerability requires increased capability, while reduced consequences decreases the motivation and degree of intention for an attack. Based on this Flynn (2018b, September, pp. 30-31) state that risk is a result of the degree of the threat, vulnerability and consequence of an attack. Reduced vulnerability and consequences will decrease the threat and lower the risk. This means that an investment in resilience measures provide a mitigative effect on threats, hence makes it more difficult for malicious threat actors to operationalize their threats towards critical infrastructure.

Zio (2018a, September, p. 33) addresses a problem with resilience management in systems and questions the flexibility of the system structure, design and the system's ability to avert extraordinary events or mitigate disruptions if a breach or incident occur. While Colding, Barthel and Sörqvist (2019) argues that resilience is a suitable planning approach to manage wicked problems in the tight coupled and complex society we live in:

> *"…resilience thinking can be used as a lens of inquiry for probing both expected and unexpected management surprises, and for studying different developmental pathways and potential thresholds in complex adaptive systems. In this way, resilience thinking represents a framework for […] policymakers and planners that can be used to identify, probe and deal with wicked problems"* (p. 517).

Shaw & Maythorne (2013) state that resilience *"… as 'survival' is also shaped by more traditional, top-down responses to dealing with 'threats' to security, and by the dominance of managerial or technical 'solutions' to problems based on disaster or risk reduction strategies"* (p. 46). This resilience discourse, where perceiving resilience as a response to managing security threats, greatly illustrates why the theory about resilience is highly relevant to this thesis. Threats can be met with strategic plans and actions initiated and rooted in top management in private companies. In Shaw & Maythorns (2013, p. 51) research their empirical results suggest that by reframing resilience as a discourse can provide more knowledge on how the terms relevance and application is perceived by managers. Their empirical results suggest that resilience can provide context to the distinction between mitigation (actions to permanently remove or reduce threats) and adaptation (capacity of a system to adjust to threats and to cope with the consequences). There are three factors that needs focus in a resilience management approach for private companies owning and managing ICT-infrastructure systems according to Flynn (2018b, September, p. 33):

1. Elemental capacity: *"the prerequisite system conditions that must be in place in order for an infrastructure system to provide its function to its users"*.
2. Essential function: *"the minimal level of function that infrastructure system needs to provide in order to: 1) support recovery, and 2) meet the critical needs of its users"*.
3. Full/normal function: *"is that which a critical infrastructure system needs to provide in order to satisfy the routine needs of its users and to remain economically viable and supportive of the public good"*.

In resilience management the system structure is a combination of the material structures of critical infrastructures and the human organizational aspect involved in the operations (Zio, 2018a, September, p. 27). Resilience is a means to achieve security, to adjust and take responsibility, but there are varying degrees of resilience in different organizations and companies. This manifest itself in the ability to identify or predict threats towards critical infrastructure when there are 1) *"unknown probability of occurrence (frequency)",* 2) *"unknown probability of extent and duration of stressor",* 3) *"unknown impact on system",* and 4) *"unknown system state or interdependence with other systems"* (Ruth & Gößling-Reisemann, 2019, p. 118). The uncertainty of wicked problems towards ICT-infrastructure can be managed by resilience management as it aims to prepare systems for unknown threats, which can also mean *"…'cannot be known' owing to undeveloped scientific understanding or to unpredictable emergent behavior of the system under management itself. The latter might be relevant especially for interdependent systems-of-systems (Kröger and Zio 2011)"* (Gößling-Reisemann & Thier, 2019, p. 118). A crucial part of resilience management is how information is organized and managed within an organisation. Information is necessary to manoeuvre in uncertain conditions. Information can both increase and decrease uncertainty (cf. 2.3.1). Networking and knowledge sharing involves a regulation of the information flow and a proactive provisioning of necessary and available data and information to employees at different hierarchical levels involved which in turn can enhance resilience (Zio, 2018a, September, p. 27).

Resilience can be perceived as a strategy to manage uncertainty (Gößling-Reisemann, 2016, p. 74), where High Reliability Organisations (HROs) can be perceived as a resilience strategy to manage wicked problems like cyber threats. Compared to previous research this thesis will connect the mentioned theoretical concepts and investigate how they can be used together. I will now look at theories related to how private ICT-companies can use networking, knowledge sharing and resilience to design and organize to be a *High reliability organization*.

2.4.1 High Reliability Organizations – a resilience strategy

Traditionally, academic literature on High Reliability Organisations (HROs) has mainly been associated as a contrast to Perrow's Normal Accident theory, as previously mentioned about critical infrastructure (cf. 2.2). HROs can according to Haavik, Antonsen, Rosness & Hale (2019) be defined as *"…a perspective and approach that describes characteristics of organisations with high complexity and tight couplings that experience extraordinarily few accidents, despite the assumption that such systems […] cannot be satisfactorily controlled in the long run"* (p. 481). Organizations in environments with high-risk technology such as aerospace, aviation, nuclear power and oil and gas are typical HROs in academic literature. The amount of academic research within the field of resilience and HRO in the ICT-sector is limited, but there is academic literature within the field of crisis management and HROs that I consider as relevant to this thesis. ICT-companies has a high degree of technological and digital complexity and the systems they have are tightly coupled, which are characteristics of HROs (Engen, et al., 2016, pp. 138-139). HROs ability to adapt is, as previously stated, defined by Weick and Sutcliffe as *resilience*. Eleven key characteristics shapes organizations ability to achieve resilience (Engen, et al., 2016, p. 153):

- *"High technological competence*
- *High performance and continuous control*
- *Persistent search for improvement*
- *Risk-driven adaptation*
- *Often characterized by complex activities*
- *Many incentives and shared expectations of reliability*
- *Reliability culture*
- *Reliability cannot be replaced*
- *Limitations in learning through trial and error*
- *Flexible management structures during crises*
- *Redundancy designed into the system ensures balance between input and output"*

These characteristics demands increased focus on security and adaptability to mitigate threats to maintain reliable performance. Weick and Sutcliffe (2015, p. 95) describes the signature feature of HROs as something not free from errors, but with the ability to not let errors disable the organization. HROs does not wait around for an error to occur before responding, instead they prepare for them to happen by being proactive (Weick et. Al, 2008, p. 98). The theory is based on the perception that incidents in high technological systems can be prevented. Weick & Sutcliffe (2015) points out that *"In moments of resilience, conditions vary yet the effect remains the same. That difference lies at the heart of a commitment to resilience"* (p. 98). Organizations that strive to be HROs should also demand that their suppliers strive to be resilient and reliable too, or they could pose as a vulnerability in the supply chain. Competitiveness is also an issue in terms of private companies' management of risks and use of resilience approach (Flynn, 2018b, September, p. 45). Users will likely prioritize and chose suppliers who are resilient and avoid those suppliers who are not. Thus, those companies that can handle increased costs and at the same time be able to cope with increased risk, will gain an advantage compared to smaller companies not willing to, or able to, take the risk and the cost of prioritizing an HRO strategy.

We can describe HROs as organizations that strive to achieve the highest degree of resilience. This is however an ever-changing process, seeing as new threats are constantly discovered. An organization will therefore never truly achieve and maintain the status as an HRO. To achieve some degree of resilience in an organization, the need for a rooted strategy on how to manage resilience in the organization is necessary. Four organizational tools to achieve this is, according to Gößling-Reisemann (2016, p. 74), *1) preparation and prevention, 2) implementation of robust and precautionary designs, 3) management and recovery from crises,* and *4) learning and increase knowledge.* This also pairs well with the four necessary conditions for dealing with resilience, which according to Njå et. Al (2020, p. 116) is *1) Security and reliability are prioritized, 2) Redundancy increases security, 3) decentralized management, strong organizational culture and continuous learning,* and *4) Organizational learning.* HROs are continuously assessing and evaluating their performance, risks and threats to identify new or better ways to monitor, manage and measure threats (Weick, 2001, p. 42). According to Boin et. Al (2016) are a crisis, or threats, a *"…real world "stress test" to the resilience of political systems and the crisis management capacities of leaders"* (p. 3). If we transfer this concept to private companies, a crisis like a cyberattack, will test the resilience of the company and how their leaders manage these events. They continue to state that *"... the quality of crisis management makes the difference between life and death, chaos and order, breakdown and resilience"* (Boin et. Al, 2016, p. 3). Hence the quality of crisis management in the company will be reflected by how well their resilience management strategy is prioritized in the organization. It is important that strategies and information are communicated broadly within the organization, while encouraging awareness among the employees of how they play a key role in the organisational system (Boin et. Al, 2016, p. 42). Information and documentation are continuously adapted, updated or replaced for the better if deemed necessary (Boin et. Al, 2016, p. 42). Organizations are dependent on its culture to achieve resilience. Reason (1997) defines *organizational culture* as *"shared values (what is important) and beliefs (how things work) that interact with an organization's structures and control systems to produce behavioural norms (the way we do things around here)"* (p. 192). An organization need to ensure effective, structured and sustainable responses in large groups of people, working continuously with repeating tasks over short and longer periods of time. At the same time preventing organizational lack of attention towards external threats (Weick & Sutcliffe, 2015, p. 130). Shared organisational values in a company makes it possible for the company to plan for a decentralize decision-making authority to those employees working in the sharp end in case of threats or incidents occur (Weick, 2001, p. 341). We can summarize the success of an HRO to be dependent on three characteristics: 1) *safety and security awareness,* 2) *decentralisation,* and 3) *training* (Boin et. Al, 2016, p. 42).

Compared to previous research, this thesis will adapt the concept of resilience and HROs to private ICT-companies which is usually not recognized as HROs. The thesis will further investigate how the HRO concept can be used as a strategy to manage wicked problems related to ICT-infrastructure, along with the use of networking societies. Relevant fields of interest are how the companies uses networking and knowledge sharing to access available information, how the companies emphasizes the importance of security in their organization, how the organizations perceives cyber threats and how these factors results in an increased sense of resilience. Instead of having a technical approach towards security measures, this thesis seeks to investigate organizational aspects of management.

3. Methodology

This chapter will elaborate the overall methodological standpoint by presenting the status of theory discussed in chapter two and how it relates to the chosen methods for this thesis, as well as justifying the use of them. I will present the case selected for this thesis, followed by the research and data collection methods, methods for data reduction and analysis, ethical considerations and this thesis' validity and reliability. I will address the structure of the argument at the end of this chapter.

The thesis seeks to understand organisational aspects of cyber threat management and how private ICT-suppliers perceive their responsibility and role in a bigger societal impact perspective. The organizational aspects of cyber threat management will be put in relation to the theoretical concepts: *critical infrastructure, wicked problems, networking and knowledge sharing, resilience* and *HRO.* The methodological choices and assumptions have the purpose of answering the problem statement of the thesis:

> *"How do private IT-companies perceive and define their role in protecting critical infrastructure?"*

There is limited research about the main theoretical aspects in relation to each other. The main theoretical aspects are *critical infrastructures, ICT-infrastructure, cyber threats, wicked problems, networking and knowledge sharing, resilience* and *high reliability theory*. To answer the problem statement of this thesis in relation to the main theoretical aspects, the following research questions will be answered in the analysis:

1. *How are ICT-suppliers affected by cyber threats?*
2. *How does ICT-suppliers perceive their societal responsibility in the protection of national security?*
3. *Does ICT-suppliers have a conscious relationship towards resilience in their work to protect ICT-infrastructure and manage wicked problems?*

3.1 Epistemology

This section elaborates on the overall methodological standpoint, ontology (nature of the social reality) and epistemology (how knowledge about the reality can be achieved). I will explain the choices I have made, and why, to answer the research questions and problem statement chosen for this thesis. Firstly, I will introduce the methodological choices and assumptions which the thesis is based on. Secondly, the chosen case study is introduced and described.

I have chosen a qualitative research method and a single-case study as the method of inquiry. Case study is according to Blaikie & Priest (2019) *"... not a methodological choice but a choice of what is to be studied"* (p. 181). This approach was chosen due to the applicability of a case study. Case study gives me the opportunity to study a real and complex "case" or phenomenon in-depth with a societal perspective. The purpose of case studies is suitable for studying organizational and managerial processes, national and/or international relations (Yin, 2018) and it becomes possible to get an in-depth understanding of the organizational aspects of cyber threat management. This approach is called *explanatory research*, an approach which can be used to understand and explain patterns between relationships, structures, processes and contexts (Blaikie & Priest, 2019, p. 81).

The application of abductive logic was chosen to answer the research questions of this thesis. Abductive logic, as understood by Blaikie & Priest (2019, pp. 70-71), can be used to answer both *what* (provides explanation) and *why* (provides understanding) questions. I have chosen to additionally ask *how*-questions, not with the purpose to cause change, but to further explain the context of how things work in the company. *How*-questions are, according to Yin (2018, p. 10), explanatory questions, which favour the use of a case study. My role is to understand what is meaningful for the actors based on their reasoning, sense making, intention and rules (Blaikie & Priest, 2019, p. 82). Abductive logic allows me to understand the meaning and interpretations that exist within the chosen case, while incorporating this into social research and theory (Blaikie & Priest, 2019, p. 99). I am not able to determine whether they are right or wrong, as I am not including neither their customers nor the Norwegian authorities' perspective. This is emphasized by the epistemological constructionism approach, where the world is understood by our knowledge of how things are, hence there does not exist only *one* truth alone about a phenomenon (Braun & Clarke, 2014, p. 30).

Social actors within this case study will provide knowledge about their perceived reality through interviews and survey. The interviews represent the management's reality and the survey represent the employee's reality within the context of the chosen case. Together they will provide me with different aspects of this reality. Data collection does not represent the full reality, as I have not managed to cover all aspects of it, but the data is a mere representation of the reality. Which through data analysis will provide a certain "truth" of the status quo of the phenomenon being studied (Johannessen, Christoffersen, & Tufte, 2011, pp. 39-40).

In the interview guide (Appendix B) and questionnaire (Appendix C) the questions are mainly descriptive formulations using *what*- and *how*-questions (Kvale, Brinkmann, Anderssen, & Rygge, 2015, p. 164). This provides descriptions about the interview participants' point of view, while *why*-questions is asked as a follow-up question to provide personal perceptive answers (Kvale, Brinkmann, Anderssen, & Rygge, 2015, p. 164). Abductive logic gave me the opportunity to provide accounts of social actor's insider view of their own social world (Blaikie & Priest, 2019, p. 99). As I am employed by the IT-company chosen as the case study, this makes me an "insider" as well. This is an opportunity to acquire knowledge about certain aspects not necessarily accessible by outsiders. This will help me in investigating the context of the phenomenon related to the company's culture and worldview from the inside (Blaikie & Priest, 2019, p. 209). I have a unique opportunity to research the chosen concepts in-depth. A crucial factor to be aware of is my own knowledge and perception about the chosen case and the study I am authoring.

3.1.1 Chosen case study

I have chosen to limit the study to a specific organization, a single-case study with three embedded unit of analysis (management, employees and documentation). The reason for this is to provide in-depth knowledge about the chosen theoretical aspects, instead of broad knowledge. The chosen private ICT-company is anonymized and "XX" will be used instead of the company name. I am aware that the thesis would benefit of using the name of the company that I am writing about. However, after careful consideration, I have decided not to use the name of the company. The reason for this is elaborated on in section *3.4 Confidentiality and consequences.*

XX is an ICT-supplier headquartered in Stavanger, Norway. They have offices spread out in Norway, UK, Canada, the US, Asia and the Middle East. There are approx. 450 employees worldwide and around 330 of them are in Stavanger. Large enterprises employ 250 and more, according to OECD (2020), which makes XX a large-scale private ICT-company. Most of the employees are working at the headquarter, including executive management, directors and managers, global departments, consultants, developers, technicians, customer support, sales, finance and HR. The company are hosting and supplying to customers internationally, national, onshore and offshore. Since the founding of XX in 2000 they have evolved from being an application service provider to a cloud service provider. During this time, they have grown to be a global digitalization partner across different industries. In addition to cloud solutions they provide software applications and consultancy services to customers in both private and public sector in the Oil and Gas industry as well as the Renewables and Ocean industry.

ICT-companies are hosting and supplying services to critical infrastructures in both private and public sectors, for example the energy sector. The companies which are hosting and supplying companies deemed as critical infrastructures, should also be perceived as critical infrastructures. Mainly due to their role in protecting critical infrastructure and their responsibility of securing assets and to prevent serious impacts on their customers production and operation. Private ICT-suppliers have a responsibility for the sake of national security and the society to protect critical functions, as a breach could have catastrophic consequences. What might only seem like terabytes, gigabytes and numbers to the ICT-company providing these services – these can in fact hold documents of great value to their customers, such as sales, purchases, merges, deals, transactions etc. There are laws regulating what types of documentation needs to be stored and protected and for how long in case of investigations, lawsuits, corruption, insider trading etc. Which means that ICT-suppliers are, due to the regulation of their customers, required to protect these assets.

Interviews were conducted on one executive management role and one manager role located at the blunt end and 50 questionnaires were sent out to employees at the sharp end. The questions asked had different purposes in relation to the research questions. Questions directed at the management were mainly political and strategic, while questions directed to the employees were intended to examine how the employees reflect the management aspect of the organization. The document analysis was conducted to see how management have formalized their role and responsibility in strategies applicable to the achievement of resilience and HRO. In the next section, the different research methods for data collection will be elaborated.

3.2 Qualitative research methods for data collection

This section introduces the chosen research approach and methods that forms the analysis strategy for this thesis. *Methods* are according to Alan Bryman (2008) about *"…the techniques that researchers employ for practicing their craft"* (p. 160). Which involves aspects of the research process and how to collect, reduce, analyze and generalize from data. Qualitative research methods are useful to achieve in-depth understanding about a phenomenon.

This thesis is based on qualitative research methods consisting of multiple sources for data collection, more specifically three sources. According to Robert K. Yin (2018) an advantage of conducting a single-case study is that it is possible to use different sources of data, also called *data triangulation*. Which makes it easier to conduct in-depth research about a phenomenon within their natural context (Yin, 2018, p. 127). Data triangulation is a time-consuming process, especially as there are three diverse types of sources to analyze data from. This means that I must be aware of how to use different data collection techniques and how to analyze the different data.

Interviews is chosen for the purpose of providing in depth data from participants involved in decision making and development of strategies on management level. Surveys are conducted with the purpose to broaden the perspective of data collection and provide context to the phenomenon. Additionally, they will be used to see and evaluate the empirical results from the interviews – if the views of the management resonate with that of the non-management employees. The third source of data collection will be conducted through review and analysis of internal company documents. This is useful to understand the applied frameworks and strategies that exist to possibly achieve resilience and reliability in the company.

I formulated three questions based on the chosen research questions prior to conducting the interviews, survey and document analysis. These questions are used for thematic and coding purposes to organize the data before I started analysing the data from the data collection. I will answer the following research questions in the analysis chapter:

1. *How are ICT-suppliers affected by cyber threats?*
2. *How does ICT-suppliers perceive their societal responsibility in the protection of national security?*
3. *Does ICT-suppliers have a conscious relationship towards resilience in their work to protect ICT-infrastructure and manage wicked problems?*

The data collected is textual or transcribed from oral to textual data, which together makes out the material used for the following data analysis. A thematic organization is used to analyze the data collected. The predefined questions made out a thematic structure which assisted me in organizing the answers from the participants. The same thematic approach was used for the survey. The questions used were mainly the same, but they were adapted to provide answers of two distinct aspects, the blunt end's aspect and the sharp end's aspect. This analytic approach made it possible to generalize across the multiple data sources. As well as provide me with an understanding about the social actor's different or similar accounts of the phenomenon being studied.

Interview

I chose to conduct individual semi-structured interviews as one of three sources of data. A semi-structured interview, as understood by Kvale and Brinkmann (2015) is used*"... when themes from everyday life are to be understood from the interviewees' own perspectives"* (p. 46) . This interviewing method of collecting data is sufficient and will provide good insight and knowledge to answer the chosen research questions. Qualitative interviews enable the researcher to get insight into the complexity of the phenomenon (Johannessen, Christoffersen, & Tufte, 2011). Semi-structured interviews made it possible to come closer to the participants' accounts of the phenomenon being studied by expressing their meanings and interpretations about the organizational aspect of cyber threat management (Kvale, Brinkmann, Anderssen, & Rygge, 2015, p. 46). I formulated three main questions:

1. *How does cyber threats affect the company?*
2. *How does the company perceive their societal role in the protection of national security?*
3. *Does the company follow any procedures/strategies to manage cyber threats?*

These questions follow the topics introduced in the research questions and the theoretical concepts (cf. 2). Each main question had several sub-questions. I used these questions for thematic and coding purposes when analysing the data from the data collection. I consider it an advantage that the participants could prepare in advance, any uncertainties could then be discussed in advance, this can also reduce the duration of the interview. The open-ended questions make it possible to have follow-up question. Semi-structured interviews give the researcher and participants the flexibility to have a more fluid conversation, but it is important that the researcher ensures all questions are answered sufficiently (Johannessen, Christoffersen, & Tufte, 2011).

I chose to limit the interview sample size to four participants with a key role in top level management. All was strategically selected based on their position and area of expertise. The positions have been manipulated to anonymize the company XX and to be easier to replicate in other studies. Out of four requested interviews, two interviews were conducted with Chief of Technology and Director of HSEQ (Health, Security, Ethics & Quality). Two potential participants did not answer my requests. The participants are positioned at top-level management as illustrated below (figure 2), the colours illustrate different levels in the top-level management:

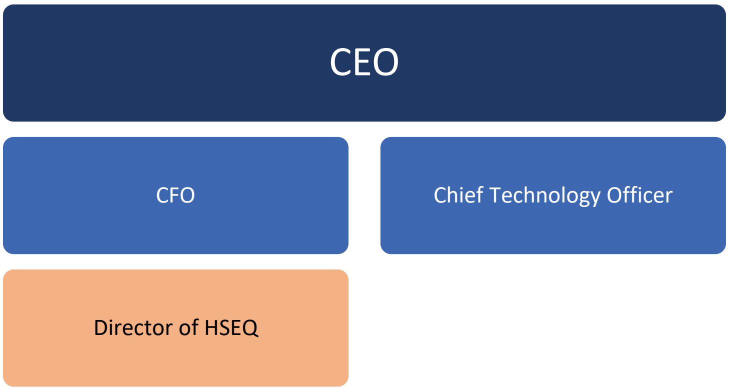

Figure 2 Hierarchical location of the interview participants in the company

The potential participants were contacted by email to request their participation in the study. Attached was an informed consent form (Appendix A) and interview guide (Appendix B). The purpose of *informed consent* is, according to (Bradburn, Sudman, & Wansink, 2015), to provide the potential respondents with *"… sufficient information about what they are actually being asked and how their responses will be used. The intent is for them to be able to judge whether unpleasant consequences will follow as a result of their disclosure"* (p. 14). The interview approach was conducted by using a predefined interview guide with open-ended questions. The interview guide was used as the foundation of the interview and contained a list of questions related to the main theoretical aspects to be addressed (Johannessen, Christoffersen, & Tufte, 2011).

The interviews were conducted as individual videocalls over Microsoft Teams. The interviews were recorded using the built-in recording function. After each interview when the recording was ended, the built-in transcript service in Microsoft Teams transcribed the interview and generated a text file. This solution was chosen due to the strict pandemic regulations due to Covid-19, which states that anyone who can, should work from home. The context of the interview can in fact help the interview as the participant is sitting in a natural and safe space at home. There is also a risk that household disturbances can occur, which can have an effect on the ability to concentrate on the interview (Johannessen, Christoffersen, & Tufte, 2011), this was fortunately not experienced.

Semi-structured interviews are difficult as the interviewer need to master the ability to interpret the answers and quickly formulate follow-up questions without prolonged delays. This is something I experienced as difficult; the follow-up questions were not as well formulated as I intended to, hence it may have had a minor impact on the quality of the interviews. The interviews were also conducted in English, this was not necessarily a disadvantage, but it made it more difficult to formulate the follow-up questions and the participants also had to use some Norwegian terms. To interview as an insider likely caused the context of the interview to be a little less formal and more open. That I already have insight and knowledge of the management system, routines, processes and the values of the company gave me an advantage, as it provided me the opportunity to associate the answers with the context more clearly. At the same time, I had to make sure that I kept my individual interpretations separate from my sense making. I felt that the conversation became a little lighter because I knew who the participants were in advance, it lowered my shoulders somewhat. At the same time, there were a few brief digressions during the interviews which affected the focus of both the participant and me, as an interviewer.

Kvale & Brinkmann (2015, p. 207) estimated, based on their own research, that an interview of one hour takes around five hours to transcribe and gives about twenty to twenty five written pages. I used 12 hours and five minutes to transcribe two interviews, one interview lasted 45 minutes and the second interview was 50 minutes. One interview was a bit more challenging to transcribe as there was confidential details that needed to be excluded from documentation after agreement with the participant. This is further illustrated in table 1:

Table 1 Overview of interview participants

#	**Referred to as**	**Role**	**Date**	**Duration**	**Transcribation**
1	*Director of Security*	Director of HSEQ (Health, Security, Ethics & Quality)	20.05.2021	45:12	04:55:00
2	*CTO*	Chief Technology Officer	27.05.2021	49:51	07:10:00

As I decided to anonymize the company, I then felt it was necessary to refer to the interview participants by their roles instead which was not initially intended. This is especially important since there are only two interview participants. One participant will be referred to by the well-known acronym *CTO* (Chief of Technology*),* but also to emphasize the responsibility and location of the participant in the hierarchy. The second participant will be referred to as *Director of Security*, this emphasizes the responsibility of the role and why it is relevant to the thesis. Even though it was intended to have more than two interviews, I am satisfied with the data from the two interviews. Which provided me with in-depth knowledge from the management perspective on how the organization manage cyber threats.

Survey

Surveys are usually perceived as a quantitative research method gathering statistical and nominal data (Blaikie & Priest, 2019, p. 31). The survey used in this thesis will gather qualitative data as the respondents are requested to answer open-ended questions in a questionnaire (Williamson, 2002, p. 235). Due to limited time this approach is helpful in effectively gathering a broad amount of data. There is no verbal contact and no face-to-face correspondence but it gives me the opportunity to reach out, in a short amount of time, to a larger amount of people (Blaikie & Priest, 2019, p. 209). Surveys were conducted with the purpose of broadening the perspective of the context of the phenomenon being studied. The survey seeks the meaning and interpretations of the employees, with the purpose to investigate if the views of the management resonate with that of the non-management employees. How the employees perceive cyber threats, the company's societal role and organizational aspects reflects how management have incorporated their strategies within the organization. Open-ended questions is useful when researching a lesser known phenomenon that there is not extensive knowledge about in order to create predefined answers (Johannessen, Christoffersen, & Tufte, 2011, p. 279). It is not possible to generate numbers out of these answers, hence a qualitative analysis of the data is necessary. Using survey allowed me to reach out to employees located at the sharp end of the company or working in certain areas within the company relevant to the thesis. Still, it is not necessarily a good thing to reach out to all employees for the sake of the amount of relevant data to analyze.

I decided on a relevant sample size based on four important factors: 1) *the degree of accuracy,* 2) *variations in characteristics,* 3) *level of measurement* and 4) *extent to which subgroups in the sample will be analyzed* (Blaikie, 2007, p. 178). I investigated the organizational chart of the company and identified the relevant departments for this thesis. I excluded managers and other roles which are further up in the hierarchy. As this is a qualitative research, I decided that a sample size of 50 respondents was sufficient. This is not a representative sample of respondents for the whole company, but it will serve the purpose as representing the sharp ends' aspect. Limited time was a crucial factor, as it would take a comprehensive amount of time to analyze the answers from more than 50 respondents if I had more than 10 questions. Based on the predefined sample size, I randomly picked three respondents from each department that I had identified as relevant located at the sharp end of the company. The hierarchical location of the respondents is illustrated, using different colours of each level, in figure 3 on the next page.

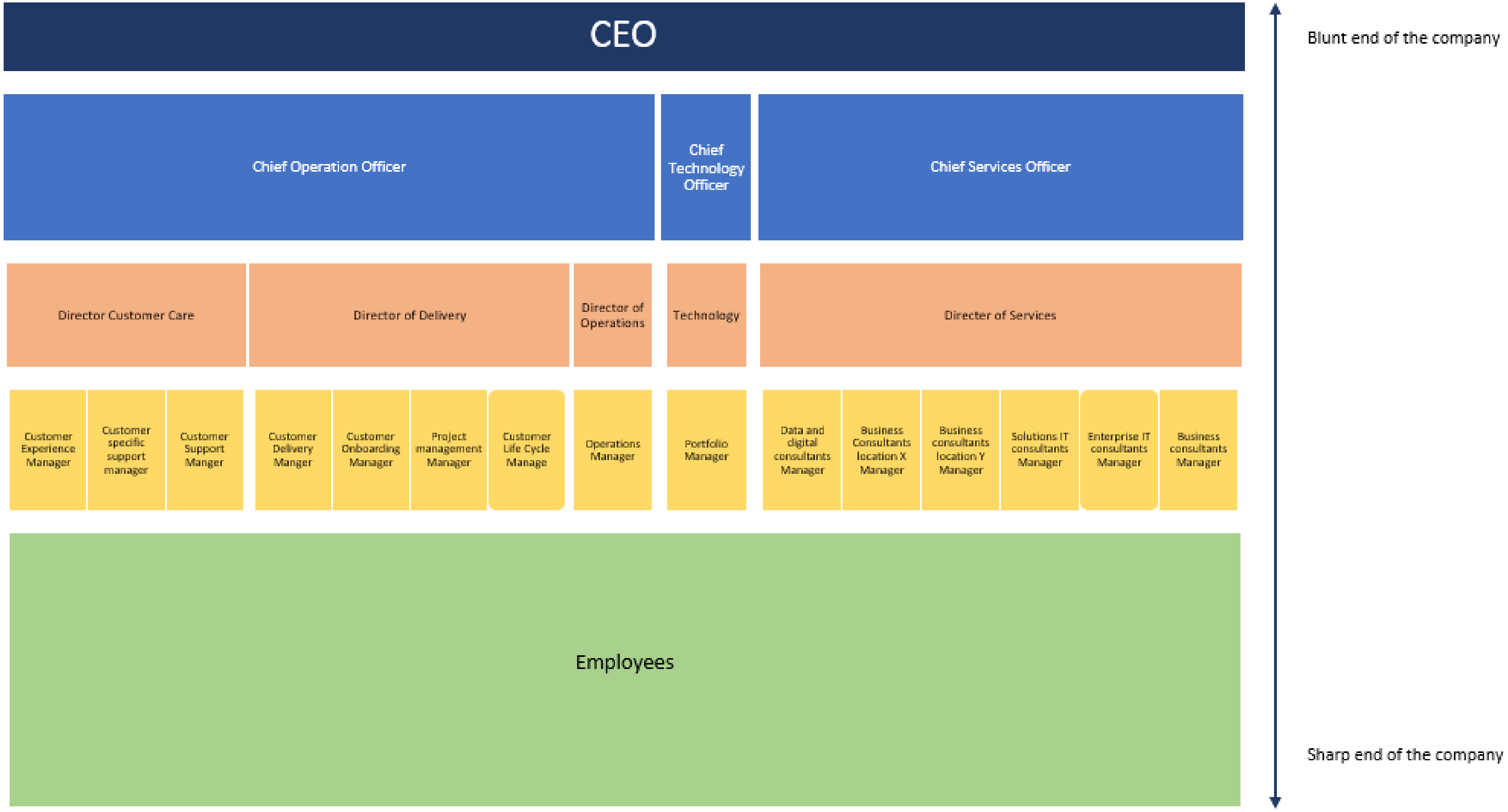
CEO
Chief Operation Officer
Chief Technology Officer
Chief Services Officer
Director Customer Care
Director of Delivery
Director of Operations
Technology
Directer of Services
Customer Experience Manager
Customer specific support manager
Customer Support Manger
Customer Delivery Manger
Customer Onboarding Manager
Project management Manager
Customer Life Cycle Manage
Operations Manager
Portfolio Manager
Data and digital consultants Manager
Business Consultants location X Manager
Business consultants location Y Manager
Solutions IT consultants Manager
Enterprise IT consultants Manager
Business consultants Manager
Employees
Blunt end of the company
Sharp end of the company

Figure 3 Hierarchical location of the survey respondents in the company.

I administered the survey through SurveyXact, a service provided by the company themselves. This ensured full anonymity of the respondents and secure information management, as well as giving me the opportunity to have control of the progress and easy access to the data. An email containing information about the study and a link to the questionnaire was sent out, with additional two sent email reminders. Mailed questionnaires are well known to have low response rate which is a risk when applying this approach to the data collection (Blaikie & Priest, 2019, p. 302). Using the company's layout for the questionnaire is seen as an advantage in increasing the response rate. There are other ways to increase the chances of higher response rate by the use of clear description of the scope and instructions, a good appearance and well-arranged simple formulated questions (Williamson, 2002, p. 239).

The previously mentioned *main questions* used for the interviews was used to create three *main themes* in the questionnaire for thematic and coding purposes. Each question is directly linked to the main questions used in the interviews, which helps me to be able to answer the research questions and link the data together from the different sources. The three main themes were:

1. *Cyber threats*
2. *Societal responsibility*
3. *Organizational aspects*

The questions was numbered from one to ten, organized after the theme along with predefined and thematic questioning for an easier data analysis (Williamson, 2002, p. 239). These predefined themes assisted me in coding the potential answers for the following data analysis. I chose to inform about a deadline (Williamson, 2002, p. 241), hoping this would encourage a quick reply. The duration of the questionnaire should also be limited to around 10 minutes, preventing the respondents to quit while in the middle of the questionnaire.

Out of 50 potential respondents, 22 percent answered: eight responded fully and three responded partially. Two email reminders were sent out, the day prior and at the day of the deadline. I will discuss this further in section 3.3 *Data reduction.* The respondents affiliation within the company was not important, the respondents were mainly selected due to fact that they were working at the sharp end.

Document analysis

To supplement the context provided through interviews and survey, an additional data collection was used. Document analysis is often used to supplement data collection through qualitative methods as interviews and survey (Bowen, 2009). Document analysis is defined by Bowes (2009) as *"… a systematic procedure for reviewing or evaluating documents […] Like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge"* (p. 27). Document analysis provides background and context to the chosen problem statement and can be used to verify empirical results from other data sources (Bowen, 2009, p. 29). The purpose of document analysis was to provide additional contextual data about the company related to the theoretical concepts of critical infrastructure, societal role, cyber threats, networking and resilience. The interviews revealed the use of noteworthy management systems, standards and policies which I used document analysis to elaborate on further.

There was an extensive number of possible documents to analyze, I chose to prioritize the governing documents and compliance documents, information from ISO and to further elaborate on addressed concepts like *competence*, *zero trust-principle* and *PDCA-cycle*. I did not provide a full analysis of the documents, instead I read the documents and used data that complemented the empirical results from the other qualitative data sources. The 13 documents analyzed are described in appendix D.

When conducting a document analysis, it is important to determine the authenticity, relevance and usefulness of the chosen documents. As I am an "insider" within the company it means that I already have access to company strategies and policies. It is important that I am constantly aware of my position as a researcher and to not be conflicted by my professional relation with the company as my employer. Documents that I have insight in can be confidential, restricted to internal purposes and have limitations regarding access and rights.

3.3 Data reduction and analysis

It is important to have a plan on how to reduce and analyze the collected data for the chosen qualitative research methods, prior to conducting the data collection (Kvale, Brinkmann, Anderssen, & Rygge, 2015, p. 140). Data reduction techniques will be used to manipulate the data to ensure a suitable form for analysis (Blaikie & Priest, 2019, p. 204). This section will elaborate on how the collected data through three different data sources was reduced and analyzed to generate meaning.

Data reduction

It was important to have a clear plan on how to collect, reduce and analyze the data before I started the data collection. Semi-structured interviews and survey generate extensive amounts of textual data that needs to be reduced after the data collection process. Data reduction is described by Blaikie & Priest (2019) as the *"… specification of, and justification for, the methods to be used to reduce and analyze the data"* (p. 27). The data reduction approach is dependent of what type of interviews, survey and documents are to be used. A useful technique to apply for data reduction purposes is to define clear coding/thematic categories before starting the data collection (Blaikie & Priest, 2019). Due to two requested interview participants did not answer my request and that I achieved a 22 percent response rate on the questionnaire, the data collection was drastically reduced. I knew there was a risk of having a low response rate, but I am satisfied with the outcome even if it was below what I expected. There are different possible reasons for this:

1. The respondents felt the questions was unrelated to their role and experience
2. The questions were badly formulated
3. The structure of the questionnaire was not encouraging the respondents to answer
4. The respondents were new to the company and had limited information about the topics (one employee sent an email to the survey-system stating this as a fact).

But I emphasize that the main reason behind the low response rate likely is that there was conducted a phishing campaign at the same time as the survey was sent out (the company regularly sends out fake phishing emails to test if their employees open illicit emails). The survey request was likely perceived as suspicious as it was sent from the SurveyXact system, instead of my personal email address.

When it comes to the document analysis, an extensive amount of data was available and could be deemed necessary one way or another. I chose to focus on the governing documentation and the compliance documentation related to the different standards addressed by the participants. This was a choice I took since I could not read all internal documentation due to limited time and that the documents were internal or confidential. It also took time to decide on what I could refer to as empirical results and how I could ensure the confidentiality of the company.

Data analysis

I organized questions in the interview guide and questionnaires using three main questions, or themes, based on the concepts introduced in the research questions and the main theoretical concepts introduced in chapter two. The three main questions[1] and sub-questions used in the interviews and questionnaire had a thematic analysis purpose. The answers to the sub-questions related to the three main questions was categorized together to generate meaning across the different sources of data (Braun & Clarke, 2016, p. 297). Thematic analysis was used to identify, analyze and interpret meaning from the qualitative data collected. The method is flexible in regard to the chosen sample size, data collection methods and meaning generation (Braun & Clarke, 2016, p. 297). It was important for me to decide on a functioning and easy data analysis method, as I am not an experienced researcher. A complicated data analysis method could affect the results if I was to misinterpret the process. The predefined themes and related sub-questions made it easier for me to organize the answers from the participants and respondents. This thematic approach assisted me in categorizing the potential answers of the research questions when analyzing the transcripts and the answers from the questionnaires. This enabled me to identify themes and variables across the multiple data sets and generate meaning from it, which was presented as empirical results.

The videorecording provides the opportunity for interpreting body language connected to the given answers. But due to the limited amount of time for the research to be completed this was overlooked. Instead I analysed the meaning based on the literal statements from the participants. I used the Microsoft built-in transcript service right after the interview ended. I continuously analysed the interviews to save time, since it is a time-consuming process. Transcribing is about changing the materialistic form and is a process of interpretation from oral data to written data (Kvale, Brinkmann, Anderssen, & Rygge, 2015, p. 204). In the transcripts the identity of the speaker is identified by our role using "I" (Interviewer) and "P#" (Participant 1 or 2), questions that I asked were identified using "Q", with an additional time stamp. An issue I encountered was that we did not talk in full sentences during the interview which is called *"sentence structure error"* by Braun and Clarke (2014, p. 163). Braun and

[1] 1) How does cyber threats affect the company? 2) How does the company perceive their societal role in the protection of national security? 3) Does the company follow any procedures/strategies to achieve resilience and reliability?

Clarke (2014) argue that spoken language rarely translate well to sentences. When reading through the transcript while watching and listening to the recording I removed non-semantic sounds like “am”, “mm”, “um” etc. and repeating words and added punctuations to aid readability. The use of punctuation can in fact alter the interpretation of the text, Braun and Clarke argues (2014, p. 163). But I experienced that this altered and easy interpretation of transcribing made it easier for me analyse and making sense of the interviews. When I had transcribed an interview, the analysis process started by the use of five steps to analyze meaning as described by Kvale and Brinkmann (2015, p. 232). I started by watching the recording and then read through the interview to get a full picture of the answers, then I identified the answers and coded them according to the sub-questions and the three main questions. I identified the natural meaning entities within each answer of the addressed main themes as simple and clear as possible. I tried to be as objective and open-minded as possible when interpreting and thematizing the answers. I investigated the meaning entity up against the purpose of the thesis and lastly, I summarized the themes in a descriptive answer. This assisted with data reduction, as unnecessary details are emphasized less.

The SurveyXact survey system coded and categorized the answers from the different respondents for me, which saved me some time. The questions asked was defined with the purpose to easily categorize the answers given. I exported the results to an excel document and divided each theme into different sheets. I used the same approach of analyzing the data from the questionnaire as for the interviews, but instead of taking one employee at a time, the analysis was conducted one theme at a time. I analyzed the meaning behind the answers of each question and I then summarized the meanings of the theme before moving on to the next theme and related sub-questions. This gave me an understanding of how the answers on each question and theme varied and I was thus able to identify the “extremes” and “standards”.

3.4 Ethical considerations

I have considered ethical aspects throughout my work with this thesis. Kvale and Brinkmann (2017, p. 102) addresses that there are four especially important areas to consider: informed consent, confidentiality, consequences and the role of the researcher. These areas will be addressed in this section.

Informed consent

The research interview as understood by Kvale & Brinkmann (2015, p. 35) consist of several ethical considerations and issues. To successfully conduct an interview is dependent on a social relation where the environment encourages safety and free speech. As part of the planning for the interview I formulated an informed consent form (appendix A) as encouraged by Kvale & Brinkmann (2015, p. 104). I sent out the form to the potential participants on email when reaching out to request their participation. The informed consent form included information about the research, how the interview would be conducted, how personal details and raw material would be managed, or information in case the interview participant wanted to withdraw from the research. Both participants stated that they thought it was important that the raw data would be deleted after censorship of the thesis. An informed consent form also has the purpose of ensuring that participants are voluntarily participating based on an informed basis. The informed consent form had to be signed prior to the start of the interview, one participant orally confirmed the voluntary participation at the beginning of the interview and sent the signed consent form afterwards.

The respondents of the questionnaire did not receive an informed consent form, it was deemed unnecessary as I would never interact with the respondents personally. I conferred with the HR department and used SurveyExacts built-in functions to ensure the respondents anonymity.

Confidentiality and consequences

It is important to have reflected on the possible consequences when conducting qualitative research methods (Kvale, Brinkmann, Anderssen, & Rygge, 2015, p. 107). The company is anonymized to prevent a negative impact on the company (cf. 3.1.1). This was decided after a careful consideration, as potentially revealing information can be exploited by threat agents. The reason for this is that threat agents start their investigations early when they plan their attacks. If threat agents search for the company's name on a search engine, this master thesis which is an open published master thesis, could come up as a potential search result if the name is mentioned. Even though I do not go into the technical details of the company's barriers and specific security measures in place. I still do not think it is wise to go out publicly with the company name and unintentionally expose the company to increased vulnerability. I think this was a smart choice, so that the master thesis can be published publicly right away instead of being withheld from the public for a brief period. This way the results can be used to contribute to academic research on societal safety.

After transcribation of one of the interviews, I offered to send the summarized answer from the analysis to one of the interview participants for a readthrough. This was due to disclosure of confidential information during the interview that was not to be included in any of the documentation related to the interview.

I had to constantly be aware of that the documents I analyzed were intended for internal or confidential use. This limits how I can refer to details from the documents, as I had to ensure the confidentiality of the company and the details, as well as not increasing the company's vulnerability towards threat agents who is interested in knowing more about the company.

Kvale and Brinkmann (2015, p. 106) address that it might be necessary to protect the participants identity using anonymity, but that it can also deprive them of the authority their voice is intended for the research. I wanted to show were the participants and respondents were located hierarchically in the organization and included a hierarchical illustration of both participants and respondents. The participants answers are not linked to their role, but it is likely possible the readers within the company understands who answered what, especially when there are only to participants. The names of the participants were excluded from the transcripts, they were instead referred to as CTO (Chief of Technology) and Director of Security in the thesis. When sending out the emailed questionnaire the respondents were informed in the email that they would have full anonymity even to me as a researcher, that personal details such as email address and their answers would be deleted after censorship of the thesis. No files include the email addresses and names of the questionnaire respondents, personal details are only kept in the SurveyExact system, which complies with GDPR.

My role as a researcher and my role as an employee could be conflicting, hence I had to be consciously aware of how this could affect my research and findings. I felt I managed to separate this well, as I resisted the temptation of adding details that are known to me but not possible to document. It is also important to me that the research adds societal value within the field of critical infrastructure, HRO and wicked problems. This is done even if the conclusions are negative or positive for the company.

3.5 Validation and reliability

As I have had a role as an insider while authoring this thesis, may make it difficult for other researchers to replicate the context and results of this thesis. I have had exclusive access to information that is not available to everyone. The collected raw data will only be accessible to the researcher, supervisor and examiner. Hence, raw data will not be available for other researchers to use for replication purposes. On the other hand, by following the reliability of the theoretical and methodological strategy and processes as presented in this thesis, other researchers can achieve comparable results in other companies (Kvale, Brinkmann, Anderssen, & Rygge, 2017, p. 276).

Validity is about how well the method(s) of choice worked for the purpose it was intended to (Kvale, Brinkmann, Anderssen, & Rygge, 2017, p. 276) I believe the choice of theoretical concepts and methods for data collection and analysis have worked well. It should be possible to recreate a similar research approach, though the results might be different in other companies. The company represents a large ICT-company with around 450-500 employees working in the segments oil & gas, renewables and ocean industries around the world. A large ICT-company are more likely to be involved with critical infrastructures as they host and supply to different customers, spread out in private and governmental sectors. Based on this, the company chosen for this study is central in the protection of national security, especially regarding the energy sector. By following the theoretical approach chosen for this thesis as a foundation for the creation of new research, similar research can be comparable. Similar research can highlight differences and similarities between companies within the ICT-industry.

3.6 The structure of the argument

This thesis involves different theoretical aspects with a varying degree of available academic research. The thesis seeks to incorporate central concepts of the debate as ICT-infrastructure, wicked problems, networking and knowledge sharing, resilience and HROs in relation to each other. It further seeks to investigate how private ICT-companies approach their role and responsibility in management of cyber threats as wicked problems. Based on that, critical infrastructures in one way or another is coupled and dependant on ICT-infrastructure, the increased frequency of complex cyberattacks, as well as that Norwegian national risk assessment places cyberattacks high on the list of importance. Based on this, the topic is considered very relevant for the ICT industry and society in general. How cyberthreats are managed by private companies that owns and operates ICT-infrastructure is highly useful to seek more knowledge on how to be better equipped for a more complex, technological and coupled world. It is interesting to investigate how top management level implements and ensures the sufficient management of cyber threats in strategies and policies in their company, and how their organization follows up these strategies and policies in day-to-day operations. How are these strategies and policies helping the organization to achieve a state of HRO, and are networking and knowledge sharing a strategic part of this?

The empirical results are presented in the next chapter *4. Analysis* by the help of the three defined main themes to answer each research question.

1. *The broad concept of cyber threats*
2. *Societal security as a commodity*
3. *A resilience discourse*

This structure ensures an analytical presentation of the data to be further discussed in relation to the theoretical concepts presented in the Theory (cf. 2).

4. Analysis

This chapter presents the data analysis of the empirical results in relation to chosen theoretical concepts: *critical infrastructure, wicked problems, networking and knowledge sharing, resilience* and *HRO*. This approach is applicable to the epistemological position *constructionism* introduced in the epistemology section (cf. 3.1). Which is based on the concept that the knowledge presented in this chapter is a product made out of how interview and survey participants interpret the reality and context of a phenomenon (Braun & Clarke, 2014, p. 30). The empirical results are a presentation of my own interpretations and understanding of the data collected to answer the problem statement (cf. 1.1) of this thesis:

> *"How do private ICT-suppliers perceive and define their role in protecting critical infrastructure?"*

I chose to study a large ICT-company with 330 employees located at their headquarter in Stavanger, Norway. There is in total 450-500 employees worldwide. The company have large oil and gas customers and customers in renewables and ocean industries. The purpose of having a case study of this company is to understand the in-depth organisational aspects of cyber threat management in a private ICT-company. The results are organised with the blunt end and the sharp end aspects in each section. The different perspectives will be set up against each other and compared to theoretical concepts.

In this chapter, I will first briefly mention the data sources and methods used for data collection (cf. 4.1). Secondly, I will introduce the results from the thematic qualitative analysis of the collected data (cf. 4.2). This constitutes an analytical conclusion (cf. 4.3) at the end.

4.1 Interviewees and survey participants

Data collection is a data triangulation between qualitative interviews, survey and document analysis. Two people from top-level management (blunt end) was interviewed and 11 employees (sharp end)) answered the survey, which resulted in 13 participants in total. The questions addressed can be found in Appendix B and C. Additionally, a document analysis was conducted of 12 documents to complement the other sources of data and further elaborate on concepts presented by the participants. A list of the documents can be found in appendix D.

Interview participants

The participants were interviewed in English via Teams. Seeing as the company is anonymized, I used the participants roles to provide authority to the answers, while still ensuring the participants anonymity (table 2).

Table 2 Overview of how interview participants is referred to as

#	Referred to as	Job	Job location
2	*CTO*	Chief Technology Officer	Stavanger, Norway
1	*Director of Security*	Director of HSEQ (Health, Security, Ethics & Quality)	Stavanger, Norway

One participant will be referred to by the well-known acronym *CTO* (Chief Technology Officer), to emphasize the responsibility and location of the participant in the hierarchy. The second participant will be referred to as *Director of Security*, this emphasizes the responsibility of the role and why it is relevant to the thesis.

Survey participants

A sample of 50 participants located at the sharp end of the company, with job location in Norway, were randomly selected. None of the participants have a managerial role in the company. All participants received an emailed questionnaire from the SurveyExact system, access was provided by the HR department. The response rate was 22 percent.

4.2 Results and discussion

This section will present the empirical results from the data collected about the chosen case and the theoretical concepts (cf. 2). The results are structured into three sections: Section 4.2.1 elaborates on the contradicting perspectives from the management and employees of the concept *cyber threats* within the company. Section 4.2.2 elaborates on how the company position themselves regarding *societal responsibility* and perceives their contribution of protection of national security. Lastly, section 4.2.3 elaborates on key theoretical concepts of *resilience* and *High reliability theory* and how these concepts is applicable to the company's chosen approach.

The overall finding is that the private ICT-company that I am studying, perceive their role as a critical supplier of cyber security to their customers. Making sure their customers can operate fully, XX perceives themselves as a contributing factor to national security.

4.2.1 The broad concept of cyber threats

This section elaborates on how the management and employees understand the concept and context of cyber threats (cf. 2.2.1) within the company. The empirical results will be used to answer the research question *"How are ICT-suppliers affected by cyber threats?"*. I have separated this section into two sub sections. Section 1 provides an understanding of what management and employees associate with cyber threats. Section 2 illustrates the different perspectives of cyber threat challenges between the blunt end and the sharp end.

The overall finding is that management perceive threats as a traditional broad concept, from unintentional environmental threats to intentional malicious threats. While the employees perceive cyber threats as operationalized malicious threats such as suspicious emails, links and attachments, social hacking and phishing.

Associations with the concept "cyber threats"

The interview participants were asked what the company associate with cyber threats. I find that management perceive threats as a broad aspect including all sorts of threats towards the company, both unintentional environmental threats and intentional malicious threats. As a multi tenancy company[2] and hosting provider, any individual or organization trying to get access to either one of their clients or the company itself is perceived as cyber threats. This perspective illustrates a corporate and individualized aspect of conceptualising cyber threats, not a societal perspective:

> *"Cyber threats are any individual or organization trying to get access to either one of our clients or XX itself. We are a multi tenancy [company], as a hosting provider we manage many customers"* (CTO).

An interesting point of view is addressed by the Director of Security who states that *"They [the threat agents] are not the problem as long as they are just threat agents. It's when they perform a threat it's a problem"* (Director of Security). I find it questionable that management do not perceive cyber threats as a problem until they have operationalized. According to the definition of a *crisis* by Boin et. Al (2016, p. 3) could cyber threats in their nature be a crisis, but it is not until someone perceives them as a crisis that it will be defined as such. It is when

[2] *"Multi-tenancy is a property of a system where multiple customers, so-called tenants, transparently share the system's resources, such as services, applications, databases, or hardware, with the aim of lowering costs, while still being able to exclusively configure the system to the needs of the tenant"* (Kabbedijk, Bezemer, Jansen, & Zaidman, 2015, p. 144).

actors perceive uncertainty different that certain types of problems arise. I interpret the employees as perceiving cyber threats as a problem, even before they have tried to operationalize. The possibility of receiving phishing emails that look realistic and are difficult to identify as illicit is mentioned as one of the biggest challenges for the employees and management:

> *"Phishing emails is something that I need to be aware of all the time. Other than that, I cannot say that I "feel" any imminent threat to the work that I do. But of course, I need to be careful and work by best practices as far as possible"* (Employee).

But the degree of worrying about this type of threat varies. Another employee feels a constant pressure of not being the one responsible for a breach: *"I feel pressure to not be the one to fall for a trick and take down the entire company"* (Employee).

Both management and employees agree that cyber-attacks can have serious consequences for both the company and their customers. It can be huge financial and reputational consequences for the company and their customers, for instance if they need to pay ransom to regain access to data or if they lose access to data completely. Cyber-attacks can lead to insurance claims or the Board of directors could be personally financially liable in case of a legal action. In case of accusations of bribery or corruption, data needs to be stored as evidence. Or the company can have compliance consequences if they do not comply to regulations demanded from the government and regulated through GDPR and the Norwegian Data Protection Authority (DPA). The Director of Security associate cyber threats with consequences for the company and emphasize the reason they are protecting the assets:

> *"If I understand your question right, I will focus on the consequence types. Because the reason why we protect our assets is because we want to avoid certain consequences. So, the first thing is obviously the financial [aspect], because if we have an attack, that will impact us in several ways also financially. The thing with the financial stuff is that you can buy an insurance, so that you are prepared. [...] But there are some other things you cannot have insurance for, and that's for instance the technology, understanding and skills and know-how, and then also the reputation. We cannot buy an insurance for reputation. You have compliance consequences. For instance, if we don't take care of personal data properly, we can have fines for that. But we also have an issue in other ways. A very important thing is that you need evidence for anticorruption. Anticorruption is very special because if you are accused*

> *of bribery or corruption, you need to prove that you have done everything right. So, you need to keep those data and it's very critical that we don't lose those kinds of data"* (Director of Security).

The perception of compliance *as a consequence* is questionable. If a company does not comply to regulations and policies and hence put their customers and the society at risk, it could cause serious harm to those who are affected. The consequence for the company is that they will be guilty in not performing their corporate security correct. Compliance is a tool to ensure companies operate in a regulated and controlled way. I also find it interesting that protection of assets is a widely understood concept, including not only personnel and physical assets, but also the reputational assets.

When asked what type of threat agents the company is experiencing, the Director of Security answers such as natural and environmental threats, single actors, a raging employee, competitors or nation states. This illustrates a traditional academic perception of the term threat in the concept of digital security (Jang-Jaccard & Nepal, 2014, p. 984). The Director of Security continues and state that *"you need to always look at the threat landscape to understand if there is anything now that is relevant [...] and protect you from that"*. Still, theoreticians such as Goessling-Reisemann and Their (2019) argue that not all threats are known. This means that even if it is emphasized to keep an eye on the threat landscape, the company still needs to consider threats that are *unknown*. Unknown threats are difficult to predict and to comprehend the impact, extent and the consequences of (Gößling-Reisemann & Thier, 2019, p. 118). Each day XX is facing *known threats* such as port scamming, automatic machine hacking or direct campaigns like CEO fraud. These types of threats are well known in today's society (Engen, et al., 2016, p. 154). These threats occur frequently and have been experienced in the past and are expected to be experienced again, hence these threats can be categorized as *known threats* (Gößling-Reisemann, 2016, p. 74). Day-to-day management see that end users, which are typically employees of customers, are exposed or compromised with crypto-ransomware, fake invoices and phishing attacks. Threat agents are getting more sophisticated every day, they speak and write fluent Norwegian, so it is difficult to separate an illicit email from other emails. The CTO addresses the academic and professional shift in how the uncertainty of cyber threats are perceived: *"A few years ago, you said "no, we will never be hacked". Now everybody says to you that you will be hacked".* I find that this statement illustrate that the possibility of a serious cyber-attack is a certainty, which further illustrate that management is not uncertain about the fact that they will experience a serious cyber-attack. It is more about the uncertainty of when.

It is my interpretation that this shift has influenced the demand and supply in the market, which have resulted in increased implementation of cyber security:

> *"…earlier when some customers were hesitant to implement two-factor authentication, we saw several of these fairly rudimentary attacks where they gained access to the individual's email or Skype accounts and then were able to intercept internal emails. Hopefully mostly a thing of the past, because the customers have understood that we can't always be so user friendly versus security. It's a fine balance, that I think [the customers] landed on"* (CTO).

I find this statement remarkably interesting. In recent years the amount of serious cyber threats has increased in the industry and government regulations have followed. Hence, customers likely do not have a choice other than to implement higher security which is not necessarily user friendly. Security enables the ability of companies to manage known and unknown threats (Engen, et al., 2016, p. 155). A signature feature of high reliability organizations (HROs) is that they experience attacks but they have the ability to not let that stop them from continuing with their daily operations (Weick & Sutcliffe, 2015, p. 95). The company and their customers are daily experiencing threats and attempts at cyber-attacks. But management seem to perceive this as an everyday thing. Another feature of HROs is that they prepare for the next big attack, they do not wait for it to happened before they react (Weick et. Al, 2008, p. 98). Which based on the daily attempts of cyber-attacks, the management is surprisingly little concerned of the unknown threats. Hence, they are extraordinarily little concerned about *uncertainty*.

It is important to see how management have conveyed their goals and values, as well as their perception of cyber threats, to the employees in the company working closest to the customers. The employees were asked how they take cyber threats into account when they perform their work tasks. The purpose of the question was to understands how the employees perceive cyber threats and mitigate them in their daily work. All the employees are taking cyber threats into account when performing their work tasks, one way or another. Most of the employees are especially aware of suspicious emails, links and attachments that they receive, especially regarding social hacking and phishing. The employees have a conscious relationship towards how they use the company devices. By only browsing familiar web pages or limit the use of company devices to work related communication. Access-, sharing- and password management are also mentioned as an important focus area. Examples of cyber threat measures employees can use while performing tasks is to have strong passwords, encrypted traffic, use of monitoring tools and other best practice configurations for physical and cloud installations. Which is exemplified by one employee:

> *"Having a constant awareness towards security while performing tasks. An example would be strong passwords, encrypted traffic, monitoring tools and other best practice configurations for new installations. Keeping awareness while going on with your daily work routine (email links, browsing etc.)"*.

One employee pinpoints the vulnerability of having physical hardware and cloud solutions when integrating security:

> *"I work much with integrations. I need to think about security and threats all the time since we are integrating both [on-premise] sources with cloud sources. It is important to maintain the security and integrity in all communications. Also, social hacking, like phishing, is a big problem that we need to be aware of"* (Employee).

I find that the employees contrary to the belief of management emphasizing their use of policies and documented routines in the company. The dialog shows that employees are performing their tasks based on best practices.

Perspectives on cyber threat challenges

The interview participants were asked how cyber threats can affect their customers and what management consider as the biggest challenges for the company in fighting cyber threats. The purpose was to understand the underlying reasons for why and how the company manages cyber threats. To understand this, different challenges and consequences needs to be addressed. Which also pinpoints how the company and employees perceive their role towards the company and their customers.

The Director of Security emphasize the importance of the cultural aspects in managing cyber threats and protection of assets and state that *"Information security is all about protecting assets"* (Director of Security). Assets are previously addressed as personnel, physical assets and reputational assets. To protect the assets, it is important to always look at the threat landscape to understand what is relevant to protect. Assets need protection to prevent threat agents from operationalize threats and utilizing vulnerabilities. The company use risk management and security management to define their assets, identify threats and always considering their vulnerabilities. A risk is the relationship between the threat, vulnerability of the assets(s) and the possible consequences in case of a cyber attack (Flynn, 2018b, September, p. 30). A resilience approach can be used to manage these risks to mitigate threats, were threats is a result of threats agents' intentions and their capability. Protection of assets can reduce vulnerability. Based on how management understands the criticality of their customers it is also difficult for them to reduce the possible consequences of a cyber-attack towards their customers. When prioritizing mitigative efforts of protection, this will increase the difficulty for threats actors to operationalize their threats.

The company goal is to understand the true value of their customers assets, which the Director of Security state is a challenging task: *"When it comes to the core problem, is that the people that work with the security, they need to understand what they are protecting".* This statement shows that the problem is not the cyber threats, but how to make their employees understand what they are protecting. If the employees do not fully understand the value of what they are protecting, are the management sufficiently communicating their views on stakeholder assets and cyber threats down in the hierarchy? The employees need to feel responsibility towards protecting assets. The Director of Security exemplifies this by further stating:

> *"When you're working in a company you don't have the same feeling about the values, so you know there is a database of critical information and if we lose that database, it's bad for the reputation and financials and so on. But as a technician you don't have any feeling about these databases, it is a database. I think that's the core problem, that if you don't feel the value you don't protect it as it is yours. You protect it because someone told you to and that is not the same"* (Director of Security).

One can interpret this quote as if the management are perceived by management to have a better *sense of value* than the employees working at the sharp end. I find that the employees certainly feel the sense of value of what they are protecting. When the employees were asked what they consider as the biggest challenges in fighting cyber threats in their role, fear of consequences was emphasized. One employee, with an admin role with access to customer's data, are remarkably aware of the exposed role they have towards cyber threats and the huge negative outcome if they are the victim of a cyber-attack:

> *"I have an admin-role which potentially gives me access to all the files in the customers organization, so all threats that could give unwanted access to my account*

> *like phishing and hostile viruses is challenges with huge potential negative outcome , but this is not a daily challenge"* (Employee).

Hence, it should not be taken for granted by management that those working at the sharp end have a lack of realistic view on the value of customers assets. Another employee address that it is in fact a challenge to educate users in customers organizations about security:

> *"[It is] normal to give externals access to Teams, SharePoint-sites, links and documents. So, the challenge here is to get the users educated on secure collaboration so that for example they are meant to share a document in a library, they don't share access to the whole library, but only the document"* (Employee).

This is reflected in the need of education and building awareness internally and towards the customers especially about best practice of security. One employee exemplifies this further by stating that:

> *"A more present challenge is to educate and inform the users in the costumers' organization about secure collaboration in Teams and other Microsoft tools. There is a lot of sharing of content with externals so the users must be updated at all time on how to share content at all times"* (Employee).

The need of constantly updating policies on access sharing and external access are also emphasized as important. I find that it is difficult for the employees at the sharp end to ensure that customers and their users have the necessary and sufficient understanding of security. Too much information could also demotivate the users and have the opposite effect. The internal challenges towards cyber threats are in fact stated by one employee as a bigger challenge than the external threats.:

> *"As Microsoft change their settings and systems the education must be updated and presented to the users. But there is a fine line here, too much information and education can make users demotivated and they could possibly neglect the information and education which leads to unsafe collaboration. So, to conclude I will say that the internal challenges are a bigger challenge than the external threats"* (Employee).

I find that the employees are apprehensive of that the customers do not understand the importance of good cyber security. Which can be a result of the fact that XX is *selling* cyber security and protection as a commodity to their customers. It is necessary to ensure the whole organization is consciously aware of external threats while remaining effective, structured and sustainable over a long period of time (Weick & Sutcliffe, 2015, p. 130). Which is something one employee exemplifies as challenging: *"Keeping up with constant evolving security threats and building cyber security awareness withing an organization"* (Employee). The CTO adds that the company do everything they can to have all the security, technology and standards in place:

> *"Our worst fear I guess is that [threat agents] could go into XX and then jump between customers. Of course, [this is] something we train for and design for will never happen. We do everything we can to have all the security, all the technologies out there and all the good ISO standards to ensure that everything we do is secured by design, and then we rehearse for worst case scenarios etc.".*

When asked how the company is implementing security by design, the CTO emphasize the skilled employees: *"it starts with skills and knowledge obviously, so that the developers are very much aware of the kind of the threats that are out there"*. While an employee address that it is an internal challenge to have the necessary competent resources: *"not enough focus due to too little resources with the right competence"*. In the management of resilience, the basic capacity is a factor that needs focus, as there must be prerequisites for a system to be able to offer its functions to their users. Enough trained and educated resources are prerequisites that needs to be in place (Flynn, 2018b, September, p. 33).

The problem with sophisticated threat agents is that they gather a lot of information and they can spend half a year preparing for an attack. Especially when it assumably take half a year for the attack to be detected:

> *"I think the average, I heard a couple of years ago, was that if you have an attacker in your network, the average time to detect them is 7 months. [Threat agents can] read a lot of data and do a lot of damage in seven months' time"* (CTO).

These cyber-attacks could, according to Goessling-Reisemann (2016, p. 74), be categorized as a *creeping threat* as they develop over time and remain undetected for longer periods of time. This is also characteristics of a *creeping crisis* as a wicked problem as understood by Boin et. Al (2020, p. 10). There is a high degree of uncertainty about when and how it started, they can potentially cause serious societal consequences and are subject to a varying degree of political, corporate or societal attention (Boin et. Al, 2020, p. 7). I find that management have a simplified approach to what cyber threats are. They are not focused on how to solve cyber threats as a transboundary wicked problem, they are rather focused on how they can manage and maintain cyber threats at the level they are today. This approach illustrates a lack of societal responsibility. A lack of societal responsibility is a big challenge for the society when trying to solve wicked problems. Especially when those involved have different perspectives on how to define the problem and how to solve it Waddock et. Al (2015, p. 996).

It is important for ICT-companies to have an extensive number of different barriers in place, in order to detect breaches early and contain them:

"…you need to have good systems in place that have a lot of barriers. So, if [threat agents] get in, they can't do much damage, [which is] down to the microservices […] and then the second thing is that you need to detect [the threat agents] when they are in" (CTO).

Having redundancy designed into their systems, having a high performance and continuous control are three important abilities to achieve resilience in an organization (Engen, et al., 2016, p. 153). These characteristics enables the company to manage uncertainty at an operational and tactical level. Keeping security configurations compliant and having the necessary defensive programming or defence mechanisms in place in-depth of the systems are also a challenge in fighting cyber threats, while developing services for the company and their customers. Which is addressed by one of the employees: *"Need to employ defensive programming / defense in depth when developing solutions"*. In this context the security is about the ability to manage the threats by technological development together with organizational adaptations (Engen, et al., 2016, p. 155).

Summary

Management perceive threats as a traditional broad concept (cf. 2.2.1), from unintentional environmental threats to intentional malicious threats. The employees perceive cyber threats as operationalized malicious threats such as suspicious emails, links and attachments, social hacking and phishing. Management perceive cyber threats as a problem to be managed and not necessarily to be prevented. While the employees are to a large extent focused on preventing cyber threats at all time by being aware and precautious. The outcome of this pinpoints a conflict between management and employees, with a positive result. Management have implemented a high level of uncertainty management at the sharp end, while focusing less on uncertainty and more on risk management at the blunt end.

Empirical results show that management perceive it as a problem how to make sure the employees understand what they are protecting. They have taken for granted that the employees do not understand the value and criticality of the customers assets. The results show that the employees working at the sharp end possess a realistic understanding of the value and criticality of the customers assets. If the employees were not to fully understand the value of what they are protecting, why is that? Are the management insufficiently communicating their views on stakeholder assets and cyber threats down in the hierarchy?

4.2.2 Societal security as a commodity

Societal security is the ability to plan, adapt and operate systems to avoid cyber-attacks and meet defined stakeholder requirements (cf. 2.2.1). How an ICT-company perceives their responsibility related to societal security is a key aspect of this thesis, which will be further addressed in this section.

The empirical results presented here will be used to answer the research question *"How does ICT-suppliers perceive their societal responsibility in the protection of national security?".* I have separated this section into three topics to give a better understanding of the context related to the concepts. Section 1 introduces the concept of critical infrastructure and the importance of digital security. Section 2 introduces key elements of the collaboration between the company and the Norwegian authorities. Lastly, section 3 will briefly discuss how the company adapts national strategies and standards on how to manage cyber threats into the organization.

The overall finding is that critical infrastructure, as how it is perceived by XX, is the criticality of their customers' ability to secure stable oil production and national income. They define themselves as a supplier of corporate security. Protection and security are a commodity to XX as they are not driven by the societal responsibility to protect the society from potential catastrophic consequences. Management do not emphasize that cyber threats can impact the society in terms of injuries, destruction, or loss of access to societal necessities. Employees contradicts this perception, as a failure on cyber threat management in XX can impact national security.

Societal responsibility and national security

The interview participants were asked how they consider XX to be important in the protection of national security. The CTO states that there can be differences in how ICT- or IT-companies are perceived as critical depending on the services they are supplying and their role towards their customers:

> *"If you call it IT- or ICT-company, that is many things. So of course, you have pure consultancy companies who develop new applications, whether they are critical or not depends on if they have an operational responsibility".*

Hosting providers such as XX are perceived as more critical, compared to companies who are pure consultancy companies or developing applications. XX have an operational responsibility, through hosting and suppling of ICT-services and data to large energy companies all over the world. This is an example of *deterritorialization and globalization*, where private companies are increasingly operating in international markets (Koppenjan & Klijn, 2004, p. 8). If the operation of an oil platform or several platforms are reduced, or production is stopped which would be a big problem. Due to the responsibility energy companies have today, the participants emphasize that XX as host and supplier, should be deemed as critical as well. I find that one participant questions what being defined as *critical* involves. The participant emphasizes their operational responsibility as critical for their customers. It is not clear how the participants perceive the outcome for the company if categorized as critical by the government towards their customers in the energy sector:

> *"I think if we served [power plants], we would have that particular infrastructure flag on us, but I don't think we have it. [...] with the responsibility of running gas customers today, that is something that you have to challenge. [...] The world needs energy and Norway need the income"* (CTO).

The management perspective indicates that the company is perceived as critical towards their customers to ensure production of oil and a stable national income. But they are not perceiving themselves as critical in the context of the protection of national security. The services supplied by XX enables the energy companies to do their work, which means that XX are an especially important part of the energy companies value chain. The Director of Security emphasize the need of stable oil production as a critical task in the society:

> *"As we all know, it's still a critical part of the society that we have this oil. So, if we don't provide IT-solutions and the data they need, they will have issues with their production. So, we enable our customers to their work, so of course we are a very important part of their value chain".*

I interpret the participants as perceiving XX as enabling their customers and having a critical role in ensuring that the Norwegian energy production is reliable. To maintain operation and employment on the Norwegian continental shelf is categorized as an necessary societal function (Justis- og beredskapsdepartementet, 2021).

The employees were asked how they think a cyber-attack on XX can be harmful to national security. I find the employees to mainly emphasize the possibility that threat agents can use XX company accounts for the purpose of hostile activity towards their customers. Which is supported by Engen et. Al (2016) who argues that *"... loss or significant changes in critical infrastructures [...] can have major consequences [...]. Loss or disruption of an organization can also create unforeseen interactions for others, depending on how closely organizations and sectors are linked"* (p. 139). I find that management and employees have the same perception of the company being critical to their customers. But what is contradicting is that the employees show a greater tendency to view the role of the company in a broader context related to societal responsibility. If threat agents succeed to get access to confidential information about their customers, then the results could be harmful to national security. *"Contact information can come in the hands of the wrong people that want to use XX accounts for hostile activities"* (Employee). A breach can cripple the nation's infrastructure and telecommunication in different business sectors, one employee remark: *"A cyber-attack on our company could cripple our nation's infrastructure and telecommunication in different types of business sectors"* (Employee). This statement is supported by Zio (2018a, September) who argues that critical infrastructure consist of natural gas and oil, as well as telecommunication (Zio, 2018a, September, p. 10). The statement also contradicts how management perceive their role in protection of telecommunication, or other critical infrastructures such as power supply and water supply. Top-level management have assessed it as unnecessary to be in contact with Norwegian authorities as the responsibility of these functions lies with the data center providers (Contact with authorities, 2020). Power supply, water supply and telecommunications are especially critical infrastructures and I find it questionable that management disclaim their responsibility for the protection of these functions. Which functions that are deemed as critical infrastructures are varying between nation-states, which could make it confusing for companies to understand their role in national or international protection (Newbill, 2019, p. 771). When there are different perceptions of criticality, then other problems may emerge. The management perceives the company as a critical resource towards their customers in the oil and gas sector, but not themselves as critical in a broader societal context. This can contribute to an emerging conflict between authorities and the company, regarding who is responsible for implementing security.

The employees were asked how a failure of cyber threat management in XX could impact the customers operations. The purpose of this was to see how the employees understands the importance of a reliable supply of services towards their customers. The employees are consciously aware of the importance of continuously reliable performance and delivery of services to their customers. Which I believe reflects a reliability culture within the company (Engen, et al., 2016, p. 153). A serious security incident and breach in the company XX can have catastrophic consequences for their customers: *"It could be [catastrophic] for our customers. All customers are dependent on their operations, and if we fail to meet the requirements to avoid incidents on this it can be severe"* (Employee). It can cripple their production and disrupt, halter, or completely stop their operations: *"Considering that most of our customers are dependent on their systems to keep their business going it would most likely cripple them"* (Employee) or, as another employee exemplifies it: *"It could be catastrophic for some of them, causing a huge loss of money if their operations are disrupted".* It could in worst case cause serious injuries: *"In worst case it can injure someone or something. It could also stop the production on the platforms".* If the customers are exposed to information theft or lose their data due to a breach in XX, it could end in extensive fines or legal actions. If the company, as a host and supplier, fail to meet the customer requirements to avoid incidents the consequences could be severe: *"We can become an insecure partner for our customers"* (Employee). This could damage the reputation of the company. It is my understanding that the reliability of XXs supply and hosting is crucial to maintain a good reputation and reliable operation for their customers. Reputation and trust cannot be insured, it is difficult to measure the value of trust and reputation. Hence, reliability cannot be replaced when first is damaged (Engen, et al., 2016, p. 153).

A breach in the company can also lead to a leak of classified information harming national security if it ends up in the wrong hands. *"If we are hosting governmental institutions, a security breach here could possibly lead to leak of classified information"* (Employee). Another employee state that *"Our company has access to a lot of different oil-platforms. Confidential information about these platforms in the wrong hands can be harmful to national security"* (Employee). The minority of the employees did either not answer, answered that they do not know or that the question was not applicable to them. As the employees are located at the sharp end, closely to the customers, I emphasize the need to increase awareness among the employees of how the company is positioned in the value chain of the energy sector. When asked about how to describe the value chain, the Director of Security answered that they are just one of many:

> *"I don't think there is a good answer to that, because we have different types of customers. Some customers are more or less on the top of the hierarchy because they don't have any they supply to, like the [companies] operating in the North Sea. They're on the top of the hierarchy and they use suppliers. So, we are a supplier somewhere down in the hierarchy".*

As previously stated in the theory, the digital value chain consists of an environment of different stakeholders like suppliers, supporting companies and organizations, authorities who imposes laws, regulations and policies, who all have requirements (Koppenjan & Klijn, 2004, p. 8). When a sector is defined as a "critical infrastructure" by the government, it also entails increased regulation from the authorities, which increases the costs for a company, which again likely would increase the price of the services supplied. But with more regulations for the private companies, they could also risk having more limitations to act. To expand the aspects of the ICT-sector as critical, private companies could also be more involved in policy making on a national level, possibly having the opportunity to influence further policy making. The different actors in the value chain are dependent of each other which illustrate another characteristic trait of the developing network society *increasing intertwinement* (Koppenjan & Klijn, 2004). Strategic alliances are built to share cost, spread risk or to help authorities achieve their policy goals, which intensifies the relationship between authorities and private companies. They need each other to fight cyber threats. But private companies and the authorities can have different perception of the problem and the solutions on how to solve it, which further illustrates *a wicked problem.* An interesting perspective is that customers need to be willing to pay for a higher level of security, or the ICT-suppliers have less incentives to develop more expensive solutions. Which further emphasize that cyber security is a commodity to XX and that the market demand is limiting their implementation of security:

> *"There is a lot of technology out there. There's a lot of skilled people, so we can always spend much more money on security. But of course, if customers would pay much more for a more premium security package, then we would [spend more money]. But of course, we know that [the customers] want to pay for a certain level of security.*

> *They're not willing to pay double […]. It's a balancing act, we have to be profitable whilst thinking about security"* (CTO).

This further implicates that the company is selling protection and is not driven by the societal responsibility to protect the society from potential catastrophic consequences. The market drive is also affected by government regulation, as companies seek to be cost effective and will like not implement higher level of security if it cost them too much, compared to what is the minimum level of security required through regulation and standards. All stakeholders have similar or different requirements that the company must comply to: *"In our company we have several stakeholders that the customers, the employees, the government, owners and so on, and they all have different requirements"* (Director of Security). These requirements are mainly regulated through GDPR and the Norwegian Data Protection Authority (DPA). Oil and gas companies are especially regulated and need to have a certain standard of IT-security, they are in fact more regulated than ICT-suppliers. Which means that, even if the supplier is not regulated just as strict, to be a provider to these companies it is demanded that XX comply to the same requirements:

> *"Our customers are more regulated than us, so they have regulations they need to comply to and we need to comply with the same regulations because we are providing to them. […] for instance, if you work on the Norwegian continental shelf you need to have a certain standard of IT-security. And to be able to be a provider, we need to comply to the same quality and security requirements",* Director of Security.

This is an example of the horizontal relations, as addressed by Koppenjan and Klijn (2004, p. 10), where there is an increased market driven relationship between authorities and companies and their suppliers. Government impose regulations, which companies need to follow, then those companies who deliver to them need to ensure that they supply services which also comply to those regulations. If regulations increase, the companies need to increase their security too. Those companies who supply to them can increase their investments in developing more secure designs to fulfil the demand. But the lack of regulation and governmental prioritization also decreases the incentives for private companies to increase their security. According to Flynn (2018b, September, p. 45) is resilience also an issue regarding competitiveness. As companies will likely choose their suppliers who strive to achieve resiliency, compared to those who do not. ICT-suppliers know that a higher degree of security is necessary to stay ahead of the threat landscape, but the perception of the necessary security is not the same with their customers. This is an example of that wicked problems are difficult to manage, when there is a distinction between available information and how the market perceive the importance of managing wicked problems (Lægreid & Rykkja, 2019, p. 2).

Collaboration with the Norwegian authorities

As previously addressed, those actors managing wicked problems are dependent on each other. Private companies need to comprehend that they need to take action that are beyond themselves and their experience. The use of networking societies and knowledge sharing are important tools to achieve this.

The interview participants were asked about how the company collaborate with Norwegian authorities in relation to cyber threats. The Director of Security emphasize that collaboration and cooperation are essential for them to protect assets. It also serves the essential purpose of discussing threat landscape and vulnerabilities to ensure that themselves and other companies are protected:

> *"That is very important. Of course, it's not only that we protect ourselves, but we also want other companies to protect themselves. Because, if the hackers succeed in one place, they will learn about that and use it other places. So, for us, it's very important to collaborate or cooperate about how to protect the assets and also to discuss the threat landscape liabilities. so, it goes both ways. we provide information and we get information about the national security quality"* (Director of Security).

It is not clear whether "other companies" involves competitors or mainly involves partners, or both. I find it interesting that the Director of Security emphasize that they want other companies to be protected, as management have previously given the impression that they are mainly concerned for their own customers. Either they do this with the purpose of societal responsibility or as a forced act of kindness through the collaboration with national authorities. As stated by Newbill (2019, p. 773), cyber-attacks on infrastructure systems are *testing grounds* to identify vulnerable targets or weak spots. To contribute to the protection of other companies in a broader aspect, reduces the vulnerability of other companies being exposed by experimental attacks, which again reduces the vulnerability in the sector. Companies benefit from other companies also being secure and protected, hence cooperation between companies and authorities are an important aspect to limit vulnerability.

When the CTO were asked who is responsible for collaboration with the Norwegian authorities, the CTO answers that that is the Director of Security. The responsibility of corporate security is designated with the information security management role of the Director of Security within the company. As XX operates internationally, they have also been assigned the Norwegian Data Protection Authority (DPA) as the lead supervisory authority in case of security incidents regarding information security breaches (Personal data breach notification procedure, 2021). Document analysis show that XX has a membership at the Norwegian National Cyber Security Centre (NCSC), they share information in terms of security incidents, notifications, alarms and running services supplied by NCSC (Contact with authorities, 2020). I find it likely that this is not fully based on voluntary participation by the company and that this is rather a requirement from the NCSC. The company also collaborate with the Norwegian National Security Authority (NSM). Collaborating with NSM is important due to the size of the company and the criticality of their customers. Collaboration between private companies and authorities as a *crisis coordination outcome* is about an observed collaboration according to Boin et. Al (2016, p. 63). This type of collaboration is about sharing of information, or integrated operation with joint coordination in case of incidents or as part of preparedness Boin et. Al (2016, p. 63). I find that it is important to the company to collaborate with Norwegian authorities and that this is something that goes both ways, but I interpret the collaboration as mainly finding place when there is an actual crisis. Collaboration is also about the management aspect, were they organize *"...collaborative processes within networks of actors involved".* Boin et. Al (2016, p. 63). The company also mentions that criminal acts is addressed to the police if observed or experienced. The Director of Security elaborates about the collaboration and cooperation:

> *"you can subscribe to information [from] the National Security Authority and you are also able to provide feedback. So, if you have issues yourself or you have some experience you want to share, you can do that. Or you are also able to have a contact person so you can contact directly"*

These interactions are mainly decentralized to be on a tactical level within the company when a crisis occurs. When asked if the company have an appointed person of contact, the Director of Security answers:

> *"Yes, but that's not myself [...]. But it's very often very technical, you have details about vulnerability. So, we have technicians for all kinds of technical issues. So, it*

> *depends on what kind of issue it is. The right person is in lead of protecting us for that specific vulnerability".*

The results from the document analysis shows that collaboration with authorities is documented and emphasized in the governing Management System (ISO 27001 Compliance Document, 2021). Work instructions for contact with authorities are in place with the purpose to define when and who the company should contact and how incidents are to be reported.

To understand how management have communicated this responsibility down in the organization, the employees were asked how they collaborate with the Norwegian authorities in relation to cyber security. Even though the company have documented the relationship towards national authorities, this was still not something the employees had experienced for themselves or had special knowledge about. I find that the collaboration with Norwegian authorities is not communicated broadly to the employees at the sharp end. As the employees have little knowledge of how the company is collaborating with national authorities.

Incorporation of national strategies and standards

When management was asked if and how the company is incorporating national strategies aimed at national security, the Director of Security answered that they do. XX comply to regulations through GDPR and DPA and best practice techniques from Norwegian authorities. National authority provides best practice techniques for how ICT-suppliers can protect their assets:

> *"Yes. They provide several best practice techniques for how you should protect your assets. You can look at these standards as the same thing, but [with] different wrappings".*

XX have chosen the ISO 27001 certification, which provides a description of the information security control mechanisms XX have in place to control their protection. The results from the document analysis show that ISO 27001 certification is an information security standard and is applied to the internal Information Security Management System (ISMS) (ISAE 3402 Type II, 2021). In accordance to GDPR do the compliance of ISO 27001 ensure that the company have appropriate security level (ISAE 3402 Type II, 2021). When asked if there is anything special with that one certification the Director of Security answered that: *"The most special thing is that it's well known all over the world, so if you comply to that standard most companies in the world knows what you're talking about".*

The company also have the ISAE 3402 Type 2 report, which involves independent third parties who audits the controls to prove that they conduct the controls they have stated that they have. Additionally, they have the ISO 9001 certification (Quality Management System). The difference between the ISAE 3402 Type II report and the ISO certifications, is that the certifications provides a description of the control mechanisms the company have in place to control their protection. It is emphasized by the Director of Security that it is especially important to have a framework to comply to:

> *"We have the controls and proof that we do the controls. So actually, that is a very important thing, you need to have a framework to comply to. Because you will never find out what to do yourself, it's too complicated. So, you need to work systematically and according to a framework".*

It is emphasized by the management that to manage security they need to work systematically and comply to a framework. But frameworks alone are not enough to manage wicked problems (Koppenjan & Klijn, 2004, pp. 10-11). Still, I find that management in an extensive degree emphasize their governing management system on how cyber threat management is incorporated in the company. This will be further highlighted in the next section (cf. 4.2.3).

To solve wicked problems can result in a broad and diverging amount of strategies between and within those actors who try to manage them, this illustrates a *strategic uncertainty* (Koppenjan & Klijn, 2004, pp. 12-13). When actors have different perceptions on how to manage wicked problems in their organization they can be easily overturned and put off track. The management in the company show that they have a risk based strategic approach to manage cyber threats and that they lack the strategic focus on uncertainty. Uncertainty is likely more emphasized by the authorities. The customers of XX emphasize a reliable service and security which enables their production of oil and gas, this is typical to high-technological and high reliability organizations. These organizations emphasize a combination of high risk, high resilience and high reliability strategies. Together all these actors provide complex interactions which further characterize wicked problems. This type of uncertainty is problematic to reduce and is likely impossible to eliminate.

Summary

The empirical results show that the management and the employees agree that the company is perceived as critical towards their customers, which enables their customers to have secure and reliable operations. Critical infrastructure in the context of how it is presented by XX, is that critical infrastructure provides stable oil production and national income. What the government perceive as critical infrastructure is perceived more as a commodity than a burden. Based on this, I find that management have interpreted societal security as a corporate logic. They are marketing themselves as a supplier of security to their customers. This is characterised by a market drive where security is sold as a resource to their customers and is not driven by a societal responsibility. Which is not necessarily a negative thing, but it means that the company is driven by the need of corporate security instead of being driven by their desire to contribute to the protection of national security. Based on how the company collaborates with the Norwegian authorities, has XX taken on the role as a mediator between the customers and the authorities. They supply their customers societal security and protection based on their customers' requirements from the authorities, hence they apply to the customers societal responsibility.

4.2.3 A resilience discourse

When it comes to resilience, I see that the company on one hand view cyber threats as something to be managed (cf. 4.2.2) and on the other hand something that can only be approached by becoming more resilient. This is illustrated by their risk approach versus uncertainty. Resilience is, in the literature (cf. 2.4), perceived as a solution to manage uncertainty in wicked problems. I find the same logic mentioned in the literature (cf. 2.4) as expressed in XX regarding uncertainty. This section explains the management and employees understanding of the organizational aspect of cyber threat management compared to theoretical concepts of *resilience* and *HRO* in the organization. Empirical results will be used to answer the research question *"Does ICT-suppliers have a conscious relationship towards resilience in their work to protect ICT-infrastructure and manage wicked problems?".*

I have separated this section into four topics to give a better understanding of the context. Section 1 presents the key aspects of how management have implemented cyber threat management in the organization. Section 2 illustrates the organizational structure when managing cyber threats. Section 3 elaborates how the company are able to prepare and adapt to new threats. Lastly, the section 4 address the concepts of knowledge sharing and networking as important tools to manage wicked problems:

1. *Incorporation of cyber threat strategies*
2. *Organizational structure of cyber threat management*
3. *Ability to prepare and adapt to new threats*
4. *Knowledge sharing and networking*

The overall finding is that there are contradictions between what management says they will do (strategies, policies, management systems, risk approach) and how they do it (employees, tools to manage uncertainty). I find that the company have a resilience management approach, but there is a lack of focus on uncertainty in the top-level management. Uncertainty is a key aspect of resilience and HROs. Instead, it is their employees and the implemented tools which indicates the high degree of uncertainty focus to manage cyber threats. I find this to illustrate a possible resilience discourse.

Incorporation of cyber threat strategies

It is important that strategies and information is communicated broadly within the organisation and that management encourage awareness among their employees. This way, the management highlights the important role of the employees in the organization. How an organization manage a cyber threat is a result of how well the resilience management strategy is prioritized in the organisation (Boin et. Al, 2016, p. 42). This section illustrates how management incorporates their strategies and encourage awareness.

The interview participants were asked how cyber threats are incorporated in company strategies. It is important to the company to have a strategy that points out the importance of having a good information security. It is emphasized by the CTO that it is very strategic for the company to have security on the top of the agenda. The Director of Security state that XX have a lot of internal policies on information security that must be complied to:

> *"Policies is something we have to do, [the policies are] our own laws that says that in XX you must comply with these policies. And we have a lot of policies which is related to information security".*

Both participants mention the internal KPIs (Key Performance Indicators) that measure that the company complies to the governing management systems different routines and standards. The CTO state that there are 16 strategic KPIs and that one of them is: *"…one of them [is] zero serious security threats"*. Document analysis shows that cyber threats are defined as *serious incidents,* such as virus and hacking impacting information security and stable operations (IT Service Continuity Plan, 2017). On the question about how the company is following any specific standards, the CTO provides an interesting aspect: *"Security comes out of quality, I guess. Then good procedures and processes".* When asked whether the participant perceives quality as a critical part of quality, the CTO answers: *"I think they go hand in hand"*. The CTO additionally mentions that the organization and the product development process are audited and regulated based on the ISO 9001 certification in addition to the ISO 27001 certification. Which is also recommended standards by Norwegian authorities[3]. The governing management system is designed to meet the requirements from stakeholders. Based on the ISO 27001 standard and ISAE 3402 Type II report (SOC 2), the governing management system contains of different layers for different requirements. The top level is the governance part within the company which sets a certain level of quality, security and ISAE standards to be incorporated down in the organization. Results from the document analysis shows that the ISO/IEC 9001 certification requires that the company have an internal Quality Management System (QMS), which XX have (ISAE 3402 Type II, 2021). Results also shows that the company have an extensive amount of documented and detailed routines, processes, roles, responsibilities and requirements in their governing management system. An emerging theoretical concept to manage wicked problems is *resilience*. As previously addressed, frameworks alone are not enough to manage wicked problems and to achieve a sufficient resilience management approach. A rooted organizational strategy is necessary to achieve resilience and high reliability. By *rooted* strategy I mean that governing strategies developed by management are incorporated in the organization, so that it is clearly reflected how the employees share the top management's visions, values and goals through the employees perspective and actions (Njå et. Al, 2016, p. 116).

I find, based on the document analysis that the company have a high risk-based approach and an incorporated Plan-Do-Check-Act (PDCA) cycle[4]-approach in their governing management system. This is part of the implemented ISO27001 and ISO9001 standards within the company (ISO 27001 Compliance Document, 2021). The PDCA-cycle consists of a continuous cycle process ensuring input and output through four stages. Which, according to the International Organization for Standardization (ISO, n/a), stands for:

[3] *"The security management system can advantageously be established on the basis of recognized standards for management, such as the ISO 9000 series and the ISO 27000 series"* (Nasjonal Sikkerhetsmyndighet, n/a).
[4] The PDCA cycle was developed in the 1950s by William E. Deming (Calder, 2013, p. 37)

1. *"Plan: set the objectives of the system and processes to deliver results ("What to do" and "how to do it")*
2. *Do: implement and control what was planned*
3. *Check: monitor and measure processes and results against policies, objectives and requirements and report results*
4. *Act: take action to improve the performance of processes"*

The company have organized the four steps into *planning, support & operation, evaluation* and *improvement* as illustrated in figure 4:

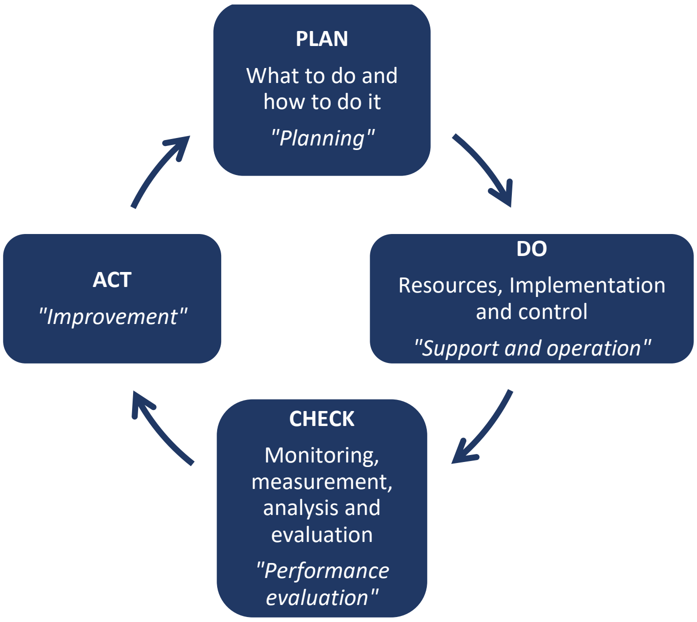
PLAN
What to do and how to do it
"Planning"
DO
Resources, Implementation and control
"Support and operation"
CHECK
Monitoring, measurement, analysis and evaluation
"Performance evaluation"
ACT
"Improvement"

Figure 4 PDCA cycle (Illustration based on Calder, 2013; ISO, 2016; ISO27001 Compliance Document)

Plan: *Planning* involves actions to address risks and opportunities by ensuring the management system establish, implement and maintain processes which either enhances wanted outcome, reduce or prevent unwanted outcome or achieves improvement.

Do: *Support* involves provisioning of the necessary and competent resources internally or from external parties, needed to establish, implement, maintain and ensure continual improvement of established internal processes. This involves mapping of existing and needed competence, security awareness, communication internally and externally, control of documented information. This will be further elaborated on in the section about networking and knowledge sharing. *Operation* involves continuous planning, implementation, risk assessments and control of processes in place. If incidents occur, processes should be reviewed or changed for mitigation efforts.

Check: *Evaluation of performance* and efficiency of the management systems through event logging, phishing campaigns, KPI measures, access management, awareness course and internal audits of standards. Top-level management is also applicable to ensure continuously compliance of the strategic direction of the company. Employees are informed about the results and documentations are updated.

Act: *Improvement* involves corrective action in case of deviations to control and correct them. Cause of deviations are identified, risks and opportunities are updated, changes are implemented and reflected in the management system. These results form the basis for further planning and the PDCA-cycle continues. It is important that strategies and information within the company is continuously updated or replaced if experience show that it is necessary (Boin et. Al, 2016, p. 42).

The resilience management approach includes how to design, manage and evaluate implemented mitigative tools in the organization (Lægreid & Rykkja, 2019, p. 1). A traditional risk approach is not able to capture the sufficient risks that exists towards ICT infrastructure (Gößling-Reisemann & Thier, 2019, p. 121).By implementing a PDCA-cycle approach the company is not only showing a high-risk adaptation, but also the ability to adapt to changing contexts (Waddock et. Al, 2015, p. 1007). It is not only about adaptation, but to illustrate the ability to focus on the capacity to be able to adapt, reorganize and recover from wicked problems (Zio, 2018a, September, p. 20). Which are necessary features of a resilient organization. Resilience management are applicable where problems, such as cyber threats, are difficult to detect, there is a low probability of a serious cyber-attack to operationalize and the potential impact could be catastrophic. Wicked problems, such as cyber-attacks, are experienced every day for the company and cyber threats are not perceived as a problem for the company unless they operationalize. The management do not comprehend the uncertainty of possibly serious cyber-attacks occurring; hence I find that they perceive the probability of a serious cyber-attack to be low. Instead, management perceive the consequences of a potential serious cyber-attack as critical, which the traditional risk management cannot adequately capture the extent of (Gößling-Reisemann & Thier, 2019, p. 118). Risk-driven adaptation is one of eleven key characteristics of HROs, as addressed by Engen et. Al (2016, p. 153). I would argue that the company inhabits a combination of risk and resilience management approaches, based on the empirical results.

To understand how the company recovers from incidents the employee perspective is important. I asked the employees about the biggest challenges they had experienced in managing former cyber threat incidents and what they were proud of. Most of the employees did not answer at all, some stated that the question was not applicable to them or that they had not been involved in any incidents they were aware of or could remember. I find it positive that most of the employees have not experienced a cyber threat. Those who had experienced a cyber security incident mentioned different scenarios: “The greatest challenge was coordination between different areas of expertise” (Employee). This statement was not elaborated further by the employee, which is a downside of having a questionnaire. Another example of a cyber threat incident was addressed in relation to the lack of access management: *“I discovered many accounts which should not have been in the system due to inactivity. I then made sure these were removed and made a process to gain control and remove inactive accounts from the system”* (Employee). I find it especially valuable for the company that the employees at the sharp end assist in developing routines based on experiences they have, thus help to limit the chance of such incidents happening again. Still, lack of access management could be a sign of deviation between intended control mechanisms and actual control. The need of constantly being aware of illicit emails was also addressed: *“Some of the emails that come through are very believable and hard to catch. I am proud that I seem to have an eye for identifying cyber security threats”* (Employee). I interpret the employees who had experienced incidents, was proud of their own ability to identify challenging issues, managing them in an efficient way and contribute to the security of the company. The organizational culture and the importance of a passionate and motivated employees are emphasized as crucial to the company’s security. These employees show organisational values that should be emphasized and encouraged by management. I interpret it as valuable for the company that the employees can assist in developing routines based on experiences they have, and thus help to limit the chance of similar incidents to happen.

Organizational structure of cyber threat management

The interview participants were asked who manage cyber threats in the company and where they are in the organization. The Director of Security answers:

> *“Myself, I am the [Director of HSEQ] and I'm the information Security Manager, it is part of the [Director of HSEQ] role. I am [responsible for] the strategic and security strategy document for how we should meet the stakeholders and clients when it comes to information security”.*

I interpret the two participants as having the same understanding of the organisational structure for managing cyber threats internally. The organizational structure in XX for managing cyber threats is split out in different areas. In XX everyone works with information security in one way or another. On the top level is the board of directors who are personally financially liable in case anything happens; they need to know all risks for the company and that they are managed and how they are managed. Then there is the CEO who are accountable for the information security in the company. The KPIs, previously addressed, are presented to the board of directors, whom the CEO reports to. The CEO is responsible when the company is faced with cyber threats. The day-to-day responsibility regarding cyber threats falls under the responsibility of the Director of HSEQ, who reports the performance of the information security and the governing management system to the CEO. There are three different governance boards that manage the tactical, strategical and operational aspects of security; The HSEQ Forum, Change advisory board (CAB) and Security Advisory Board (SAB). The company also have a security coordinator, security operations team and an incident response team if there is a situation, and a service continuity plan with an IT-continuity team to oversee the processes:

> *"We also have a Security coordinator and we have a security advisory board with members. We have a security operation team and we have an incident response team if there is a situation. We have [a] business continuity plan with an IT-continuity team on processes",* (Director of Security).

There are several employees in the delivery organization who manages cyber threats. Everyone in the company with responsibilities needs to investigate and identify risks related to information security and are applied to have a risk register:

> *"If you have a role that is responsible, you are also applied to have a risk register. So, by having a role you also need to investigate and identify risks related to information security",* Director of Security.

I find that the company have a hierarchical structure for management of cyber threats. With a combination of central and decentralized decision making to manage cyber threats, depending on the severity. Tactical and operational levels located at the sharp end of the company can manage different minor or medium incidents, but all risks or threats need to be reported in the risk register and up in the hierarchy. Serious threats and risks are reported by the executive management to board of directors, the management of the threats are delegated to different advisory boards and designated roles within the company. When it comes to contact with national authorities, the organization decentralizes the decision-making authority to the roles with best technical understanding and knowledge. This is according to Kruke and Olsen (2011, p. 2) consistent with research on HROs. On the follow-up question if anyone closer to the customers are manging cyber threats, the CTO answers that *“that's something that's part of all of the product and portfolio managers responsibility. It's not one person”.* The developers in the company are implementing security by design through skills, knowledge and awareness about the threat landscape and worst-case scenarios. The product delivery is documented and described on how to build and operate the products when delivered to the customer. This is supported by the Director of Security who state that:

> *“Everything starts with product security by design. If we have a product ID, our product process will take this product ID and transform it into a commercial product. A part of that process is to ensure that we commercialize a product that is also secure, so it starts with having a secure product. [...] Also, we have a lot of controls on the backside to understand the performance of the delivery, so we see that we actually protect [the customers] as we are supposed to”.*

Which means that developers in the company play a key role in fighting cyber threats and need to inhabit skills, knowledge and awareness of the threat landscape. Flexible management structures during management of serious incidents as cyber-attacks is one of eleven key characteristics of HROs addressed by Engen et. Al (2016, p. 153). The CTO further exemplifies: *“We do penetration testing for some of the key products and have very good results actually on that. So, it kind of proves that we are working in the best possible way”.* The company collaborate with third-party vendors for evaluating the company’s ability to manage different cyber threats and how their employees respond to different threats. The employees agree with management that external third-party penetration-testers are an important resource to the company: *“Follow the standard set by the company. [This is] important to enforce security best practices on infrastructure and code. External pen-testers are an important resource”.*

The employees were asked who they are collaborating with internally/externally regarding cyber threats. Most of the employees answered that they are using the information security management system (ISMS), inhouse experts, security manager, security consultants and technicians on matters related to cyber security and cyber threats. As exemplified by one of the employees: *“Whenever I need support on security matters, I contact the inhouse experts”.*

Both management and employees emphasize the importance of collaboration with cloud suppliers, along with discussions and cooperation with customers and partners, especially during an ongoing security incident: *"As we are delivering a lot of cloud solutions, it is important to cooperate with cloud supplier"* (Employee). The Director of Security exemplifies the collaboration with customers: "*And also, we discuss with customers, our customers. They often know very much about information security themself. So, we are able to discuss security in the nicety level".* While one of the employees emphasize the collaboration internally and with partners:

> *"Security threats are discussed in-between members of the security operations team and a notice is given to the one(s) responsible for running the service (sometimes the other way around). Partners might be notified for consultancy during an escalated incident".*

I find that these statements pinpoint that the company has a large internal competence base with the potential to be better utilized internally. Perhaps that these in-house experts arrange internal events (webinars, courses, training) which is not overly technical, hence targeted at the "average" employee. Even if the employees use of their time, this could be a low-cost initiative from the management to increase awareness on a regular basis.

The SANS Institute of Technology is mentioned by one of the employees as a current or potential collaborator in relation to cyber security. It is not clear whether the employee have a relation to SANS through personal initiative or through the company. The minority of the employees are either not collaborating with anyone or they do not have any opinions related to potential collaborators to the company.

The Director of Security emphasize that the organizational culture is an important aspect: *"You need a good culture. You need a good management system. Then you are well prepared for the future".* Good routines for operation are emphasized as necessary for the company to be well prepared, but this is also dependent on the employees in the company complying with the policies and processes:

> *"Security is much about the technology and things we need to protect, but those things change all the time. So, you cannot be an expert on technology because it will not last for long. But you have the same people. So, people are there, and they need to be motivated and feel that they help and is an important part of the security in their work"* (Director of Security).

When asked if culture is important to management of cyber threats, the Director of Security answers:

> *"It's the most critical thing. This, and the attitude or the passion for doing things in a good way to meet the stakeholder requirements. That's the core of doing business. If you're not passionate about your work and want to be good and skilled, you will not succeed".*

This shows that the company is dependent on their employees to be able to operate, while staying protected. For the company to succeed, management need to ensure that their employees are skilled and passionate about their work and encouraged to stay up to date. There are roles in the company which are not typical roles where one needs assistance with cyber threats. This might also be the reason why some employees do not seek internal collaboration on cyber threats. This points out, again, the need to raise awareness of the internal opportunities the employees have if they should experience a threat.

Ability to prepare and adapt to new threats

The ability to adapt and prepare is a key characteristic of HROs and is defined by their high degree of *resilience management* (Weick & Sutcliffe, 2015, p. 98). The interview participants were asked how they would consider the company's ability to prepare and adapt to potential new threats. The CTO state that the company strive to work in the best possible way and are very good at preparing and adapting to new threats: *"I can't say anything else than that I think we're very good at it. This is super important to us"*. It is my interpretation that management are perceiving the company as well prepared for cyber threats and cyber-attacks by having documented routines, available technology and their many skilled employees preparing and training for anything to happen:

> *"There are always new threats all the time, so that is, of course a problem. But we also use software and hardware that are made to meet those threats. So, by always have followed good routines for keeping the machines and hardware updated and new and also keep the software updated. We are well prepared for information security attacks. [...] Because we have documented this in the XX management system, we know how to always continue to improve to meet those threats. I think we are well prepared",* Director of Security.

By having tools in place to prevent, manage and detect threats illustrate a focus on uncertainty. Which is contradicting to what management have illustrated in previous sections (cf. 4.2.1). The combination of material structures and human aspects are what makes the system structure of resilience managements in organisations (Zio, 2018a, September, p. 27). It is important to have security systems in place like two-factor authentications to secure employees and customers users and devices. XX have a *zero trust-model*[5], which means they treat devices as external and keep them on the "outside" of their systems. In resilience management the system structure is a combination of both the material structures and the human organizational aspect involved in the operations (Zio, 2018a, September, p. 27). The systems that the employees are accessing must be secured to prevent any threat agents to gain access to the inside of the organization. The *zero-trust principle* is explained as:

> *"This zero-trust principle is that you don't trust any of your clients. This is a big change from the kind of the classic firewall guys where they said that "now we want to create a super secure shell. While you are on the inside of that super secure shell, we trust you". That is a big principle change. You shouldn't trust any devices like the mobile phones or PC's or Macs. You should keep them on the outside", the CTO.*

This principle involves the company having multiple barriers in place to prevent threat agents to gain direct access to systems, data centers and customers. If a threat is operationalized, they can be stopped and contained. This way the attack is compartmentalized and solved before the threat agents reach further into the system, they have then limited the impact of that attack. The perspective presented by the management is contradicting the theories that incidents can easily have consequences throughout an ICT-infrastructure system, as addressed by Engen et. Al (2016, p. 155). Even though an undetected threat of course could have catastrophic consequences if remained undetected for a longer period and hence have a catastrophic impact on customers, this is still not something which is as easily achieved by the threat agents. Boin et. Al (2020, p. 3) also argues that minor incidents and deviations could easily travel unnoticed through systems. I would argue that in the case of company XX, already known threats would likely be picked up by the complex tools consisting of different barriers and incidents- and detection mechanisms. It is therefore important to the company to always follow their routines for keeping machines, hardware and software updated and new:

[5] *"Zero Trust-architecture [..] is intended to make it as difficult as possible to compromise the entire infrastructure"* (PWC, 2020)

> *"…if you just keep it updated you are pretty much quite safe. But if you combine that with knowledge about how to put them together and then also [be aware of that] you maybe are the weakest point",* (Director of Security).

High Reliability Organizations (HROs) are proactive instead of waiting for an error to occur before responding (Weick et. Al, 2008, p.98). It is important to continuously improve to meet existing and new threats and to implement software and hardware that are made to mitigate those threats. Routines for identifying vulnerabilities and solutions and how to implement solutions is necessary. Persistent search for improvement is one of eleven key characteristics of HROs addressed by Engen et. Al (2016, p. 153). If there are vulnerabilities and there is a solution for it, it is important to implement the solution and if they do not - then they are vulnerable. The employees were asked how they consider the importance of persistent improvement in managing cyber threats and vulnerabilities. Most of the employees agreed with management that persistent improvement in managing cyber threats and vulnerabilities are important to the company. One employee emphasizes the importance of staying ahead: *"It is very important for the company and the employees to be on top of this subject"* and that this is *"…extremely important and shouldn't be taken lightly. There are new stories of cyber security incidents all the time"* (Employee). Another employee exemplifies why this is so important: *"The threats always changes and develops to outsmart us, so one must always strive to improve management of cyber threats and vulnerabilities".* As services, prevention mechanisms and cyber security measures need to evolve with the constant change in cyber threats along with necessary training to increase knowledge: *"Our services and its threat prevention measures has to evolve with the constant change in cyber threats"* (Employee).

This dialog show that the importance of implemented tools and that these tools are maintained to reduce the chance of a threat to operationalize are emphasized in the company. These tools reduce uncertainty in the company, which contradicts how management focus on uncertainty. The employee's perspective, emphasizes again, the possible use of a resilience discourse in the company, where management do not focus on uncertainty at the strategic level, but uncertainty is implemented in the operational and tactical level of the organisation. This discourse could pinpoint what Shaw and Maythorn (2013, p. 46) have illustrated in their research, that by including how management perceives and apply resilience thinking could reframe resilience as a concept.

Networking and knowledge sharing

Networking and knowledge sharing is introduced as tools to manage wicked problems (Koppenjan & Klijn, 2004, pp. 10-11). As previously addressed are organisational frameworks not enough to manage wicked problems, it is also dependent on the strategies being rooted in the organisation. Knowledge is information acquired through training or theoretical understanding which further builds competence within the organisation (Olsen & kruke, 2011, p. 2). Companies need each other to increase their knowledge, especially on concepts such as cyber threats. But knowledge sharing between different companies and organisations are affected by the uncertainty in between the networking participants. An uncertainty called *institutional uncertainty.* Between and within companies exists diverging organisational frameworks, dynamics and knowledge. This is due to different cultures, policies and perceptions within the company. Institutional uncertainty can be reduced by training and encouraging employees to stay up to date with their expertise (Koppenjan & Klijn, 2004, pp. 12-13). As the employees at the sharp end are working closest to the customers and the internal systems, the need of awareness and knowledge on the threat landscape and how to manage cyber threats is necessary. Networking and knowledge sharing involves a regulation of the information flow and a proactive provisioning of necessary and available data and information to the actors involved which in turn can enhance resilience (Zio, 2018a, September). This section will elaborate on how this is prioritized in the company.

The interview participants were asked how the company utilises networking and knowledge sharing in special interest groups, specialist security forums and professional associations to mitigate cyber threats. The CTO did not have any special knowledge of this subject, while the Director of Security answered that *"The information security is very divided into a lot of things, it's not possible to be an expert on security because it's too much. You can be expert in some areas".* Here it seems that there are contradicting views on the importance of networking and knowledge sharing in the top-level management. Results from document analysis show that the management have implemented a policy for strategic competence management for they employees. Here the company refer to *competence* as defined by Linda Lai (1997)[6]: *"…knowledge (to know), skills (being able to), abilities (having talent) and attitudes (whishing and wanting) that make it possible to perform functions and tasks in line with defined requirements and goals"* (Competence Management, 2020).

[6] Lai L., 1997. *Strategisk kompetansestyring* (1.utg.ed.). Bergen: Fagbokforlaget.

The Director of Security emphasize that to stay up to date their employees have the options of conducting *"…training internally and also externally, we join conferences and courses and webinars a lot"*. Each role in the company have a role description, which includes responsibility and how the employees should stay updated within their area of expertise. Private companies who sees the true value of collaboration reflects this in ensuring the company have the resources and competence which exceeds themselves (Waddock et. Al, 2015, p. 1003). As previously stated (cf. 4.2.1), enough trained and educated resources are prerequisites that needs to be in place in a company to manage wicked problems (Flynn, 2018b, September, p. 33). One employee addressed the concern of not having enough focus on cyber threat management in the organization due to limited competent resources on the concept. When the employees was asked about networking and knowledge sharing about cyber security, most of the employees answered that they had not participated in any interest groups, forums or webinars about cyber security, or they did not answer the question at all. I interpret this as networks about cyber security is not something that is widespread among the employees in the sharp end of the company. Which is inconsistent with the management perspective, where staying up to date is crucial to the company. The CTO are more focused on the actual internal training of their employees and emphasize that the best way to train is to have realistic tests with worst case scenarios performed internally and towards customers. The company is cooperating with third-party companies to conduct these tests. External parties are necessary to audit and test the company, as it is my understanding that the company would not be critical enough if they did it themselves: *"They need to audit us, if we do it ourselves, then we would perhaps be too nice and then you don't go deep enough"* (CTO). Networking and the participating roles are dependent on cyber security being discussed, but the participants need to be on the same technical level to understand each other. In the high-level segment they need to understand how to describe and understand roles wherever they are positioned in the organisation:

> *"If you are really into technical details, you need to be on the same level to understand each other. On my level, I'm working more with how to tell it in a simple way. Because we cannot be a technician in the high-level segment, we need to understand our role wherever we are in the organization. so, my work is more about building a security culture, a culture that understand how to utilize the XX management system"* (Director of Security).

Networking and knowledge sharing on strategic level is more about building a security culture, a culture that understands how to utilize the governing management system. This illustrates another type of uncertainty, the *substantive uncertainty* (Koppenjan & Klijn, 2004, pp. 12-13). When there is overwhelming amount of information, it can do more damage than good when trying to solve wicked problems. While the management emphasize their governing management system, it is likely that for management to fully rely on their employees to read their documentation could instead lead to more confusion and uncertainty. Substantive uncertainty can be reduced if the company prioritize training and encourage their employees to participate actively in networking societies (Koppenjan & Klijn, 2004, pp. 12-13). The employees were asked whether they had conducted any training in managing cyber threats or vulnerabilities, either on their own or through the company and it was varied responses: *"Been reading through the guidelines provided in internal documentation, as well as keeping current with OWASP recommendations"*[7] (Employee). Results show that those who received training, had mainly received training through the company. The employees mentioned phishing campaigns, annual awareness course, reading internal guidelines and documentation and presentation on security demands for vendors as types of training. These types of training are based on internal resources, which I find is mainly emphasized by the management. External training and certifications are regulated by management due to the cost, hence employees need to ask for permission to conduct such training (Competence Management, 2020). One employee remarked that they had received training but mainly on their own initiative: *"very little internally, but some externally specifically through SANS"*[8]. The minority of the employees answered that they had not undergone neither internal or external training in managing cyber threats or vulnerabilities. This was exemplified by one employee: *"The training in varying areas has been conducted by myself and not through company resources. Topics such as firewall, encryption, forensics, and specialized tools used within the company etc."* Another employee answered that they had conducted training on *understanding* cyber threats, not in *managing* them.

Those employees who had participated in a network or knowledge sharing event stated that: *"I have been to webinars about cyber security. Very important to get updates", "Webinars, forums and newsletters are great tools for keeping up with the evolving cyber security threats and tools for preventing mentioned threats. Community forums can help you detect and solve*

[7] Open Web Application Security Project-recommendations.
[8] SANS Institute of Technology

existing and new threats" and that *"I find them very valuable and enjoy hearing the real-life examples"*. It is also possible to receive important updates about new technologies, cyber security threats and tools for prevention management. Which is something I interpret as essential if the employees should be able to stay up to date on the threat landscape and how to manage threats. The company should encourage the use of networks and other information sharing tools to contribute to the employees staying up to date about cyber security. Still, it is important to reduce substantive uncertainty by balancing the amount of necessary information and too much information (Koppenjan & Klijn, 2004, pp. 12-13).

Summary

I find that the management of cyber threats reflects a resilience discourse, with a lack of focus on uncertainty at the top-management level but a strong indication of uncertainty management at operational and tactical level. While the company have implemented tools to manage uncertainty, the management perspective contradicts the focus on uncertainty. Their perception of cyber threats is that threats is only a problem if they operational, they are not focused on the uncertainty before a threat operationalized. They focus instead on how to manage threats when they are a problem, not as much as how to prevent them. Uncertainty is an important element in resilience and HRO theory, the employees and the implemented tools in the company reflects a strong presence of resilience thinking and uncertainty management. Management do not fully comprehend the value of how their employees and their tools manage uncertainty.

Management perceives it as important for their employees to stay up to date on the threat landscape and their competence. This is also implemented in their governing management system. Which contradicts how I find this to be prioritized down in the organization based on the lack of participation in networking societies, which can further reduce institutional uncertainty. There is an extensive amount of information in the governing management system, which I find to increase the substantive uncertainty in the organization. There is little mentioning of the organizational policies and strategies by the employees, but results show they still follow best practices.

Three characteristics is used to define HROs: awareness, decentralization and training. Employees at the sharp end illustrate awareness of cyber threats in their day-to-day tasks. Even if management are problematizing how their employees perceive value, they trust their employee's expertise. Employees are enabled by a planned decentralization to manage cyber threats at the tactical level and they are encouraged to address concerns up in the hierarchy. The employees are not encouraged sufficiently by management to participate in networking societies, to train or stay updated on cyber threats.

4.3 Analytical conclusion

The purpose of the analysis was to discuss my empirical findings against the main theoretical concept's *critical infrastructure, wicked problems* and *resilience* in order to answer the problem statement of this thesis:

> *"How do private ICT-supplier perceive and define their role in protecting critical infrastructure?".*

The main analytical take away is that the private ICT-company that I am studying, perceive their role as a critical supplier of cyber security to their customers. Making sure their customers can operate fully, XX perceives themselves as a contributing factor to national security.

This section will further present the analytical conclusions addressed in the above sections (cf. 4.2) and answer the chosen research questions of this thesis:

1. *How are ICT-suppliers affected by cyber threats?*
2. *How does ICT-suppliers perceive their societal responsibility in the protection of national security?*
3. *Does ICT-suppliers have a conscious relationship towards resilience in their work to protect ICT-infrastructure and manage wicked problems?*

How are ICT-suppliers affected by cyber threats?

In the case of XX, are they exposed to different cyber threats every day and so are their customers. Threat agents with malicious intentions are rapidly evolving and getting increasingly more sophisticated in their attempts. It is how the management and the employees perceive these threats that are contradicting. Management perceive threats as a traditional broad concept from unintentional environmental threats to intentional malicious threats that they need to manage. The employees perceive cyber threats as operationalized malicious threats that they are trying to prevent.

The blunt end is worried about the sharp end not understanding the true value of customers assets while the employees at the sharp end do understand the value of their customers assets. The outcome of this pinpoints a conflict between management and employees. Management have implemented a high level of uncertainty management at the sharp end, while focusing less on uncertainty and more on risk management at the blunt end.

How does ICT-suppliers perceive their societal responsibility in the protection of national security?

In the case of XX do they perceive their societal responsibility as being a protector of their customers assets. The services that the company supplies to their customers are perceived as critical in enabling their customers operations in the oil and gas sector. By enabling their customers and making sure they have a reliable production, is by XX perceived as a contributing factor to the protection of national security. I find that they have interpreted societal security as a corporate logic and market themselves as a supplier of security to their customers. In the case of XX, they might not be driven by societal security, but they use societal security as a strong argument for business. Which is not necessarily a negative thing, but I find this to illustrate that societal security is a commodity to the company.

Based on how XX collaborates with the Norwegian authorities, is it possible to state that they have taken on the role as a mediator between the customers and the authorities. They supply their customers societal security and protection based on their customers' requirements from the authorities, hence they apply to the customers societal responsibility.

Does ICT-suppliers have a conscious relationship towards resilience in their work to protect ICT-infrastructure and manage wicked problems?

Based on the analytical findings, is it my conclusion that in the case of XX they are not having a conscious relationship towards resilience management in their work to protect ICT-infrastructure and manage wicked problems. In the case of XX they have instead adapted a resilience discourse. Top-level management perceives cyber threats as something they must manage and is not paying much attention to the aspects of uncertainty. When it comes to managing cyber threats and risks, does the internal documentation show a lack of uncertainty-adaptation. Uncertainty is a key element in resilience and HRO theory. Management are instead showing an extensive *risk-driven* approach, where risks are regularly assessed and adapted in their governing management system framework. Cyber threats have become a daily thing and is not perceived as a problem, it is when a cyber threat operationalize that management sees them as a problem. This managements approach is contradicting how the organisation at the operational and tactical level are perceiving cyber threat management. Hence, management have been interpreted differently down in the organisation. As there is a strong indication of uncertainty management based on the incorporation of management tools and how employees reflect a reliability culture. The employees are emphasizing a persistent improvement and the importance of awareness on how a failure of cyber threat management in the company can affect their customers. By seeing the uncertainty and risk driven adaptation in relation to each other, emphasize that this resilience discourse can be perceived as a response to managing cyber security threats in the case of XX.

5. Discussion; main contradictions and how to move forward

This chapter is dedicated to the main contradictions that emerged in the analysis. The baseline is that we need to understand those contradictions to help the company move forward. These contradictions can be perceived as *organisational problems* that the management need to acknowledge before they can solve them. Based on the conclusions made in chapter 4, I will present the main findings and suggest how practices can be improved and managed in the future. The four main contradictions are organised in the following sections:

1. *Incorporation of uncertainty-adaptation in management*
2. *Shift from societal security as a commodity to a conscious societal responsibility*
3. *Reduction of substantive uncertainty*
4. *Utilization of networking societies*

First, I will address the contradictions presented in section 4.2.1 and discuss why the management should incorporate uncertainty at the blunt end.

Secondly, the contradictions in section 4.2.2 will be presented and discussed on how XX can contribute to the protection of national security.

Thirdly, the contradictions related to organizational management of cyber threats presented in section 4.2.3 will be addressed. This includes how to manage substantive uncertainty at the sharp end and that XX should utilize networking societies in a larger extent.

5.1 Incorporation of uncertainty-adaptation in management

How management understands their organizational efforts are mainly *risk-driven* and illustrate a high degree of an emphasis on their governing management system framework. The strategies, policies, management systems and their risk-driven adaptation show a lack of uncertainty-adaptation when it comes to managing cyber threats and risks. This is contradicted by how management have been interpreted down in the organization and by the employees at the sharp end. Where there is a focus on high performance, reporting of threats and incidents, risk-registers, continuous assessment and adaptions of implemented cyber threats mechanisms and persistent improvements. The employees are also found to be very conscious and aware about cyber threats, how they can prevent them as well as how a failure of this would impact their customers. These efforts are aimed at managing *uncertainty*, which is a key element in organizations with a resilience management approach.

Based on this, I find that the top-level management are communicating other goals and values down in the organization compared to what they perceive as their management approach. I believe that the top-level management is grateful for the high degree of uncertainty-adaption in their organization. As I find it likely that it has prevented serious cyber-attacks from operationalizing, but because of this it can unintentionally have affected how management place their priorities in their strategies as serious cyber threats are not occurring on a regular basis.

Due to these findings and my interpretations, I believe that the company will further benefit from incorporating an uncertainty-adaptation in their strategies. For the company to be able to fully comprehend the potential of having an increased focus on uncertainty, they also need to emphasize these efforts to be measured. By this I mean, that the company need to measure the product of their risk- and uncertainty-adaptions, which is *resilience.* As I have previously referred to (cf. 2.4), resilience can be perceived as a strategy to manage uncertainty as it prepares organizations and systems to manage *unknown threats.* A resilience approach also has the ability to manage risks by mitigating threats (cf. 2.4). With a strategic resilience approach rooted at the top-level management, it further enables the company to *investigate*, *identify*, *prevent* and *manage* wicked problems, such as cyber threats (cf. 2.4).

5.2 Shift from societal security as a commodity to a conscious societal responsibility

The employees at the sharp end show a greater tendency of perceiving the role of the company as important to the protection of national security, than the management. Employees emphasize that failures in cyber threat management could cause serious harm in terms of injuries, leak of sensitive information and breakdown of telecommunications. While the management, at the blunt end, instead perceive the role of the company as being a critical supplier of security to their customers in the oil and gas sector. Which management emphasize are important to ensure reliable production of oil and national income. By this, the management perceive this as a contributing factor to the protection of national security.

The term *critical infrastructure* emphasize conceptualises the relationship between how private companies are important to the protection of national security and how government takes responsibility and prioritize societal security (cf. 2.2). As I have stated previously, governmental regulations and prioritizations does not necessarily reflect which functions are critical in their nature (cf. 2.2). Norwegian authorities do not perceive companies such as XX as critical infrastructures, but the management in XX contradicts this by stating that they are in fact critical due to their role as host and suppliers of security to their customers (cf. 4.2.2). Even if management by this defines themselves as critical infrastructure, they show limited concern to the protection of national security. Instead they perceive societal security as a commodity, as something they can sell and earn money on, which is necessarily not a bad thing (cf. 4.2.2). By this I mean that, they are in fact providing solutions enabling companies to have an increased level of security in their performance.

If we look back at how the employees perceives the role of the company, it is not only about supplying a solution or a service. They show awareness of the need to take responsibility to reduce the vulnerability of national security. While the company is not emphasizing that their role is crucial in protection of national security as a broad term. This is probably also connected to how the company perceives cyber threats (cf. 4.2.1). The company is not managing cyber threats as a problem that needs to be solved or prevented in a context which exceeds themselves and their customers. Wicked problems, such as cyber threats, are not possible for governments, companies and civil society to manage on their own (cf. 2.3) if they aim to prevent serious cyber-attacks to happen. They are dependent on collaboration. XX is collaborating with the Norwegian government, but I find that they have taken on the role as a mediator between the customers and the authorities. Norwegian authorities implement regulations and companies need to comply to these regulations, then these companies are the customers of XX. Based on this, XX are also complied to the same regulations for them to provide security back to their customers. Then the customers have requirements to how much security they need and want (4.2.2). Out of this comes security as *a commodity*. Security is sold as a resource to their customers and is not driven by a societal responsibility.

That I have decided on excluding the company name from the thesis, is an interesting aspect to consider (cf. 3.4). This was done to ensure that threat agents could not search for information about the company online. It could be that the company are hesitant to contribute publicly in the fight against cyber threats, but I do not find that this is emphasized by the management.

If the company expands their perceptions on how cyber threats can affect the society as a whole and root their perception in strategies, then I think the company would contribute in a larger extent to societal responsibility and hence the protection of national security. Those customers who are high reliability organisations (HROs) could possibly perceive a change of mind by XX as something attractive.

5.3 Reduction of substantive uncertainty

The management in the company is emphasizing their extensive governing management system when it comes to managing cyber threats. The management system has a substantial amount of documentation of routines, processes, policies and work instructions (cf. 4.2.3).

In resilience management the organization and management of information is a key element, as information and knowledge are necessary for those who manage cyber threats. But the amount of information can both increase and decrease the uncertainty in the organization, which the latter is called *substantive uncertainty* (cf. 2.3.1). A characteristic with managing wicked problems, such as cyber threats, is the availability of information. Having a substantial amount of information is not necessarily the solution to reduce uncertainty, the same goes for how the information is interpreted by the reader. If management have an extensive amount of available information that have been formulated with a strategic purpose, this could in fact lead to more uncertainty at operational and tactical management.

I find it contradicting that the management emphasize their use of policies and documented routines when their employees do not emphasize the role of documentation when they are managing cyber threats in the company. Still, based on the answers from the employees it is my interpretation that the employees are performing their tasks while using best practices to prevent cyber threats (cf. 4.2.3). It is not clear whether this is corporate best practices or authorities' best practice and how they are used.

So, how can the top-level management ensure that information is contributing at the sharp end to the reduction of uncertainty in the company? It is important that employees know where to find information when they need it. The governing management system is not easy to maneuver in if you do not know what to look for (reference is made to the conducted document analysis). Hence it might be perceived as cumbersome by those employees who are more technical oriented than others, and these are the employees usually working at the sharp end in an ICT-company. For the company to be more user friendly in regard to their governing management system in the future, I suggest they regularly assess the employees needs related to information of how to manage cyber threats (4.2.3). Not only technical information on how to use tools, but also information that increases awareness of the importance of fighting cyber threats in terms of societal responsibility.

5.4 Utilization of networking societies

Another contradiction that has emerged from the results is how the employees is supposed to stay up to date on the threat landscape and knowledge. I find that management expects their employees to take responsibility of their own learning and is insufficiently encouraging their employees to participate in networking societies increase their knowledge. There is also a diverging perception of the importance of networking societies in management and in which extent they are used in the company, as one of the directors is not using it for themselves. Results show that most of the employees are not participating in networking societies about cyber threats, only a few have. For the employees to be encouraged to use networking societies and knowledge sharing can proactively provide necessary and available information to employees at the sharp end of the company (cf. 2.4), without too much hassle from the management. When encouraged and emphasized this could be perceived as a valuable resource of information to the employees. If the company, see the true value of *collaboration* (cf. 2.3.1) this will likely be reflected in their resources and their competence exceeds themselves. Results show that a challenge in the company is the lack of resources with the necessary competence on managing cyber threats. Which is inconsistent with the management perspective, where staying up to date is crucial to the company. When employees within the company, or within networking societies, possess different institutional backgrounds, it could lead to *institutional uncertainty* (cf. 2.3.1). If this thought is adapted to involve the internal institution, then this would be translated to employees having different tools, understanding, perceptions and background leading to different perceptions of the concept cyber threats. It is necessary to ensure that employees are trained and educated, as this is prerequisites (cf. 2.3.1) that needs to be in place to manage wicked problems, such as cyber threats.

To ensure the use of networking societies and knowledge sharing, the company need to prioritize that the employees are given time and resources to do so. At the same time, there are solutions available that are less time consuming and free of charge, such as webinars, forums, newsletters. Networking societies enables the employees with detecting and solving new threats, hear about real-life experiences and learn from them, stay updated on new technology and tools to manage cyber threats.

There are many factors involved to keep employees enthusiastic and interested, perhaps some employees do not care about cyber threats and feel it is not applicable to them. The management need to consider that there are different roles and people working at the sharp end of the company. To ensure a broad and rooted strategy to achieve "zero serious security incidents", the company need to prioritize a broad strategy of encouraging their employees at the sharp end to participate in networking societies. This will likely be reflected in a decreased level of *institutional uncertainty* where the employees possess a broad and varied background in their distinct roles. For the company to prioritize networking societies as tools for their employees (at all levels) to stay updated, this would also manage another contradiction that have been addressed (cf. 4.2.1): *the broad concept of cyber threats*. I believe that as the employees working at the sharp end also are those who manage cyber threats, is causing the employees to perceive cyber threats as operationalized threats that must be prevented. While top-level management who are deciding the company's values, goals and defining their strategies have a more broad and traditional perception of threats (cf. 4.2.1). This difference in perception of the concept *cyber threats* emphasize a key difference and the *institutional uncertainty* within the company. I think it is important for management to also participate in networking societies where cyber threats are perceived as something which must be prevented (cf. 4.2.3). Which again takes us back to the difference between what the company do and what the management say they do.

6. Conclusion

Based on the conclusions made in chapter 4 and 5, I would like to answer the chosen problem statement of this thesis:

> *"How do private ICT-suppliers perceive and define their role in protecting critical infrastructure?"*

The main analytical take away is that the private ICT-company that I have studied, entitled XX, perceives and defines its role as being a critical supplier of cyber security to their customers. Making sure their customers can operate fully, XX perceives themselves as a contributing factor to national security. Still, the company is not prioritizing protection of national security in their company strategies.

I have studied a single case, a private ICT-company, to answer the chosen problem statement. The chosen method was a qualitative method with the use of data triangulation of interviews, survey and document analysis. The purpose was to understand organisational aspects of cyber threat management. My role was to understand what was meaningful for the actors at the blunt end (top-level management) and the sharp end (employees at technical and operational level). The application of abductive logic was chosen to answer the research questions of this thesis. The actor's "world" was interpreted by me based on their knowledge and understanding of how things are, which is applicable to the epistemological constructionism approach. Analysis was conducted using themed questions for coding purposes.

I conclude that in the case of XX are they having a broad and traditional understanding of cyber threats which results in a few internal misunderstandings on how to manage the cyber threats. How the company perceive their societal responsibility is reflected internally on how they organise their own security. Based on the main contradictions, the company inhabits different types of uncertainty that needs to be managed for the company to be more resilient and to fully be able to be perceived as a high reliability organisation. They also need to prioritize the use of networking societies and knowledge sharing to broaden how the internal organisation perceive cyber threats.

In the case of XX, they construct themselves as a private company with a traditional risk-adaptation. But show instead a combination of risk- and uncertainty-adaptation, which illustrate that the company in practice have a resilience management approach. With the existing focus of uncertainty on operational and tactical level, in the case of XX, they should be able to measure resilience. This is something the company need to pinpoint in the organisation and the adaptation needs to be strategically incorporated at top-level management. A resilience-adaptation is dependent on how the top-level management will go about to measure accurate resilience and uncertainty in the organisation.

6.1 Further research

Based on the analytical results from the conducted research, I encourage further research on how ICT-companies, such as XX, incorporate and measure risk- and uncertainty adaptations in their strategies and internal organisation. It would also be interesting to further research the prioritization of networking societies to increase societal responsibility in ICT-companies. As an increased use of networking societies could strengthen the fight against cyber threats and further increase the protection of national security.

References

Bergsjø, H., Windvik, R., & Øverlier, L. (2020). *Digital sikkerhet.* Oslo: Universitetsforlaget.

Blaikie, N. (2007). *Approaches to Social Enquiry: Advancing Knowledge* (2 ed.). Cambridge: Polity.

Blaikie, N., & Priest, J. (2019). *Designing social research* (3 ed.). Cambridge; Medford: Polity Press.

Boin, A., Ekengren, M., & Rhinard, M. (2020, April 12). Hiding in Plain Sight: Conceptualizing the Creeping Crisis. *Risk, Harzards & Crisis in Public Policy, 11*(2), pp. 116-138. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/rhc3.12193

Boin, A., Hart, P., Stern, E., & Sundelius, B. (2016). *The politics of crisis management: Public leadership under preassure* (2 ed.). New York: Cambridge University Press.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40. Retrieved from http://ngsuniversity.com/pluginfile.php/134/mod_resource/content/1/DocumentAnalysis.pdf

Bradburn, N. M., Sudman, S., & Wansink, B. (2015). *Asking Questions: The Definitive Guide to Questionnaire Design -- For Market Research, Political Polls, and Social and Health Questionnaires* (2 ed.). John Wiley & Sons.

Braun, V., & Clarke, V. (2014). *Successful qualitative reserach.* London: SAGE Publications.

Braun, V., & Clarke, V. (2016, December 9). Thematic Analysis. *The Journal of Positive Psychology, 12*(3), pp. 297-298. Retrieved from https://doi.org/10.1080/17439760.2016.1262613

Bryman, A. (2008). Of methods and methodology. *Qualitative Research in Organizations and Management: An International Journal, 3*(2), pp. 159-168. Retrieved from www.emeraldinsight.com/1746-5648.htm

Calder, A. (2013). *ISO27001/ISO27002 A pocket guide* (2 ed.). Cambridgeshire: IT Governance publishing.

Colding, J., Barthel, S., & Sörqvist, P. (2019, November 7). Wicked Problems of Smart Cities. *Smart cities, 2*(4), pp. 512-521. Retrieved from https://www.mdpi.com/2624-6511/2/4/31

DSB. (2015). *Risikoanalyse av «Cyberangrep mot ekom-infrastruktur» – delrapport til Nasjonalt risikobilde 2014.* Direktoratet for samfunnssikkerhet og beredskap. Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/risikoanalyse-av-cyberangrep-mot-ekom-infrastruktur.pdf

DSB. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Direktoratet for samfunnssikkerhet og beredskap. Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

DSB. (2019). *Analyser av krisescenarioer 2019.* Direktoratet for samfunnssikkerhet og beredskap. Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Engen, O., Kruke, B., Olsen, O., Olsen, K., Lindøe, P., & Pettersen, K. (2016). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm.

European Commission. (n/a). *Who does the data protection law apply to?* Retrieved March 14, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

Fischer, L., & Lehnhoff, S. (2019). IT security for functional resilience in energy systems: effect-centric IT security. In M. Ruth, & S. Gößling-Reisemann, *Handbook on Resilience of Socio-Technical Systems* (pp. 316-340). Edward Elgar Publishing Limited.

Flynn, S. E. (2018b, September). The Future of Infrastructure and Resilience. *System thinking for critical infrastructure resilience and security - OECD/ JRC Workshop.* Paris. Retrieved from http://www.oecd.org/gov/risk/Stephen%20Flynn_Keynote.pdf

Gundersen, M., & Grut, S. (2021, March 9). Microsoft Exchange: La igjen bakdør hos trøndersk kollektivselskap. *NRKbeta*. Retrieved from https://nrkbeta.no/2021/03/09/microsoft-exchange-la-igjen-bakdor-hos-trondersk-kollektivselskap/

Gößling-Reisemann, S. (2016). Resilience – preparing energy systems for the unexpected. In M.-V. Florin, & I. Linkov, *IRGC Resource Guide on Resilience* (pp. 73-80). Lausanne: International Risk Governance Council. Retrieved from https://infoscience.epfl.ch/record/228206

Gößling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures. In M. Ruth, & S. Gößling-Reisemann, *Handbook on Resilience of Socio-Technical Systems* (pp. 117-135). Edward Elgar Publishing Limited.

Haavik, T. K., Antonsen, S., Rosness, R., & Hale, A. (2019, August). HRO and RE: A pragmatic perspective. *Safety Science, 117*, pp. 479-489. Retrieved from https://www.sciencedirect.com/science/article/pii/S0925753516301722

ISO. (2015). *The process approach in ISO9001:2015.* Retrieved from International Organization for Standardization: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso9001-2015-process-appr.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), pp. 973-993. Retrieved from https://www.sciencedirect.com/science/article/pii/S0022000014000178

Jibilian, I., & Canales, K. (2021, February 25). Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal. *Insider*. Retrieved from https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2011). *Forskningsmetode for økonomisk-administrative fag* (3 ed.). Abstrakt Forlag AS.

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security. *European Journal for Security Research, 4*, pp. 157-174. Retrieved from https://link.springer.com/article/10.1007/s41125-017-0021-9

Justis- og beredskapsdepartementet. (2021, April 28). *Liste over virksomheter med kritisk samfunnsfunksjon og nøkkelpersonel.* Retrieved from https://www.regjeringen.no/contentassets/8da70b8196a24296ae730eaf99056c1b/liste-over-kritiske-samfunnsfunksjoner_oppdatert.pdf

Jaatun, M. G. (2015). *Security in Critical Information Infrastructures [PhD Thesis University of Stavanger no. 254].* Retrieved from Brage: https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/293101/Martin_Gilje_Jaatun.pdf?sequence=1&isAllowed=y

Kabbedijk, J., Bezemer, C.-P., Jansen, S., & Zaidman, A. (2015, february). Defining Multi-Tenancy: A Systematic Mapping Study on the Academic and the Industrial Perspective. *Journal of Systems and Software, 100*, pp. 139-148. doi:https://doi.org/10.1016/j.jss.2014.10.034

Koppenjan, J. F., & Klijn, E. H. (2004). *Managing Uncertainties in networks. A network approach to problem solving and decision making,.* London: Routledge. Retrieved from https://www.researchgate.net/publication/200026701_Managing_Uncertainties_in_Networks

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. (2015). *Det kvalitative forskningsintervju* (3 ed.). Oslo: Gyldendal akademisk.

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. (2017). *Det kvalitative forskningsintervju* (3.3 ed.). Oslo: Gyldendal Akademisk.

Langved, Å., & Kibar, O. (2021, February 18). *Norway's 11179 billion NOK wealth fund affected by the SolarWinds hack.* Retrieved from Dagens Næringsliv: https://www.dn.no/teknologi/oljefondet/hacking/solarwinds/norways-11179-billion-nok-wealth-fund-affected-by-the-solarwinds-hack/2-1-964180

Lægreid, P., & Rykkja, L. H. (2019). Governing and organizing for crisis managment and civil protection: Advancing and improtant but neglected research field. *International Public Management Review, 19*(2), pp. 1-6. Retrieved from https://bora.uib.no/bora-xmlui/bitstream/handle/1956/21609/387-1715-1-PB.pdf?sequence=3

Nasjonal Sikkerhetsmyndighet. (n/a). *Veileder i sikkerhetsstyring.* Sandvika: Nasjonal sikkerhetsmyndighet. Retrieved june 11, 2021, from https://nsm.no/getfile.php/132933-1591350417/Demo/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf

Newbill, C. M. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies*, *26*(2), pp. 761-780. Retrieved from https://www.repository.law.indiana.edu/ijgls/vol26/iss2/11

Njå, O., Sommer, M., Rake, E. L., & Braut, G. S. (2020). *Samfunnssikkerhet: Analyse, styring og evaluering.* Oslo: Universitetsforlaget.

Norwegian Ministeries. (2019). *National Cyber Security Strategy for Norway.* Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

NSM. (2019). *Helhetlig digitalt risikobilde 2019.* Nasjonal Sikkerhetsmyndighet. Retrieved from https://nsm.no/getfile.php/133669-1592830841/Demo/Dokumenter/Rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

Nystuen, K. O. (2020, March 20). Hva er infrastruktur? – en tur gjennom begreper, hva begrepene kan bety og ikke minst noe om kompleksitet. *UiS, SAM500 Forelesning 20. mars 2020: Et helhetlig perspektiv på kritisk infrastruktur* (pp. 1-26). Stavanger: Forsvarets forskningsinstitutt.

OECD. (2020). *Enterprises by business size (indicator)*. Retrieved november 14, 2020, from https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm

Olsen, O., & kruke, B. (2011, October). Knowledge creation and reliable decision-making in complex emergencies. *Disasters: Journal of Disaster Studies, Policy & Management, 36*(2), pp. 212-232. Retrieved from https://www.researchgate.net/publication/51712715_Knowledge_Creation_and_Reliable_Decision-making_in_Complex_Emergencies

O'Neill, P. H. (2021, March 6). Four new hacking groups have joined an ongoing offensive against Microsoft's email servers. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/2021/03/06/1020442/four-new-hacking-groups-microsoft-email-servers/

Perrow, C. (1999). *Normal accidents: Living with high risk technologies.* Princeton, New Jersey: Princeton University Press.

PWC. (2020, November 4). *Zero Trust-arkitektur: gjør det skyen din sikrere?* Retrieved from https://www.pwc.no/no/pwc-aktuelt/zero-trust-arkitektur.html

Reason, J. (1997). *Managing the risks of organizational accidents.* Aldershot: Ashgate.

Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World.* London: Routledge. doi:https://doi.org/10.4324/9781849772440

Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences, 4*(2), pp. 155-169. doi:https://doi-org.ezproxy.uis.no/10.1007/BF01405730

Ruth, M., & Gößling-Reisemann, S. (2019). *Handbook on Resilience of Socio-Technical Systems.* Cheltenham, Gloucestershire: Edward Elgar Publishing.

Shaw, K., & Maythorne, L. (2013). Managing for local resilience: towards a strategic approach. *Public Policy and Administration, 28*(1), pp. 43-65. Retrieved from https://journals.sagepub.com/doi/10.1177/0952076711432578

Stark, A. (2014). BUREAUCRATIC VALUES AND RESILIENCE: AN EXPLORATION OF CRISIS MANAGEMENT ADAPTATION. *Public Administration, 92*(3), pp. 692-706. doi:https://doi-org.ezproxy.uis.no/10.1111/padm.12085

Sterud, K. (2021, March 13). Seks hackergrupper utnyttet Microsoft-sårbarhetene før de ble kjent. *NRKbeta*. Retrieved from https://nrkbeta.no/2021/03/13/seks-hackergrupper-utnyttet-microsoft-sarbarhetene-for-de-ble-kjent/

Sørensen, J. L. (2017). Samfunssikkerhet og beredskap: Det norske beredskaps- og krisehåndteringssystemet. In E. Krisiansen, L. I. Magnussen, & E. Carlström, *Samvirke: En bok i beredskap.* Oslo: Universitetsforlaget.

Ulsch, N. M. (2014). *Cyber threat! : how to manage the growing risk of cyber attacks.* Wiley.

Waddock, S., Meszoely, G. M., Waddell, S., & Dentoni, D. (2015). The complexity of wicked problems in large scale change. *Journal of Organizational Change Management, 28*(6), pp. 993-1012. doi:https://doi.org/10.1108/JOCM-08-2014-0146

Weick, K. E. (2001). *Making sense of the organization.* Oxford: Blackwell.

Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the unexpected : Sustained performance in a complex world* (3 ed.). Hoboken, New Jersey: Wiley.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. In A. Boin, *Crisis Management: Volume II* (pp. 31-66). Sage. Retrieved from https://theisrm.org/public-library/Boin%20-%20Crisis%20Management%20(Book).pdf

Williamson, K. (2002). *Research Methods for Students, Academics and Professionals.* Witney: Elsevier Science & Technology.

Yin, R. K. (2018). *Case study research and applications: design and methods* (6 ed.). Los Angles: Sage publishing.

Zio, E. (2018a, September). A Systemic View to Critical Infrastructure Resilience. *System thinking for critical infrastructure resilience and security - OECD/JRC Workshop.* Paris. Retrieved from https://www.oecd.org/gov/risk/enrico-zio-session-one.pdf

Appendix A Informed consent form for interview participants

"A study of organisational aspects of cyber threat management in a private IT-company"

Background and purpose

I am a MSc student in Societal safety at the University of Stavanger currently authoring my master thesis. The purpose of the thesis is to understand and explain how a private IT-company engage in the protection of critical infrastructures considered as crucial to national security. By the application of resilience, reliability and the use of forums/networks to manage cyber threats. In this thesis, cyber threats are perceived as wicked problems, which are complex, nearly impossible to solve and demands transboundary cooperation.

I have contacted you as I want to interview people with the expertise and knowledge about the company's strategies and organizational structure to manage cyber threats.

What does it mean to participate in the interview?

The data collection consists of interviews, questionnaire and document analysis. The participants receive an interview guide (questions) prior to the interview. Duration of the interview is no longer than 60 minutes. The interview will be conducted in English with the use of videocall (Microsoft Teams). The interview will be recorded.

What happens with the information about you?

Project end date is 15th of June 2021. Participants will be referred to as "participant 1, participant 2, etc." in the text. A table of the participants will be included in the thesis, here you will only be referred to by your position in the company. Your name will be anonymized when the recorded interview is transcribed. Access to raw material is limited to the student, supervisor and examiner. Raw material will be deleted after censorship.

Participation

It is voluntary to participate in the study. You can withdraw from participation at any time without giving up a reason. All details and information about you will be deleted if you chose to withdraw from the research.

If you have any questions regarding the research, please contact:

> *Student: Caroline Midtlien Mathiassen, Mobil: +4x xx xx xx xx*
> or *Supervisor (University of Stavanger): Karen Lund Petersen, Mobil: +4x xx xx xx xx*

If you want to participate please confirm by replying to the email you received with a signed copy of this consent form.

I consent to participate in the study:

____

(Signed by the participant, date)

I have received necessary information about the study.
I agree to participate voluntarily in the interview.
I agree that information about me can be obtained from the university's supervisor or examiner of this master thesis.

Appendix B Interview guide

Introduction

About the researcher, thesis and problem statement
Consent form and practical information
Potential questions before the interview starts

The participants background

Name, position, responsibility and experience

Thematic structure of the questions

How does cyber threats affect the company?

1. What does the company associate with cyber threats?
2. What do you consider to be the biggest challenge(s) in fighting cyber threats for your company?
3. What are the types of cyber threats your company is facing?
4. How can cyber threats affect your customers?

How does the company perceive their societal role in protection of national security?

1. How do you consider your company to be important in the protection of national security? Why?
2. How does the company work with the Norwegian authorities in relation to cyber security?
3. Is the company incorporating national strategies aimed at national security? How?
4. Which organizational structures/processes/standards are the company using to manage cyber threats?

Does the company follow any procedures/strategies to manage cyber threats?

1. How is management of cyber threats incorporated in company strategies?
2. Who are managing cyber threats in the company? Where are they located in the organization?
3. How would you consider your company's ability to prepare and adapt to potential new threats?
4. How would you describe the management structure (or organizational structure) of the company when faced with cyber threats?
5. How are the company utilising networking and knowledge sharing in special interest groups, specialist security forums and professional associations to mitigate cyber threats?

Summary

To finish off, is there anything else you think is important, relevant or useful for me that we have not talked about?

Appendix C Questionnaire

Hi,
I am a XX employee currently studying a master degree in Societal safety at the University of Stavanger.
This questionnaire is part of a study of organisational aspects of cyber threat management in XX.
The employees will have full anonymity (also to the researcher). The employees identity will not be disclosed at any point of time.
I hope you can spend 10-15 minutes of your time to answer ten questions.

Deadline for responding is 28th of May 2021.

Kind regards,
Master student in XX

Cyber threats

1. How do you take cyber threats into account when performing your work tasks?	____________________ ____________________ ____________________ ____________________
2. What do you consider as the biggest challenge(s) in fighting cyber threats in your role?	____________________ ____________________ ____________________ ____________________

Societal role and responsibility

3. How can a cyber attack on your company be harmful to national security?	____________________ ____________________
4. How do you work with the Norwegian authorities in relation to cyber security? For example: through implementation of national regulations and strategies, to seek information from or provide information to Norwegian authorities.	____________________ ____________________ ____________________ ____________________ ____________________ ____________________
5. Have you participated in special interest groups, forums or webinars about cyber security? How do you consider the value of such networks?	____________________ ____________________ ____________________ ____________________

Organizational aspect

6. Who are you collaborating with internally and/or externally regarding cyber security? Are there other actors that you think are important to cooperate with?

____
____
____
____
____

7. Have you conducted any training in managing cyber threats or vulnerabilities either on your own or through the company? What type of training?

____
____
____
____

8. If you look back at former cyber security incidents, what was the greatest challenge? What were you most proud of?

____
____
____

9. How do you consider the importance of persistent improvement in managing cyber threats and vulnerabilities?

____
____
____

10. How could a failure of cyber threat management in your company impact your customers operations?

____
____
____

Thank you very much for participating.

All participants are completely anonymous (also to the researcher). The employees identity will not be disclosed at any point of time.

Data will be deleted after the examiners censorship.

Appendix D Document analysis

1. **Document:** XX Management System overview (2021).

What: Governing process document

Authored by: The company

Information classification: Open

Purpose: Documents all themes in the governing management system

2. **Document:** ISAE 3402 Type II (2021).

What: Report

Authored by: Independent third-party auditor

Information classification: Internal company

Purpose: Independent service auditor's assurance report on the description of controls and their designs

3. **Document:** Stakeholder requirements (2020)

What: Report

Authored by: The company

Information classification: Internal company

Purpose: Overview of all relevant legal, regulatory, contractual and other requirement related to information security and business continuity.

4. **Document:** Quality policy (2020)

What: Report

Authored by: The company

Information classification: Internal company

Purpose: Documents the necessary quality controls in the company for auditing purposes

5. **Document:** Information security policy (2020)

What: Report

Authored by: The company

Information classification: Internal company

Purpose: Documents the internal information security policy

6. **Document:** ISO 27001 Compliance Document (2021)

What: Document

Authored by: The company

Information classification: Confidential

Purpose: Illustrates the aspects of control mechanisms implemented as part of the ISO27001 standard and certification.

7. **Document:** Competence Management, 2020

What: Policy

Authored by: The company

Information classification: Internal company

Purpose: Establish framework and guidelines for competence assurance

8. **Document:** Contact with authorities, 2020

What: Work instruction

Authored by: The company

Information classification: Internal company

Purpose: Work instruction for appropriate contact between the company and the authorities

9. **Document:** Personal data breach notification procedure, 2021

What: Procedure GDPR

Authored by: The company

Information classification: Internal company

Purpose: Procedure to define when and which national authorities should be contacted in case of incidents.

10. **Document:** Selection and use of the ISO 9000 family of standards, 2016

What: Document

Authored by: The ISO/TC 176, (ISO technical committee)

Information classification: Public

Purpose: Provides an overview of the ISO 9000family of core standards, step-by-step process to implement a quality management system, examples of typical applications of the standards, and a bibliography listing the ISO 9000 family of standards

Link: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100208.pdf

11. **Document:** The process approach in ISO 9001:2015, n/a

What: Document

Authored by: The ISO/TC 176 (ISO technical committee)

Information classification: Public

12. **Purpose:** The purpose if this paper is to explain the process approach in ISO9001:2015. The process approach can be applied to any organization and any management system regardless of type, size or complexity.

Link: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso9001-2015-process-appr.pdf

13. **Document:** IT Service Continuity Plan (2017)

What: Plan

Authored by: The company

Information classification: Restricted

Purpose: instructions to recover technical services and systems