FACULTY OF SCIENCE AND TECHNOLOGY

MASTER’S THESIS

Study Programme: Societal Safety	The Spring Semester, 2023 Open Access

Author: Marlene Svela Øvrebø

Supervisor at UIS: Ole Andreas Hegland Engen

External supervisor: Maria Kjærland-Haga

Thesis title: Contributing Factors in Building Cyber Resilience in Complex Organisations

Credits (ECTS): 30

Keywords: Risk, Security, Cyber Security, Resilience, Cyber Resilience, Complex Organization, The Energy Sector, Adaptive Capabilities, Human Factors	Pages of text: 83 Pages in total: 108 Stavanger, 17th of July, 2023

Abstract

Introduction: This master thesis explores the concept of cyber resilience and aims at identifying cyber resilience enhancing measures relevant to a complex organisation. Cyber security is a highly relevant field as the world gets more digitalised, and evaluating sufficient cyber protective measures is essential. Cyber Resilience can be seen as an extension of Risk Management and Cyber Security by providing a necessary layer of protection the fields currently lack; to continue operations and functions despite a threat.

Methods: Semi-structured interviews with practitioners, senior management and expert informants were conducted, and relevant cyber-resilient frameworks were analysed to identify cyber-resilient enhancing measures.

Results: The analysis showed that cyber resilience enhancing measures for complex organisations originate from understanding the construct, and adding it to existing structures is beneficial. However, for this to be effective, there must be a clear definition, directives and standards from which complex organisations can build a resilience understanding. The main findings include fostering a resilient mindset through adaptability, trust and flexibility, aligning to working with the complexity of such an organisation.

"Resiliency is the Ultimate Goal of Cybersecurity"
Wen Masters, Vice President, Cyber Technologies, MITRE

Acknowledgements

I want to express my gratitude towards the organisations that wanted to collaborate on a project focusing on resilience. I will be forever grateful to my external supervisor, Maria Kjærland-Haga, who positively responded to my inquiries and further guided me towards a relevant and exciting research statement. Your insights, guidance, kindness, and trust have been essential for completing this project. I am honoured to have been allowed to work with you and your team, and I will remember this experience as the starting point for my professional career within the security domain.

I extend my gratitude towards those willing to participate in this project, allowing me access to your brilliant minds and perspectives. You were all kind and welcoming, providing excellent perspectives on this project. The practitioners, the expert informant and the senior leader; thank you. I want to extend an extra thank you to Bjørn for your support and kindness.

I also want to express my appreciation and gratitude towards my supervisor Ole Andreas Engen. You have shown me guidance, new perspectives, and kindness. I appreciate your input, your conversations, and your drive.

Personally, Henrik Hagen and Catherine Stevens, thank you from the bottom of my heart for being my biggest supporters. Providing me with motivation and love. This is yours, as much as mine.

Conceptual Clarifications

Two concepts must be distinguished to clarify the difference due to disagreements within relevant fields to ensure a common understanding from the start.

OT and IT Differences: Information security (IT) and Operational technology (OT) are two different fields that are responsible for separate areas within the same security structure (Wangsness, 2023). IT has traditionally described how technology uses information processing and management, while OT refers to the systems and machines operating physical processes (Wangsness, 2023). IT is responsible for data safety and security, while OT focuses on the physical world through observing productions (Wangsness, 2023). As such, IT protects information and knowledge, while OT aims to prevent production disruption or effectiveness. With modern technology and cyberspace, it can be difficult to separate how tasks and responsibilities should be divided between the two concepts (Maleh, 2021). Historically, IT has been responsible for security threats on a technical level (Conklin, 2016), thus is rarely applied when considering the consequences or implications of operating in the broader physical OT system (HSD, 2021). The two fields are meant to integrate into each other.

Difference between Cyber Security and Information Security: There is a vast disconnect in the separation and understanding between cyber security and information security. Cyber security and information security are often used to describe the same field, but essentially the differences hold value for this project. Solms and Niekerks (2013) argue that cyber security is more complex than information security because it goes deeper into protecting not only information but informants, assets and people involved. Another distinction that Cybersecurity has to Information Security is that humans can be targets or involved (unknowingly) in cyber-attacks (Solms & Niekerks, 2013). Cybersecurity's main objectives centre around (1) ensuring business continuity and (2) minimising the damage done by security incidents (Solms & Niekerks, 2013). Due to this thesis's interest in ensuring cyber proception, especially within business enlivenment, cybersecurity is the correct term for this research project.

Table of Content

1. Introduction

1.1 Overview

This project aims to understand how complex organisations within the energy sector can build cyber resilience by examining various resilience-contributing factors. This includes investigating and understanding how the concept of resilience and compatible constructs related to risk, cybersecurity, and human factors are understood. Furthermore, relevant cyber resilience frameworks will be examined to identify beneficial tools and structures for building cyber resilience. To aid further exploration, the perspectives of relevant experts have been included through interviews.

Cyber resilience can be described as a topic of recent importance for companies and businesses internationally, creating a great need to understand what cyber resilience entails and how it can be implemented within complex organisations. Cyber resilience is an organisation's capacity to "anticipate, withstand, recover from and adapt to" (Ross et al., 2020) challenges and stressors on systems that require cyber resources.

Employees and a Senior Leader within one international energy company have been interviewed for this project, focusing on those working with risk and threat management and assessment, IT and OT. Additionally, an expert on safety and security was also interviewed. All informants were asked about their thoughts, expertise, and perspectives for a thorough examination of the understanding of cyber resilience on a practical level. Additionally, a literature review and document analysis of current cyber resilience frameworks has been conducted to thoroughly examine the contributing factors for strengthening cyber resilience.

1.2 Structure

This master thesis will take the following structure: Firstly, a justification for the relevancy of this research topic will be discussed, followed by the research statement and questions. Secondly, the literature on risk is overviewed to ensure a strong understanding before aspects of resilience, cyber resilience and cyber security are included. Complex organizations and human factors will also be included as an extension to these areas. Thirdly, an overview of the project's methodology is explained in addition to a short discussion of the decisions made in the project and relevant researcher biases. The findings of this project, from the interviews and document analysis, are then given, followed by a discussion of the main findings, a conclusion with suggestions for further research.

1.3 Background

Firstly, it is essential to examine why the development of cyber security is important to study. According to the Norwegian Intelligence Service (2022; 2023), an extreme rise in cyber-threats towards Norwegian businesses has been reported, and the trend is likely to continue (The Norwegian Police Security Services, 2022; 2023). As the world gets more digitalized, so does the risk in the cyber sphere (World Economic Forum, 2021; Norwegian Intelligence Services, 2023). The energy sector is one of the most likely targets for a cyber-attack, as international threat actors have an interest in utilizing technologies, safety procedures and data (The Norwegian Police Security Services, 2023). It is crucial to continuously improve defences against attacks in the energy sector and be aware of possible threats. These threats are now not just threats; but expected realities (Conklin et al., 2017), making cyber resilience an outright necessity within the risk management of cyber security. When it is stated that an attack cannot be prevented, the targeted system must be structured in a way which allows for its continuous function despite an attack.

Therefore, it is vital to investigate cyber security to gain an understanding of the current operational environment and its cyber resilience protocols to build further layers of protection against unknown threats. Technological advancements are creating an endless possibility of how threats can damage an organization, making it challenging to establish protective barriers. Assuming that there is a limit on resources and time coupled with the often multitude of protective options with often little indication of their sustainability, it could be wise to focus on strategies that adapt to current circumstances. (Conklin et al., 2017). Therefore, cyber resilience must be added to risk management and security processes.

To understand cyber resilience, it is necessary to attain an understanding of relevant terms and concepts. Significantly, all aspects will be explored further; however, a shorter description of the most relevant terms will follow to introduce the most relevant; resilience, cyber resilience, complex organizations, cyber security, and risk.

Recent studies on cyber protection suggest that cyber security can be achieved through resilience, specifically cyber resilience (Linkov et al., 2019; Hausken, 2020). *Resilience* is the forceful capacity to adapt to changes without reducing performance (Bento et al., 2021). Commonly for the oil and gas industry, most research on resilience focuses on a system's ability rather than the process of resilience itself (Bento et al., 2021). Cyber resilience can be seen as an extension and targeted form of resilience. The addition of "cyber" includes the continuance of a system when it experiences attacks via cyber resources (Galinec & Steingartner, 2017).

Cybersecurity has had more traction than physical security in the last few years, indicating a focus shift (Shafqat & Masdood, 2016). *Cyber security* can be defined as the structures, assets, and resources a system has to defend against threats and attacks in cyberspace (Schatz & Bashroush, 2017). With cyberspace comes a tremendous increase in opportunities, communications, and effectiveness for companies, but it also leaves businesses more open to vulnerabilities and new threats (European Commission, 2022). Such vulnerabilities are imperative to understand and build resilience against, for which there is still a way to go.

When an organization is described as complex, there are connections and elements within the organization that vary in expertise, structure and function (Dooley, 2002). For a *complex organization* to function, multiple unique parts require different needs, goals and resources that must exist independently and, ideally, cooperate (Dooley, 2002). With this duality, it can be challenging to implement common understandings, agreed-upon definitions and processes that will suit all.

According to Engen et al., (2021) and Aven (2010), *risk* refers to anything that happens or could happen and the active choices presented and subsequent decisions taken. Furthermore, the Norwegian Petroleum Safety Authority (PTIL) defines *risk* as the consequences of an action and its attached uncertainty (n.d). Due to its operational environment (the cyber domain), inherently, cyber security will never involve "risk-free" decisions and choices (Bochman, 2018). Advantageously, cyber resilience can help mitigate the proportions of the inherent risk found within cyber security. Accepting that there is, and always will be, some form of risk can allow for cyber resilience building to develop and flourish properly.

2. Research Statement

In this master thesis, the goal is to explore how the concept of cyber resilience is understood by those working within complex organizations within the energy sector. In addition to establishing contributing factors that may strengthen cyber resilience identified via scientific peer-reviewed studies and proposed frameworks. The research statement that guides this project explores the:

Contributing Factors in Building Cyber Resilience in Complex Organizations

2.1 Research Questions

To investigate the aspects of cyber resilience in complex organizations, some related concepts require exploration. In addition to attempting to answer the official research statement, three additional research questions have been developed.

The first question attempts to cover different understandings and perspectives of cyber resilience. Due to its novelty and lack of consensual definition, it is imperative to understand how current practitioners interpret and understand cyber resilience. As such, the first research question explores the following:

1. *How does the Energy Sector Understand the Concept of Cyber Resilience?*

The second research question explores how the understanding and acceptance of risk influence the understanding of cyber resilience and how it is valued. Risk is an underlying concept within cyber resilience that requires exploration to cover the basic understanding of what values one is protecting. Furthermore, the research questions aim to investigate how the understanding of security shape one's understanding of cyber resilience. In some areas, security is seen as either the opposite of resilience or the primary discipline, while cyber resilience is viewed as an additional layer. Exploring this relationship can provide insight into how the two terms differentiate or complement each other, creating the second research question:

2. *How does the understanding of risk and security influence the understanding of cyber resilience?*

Thirdly, as the primary goal of this thesis is to explore contributing factors that strengthen cyber resilience, relevant frameworks have been examined to explore appropriate methods, measures, and ideas, creating the final research question:

3. Which elements enhance cyber resilience for a complex organisation?

2.2 Context

A short description of the relevant sector will give insight into what the sector entails. Also, an overview of the relevant laws, international standards and pledges regarding a company's cyber security and cyber resilience policies will be presented. The Norwegian Energy Sector is required to follow the Security Act, which entails goals and procedures that must be followed. International standards are created to ensure common goals and collaboration between companies. To propose how cyber resilience could be built and prioritised within the energy sector, the laws, procedures, and standards the industry is subjected to must be included to ensure that the suggestions concur with the given regulations. A short description of the Norwegian energy sector, The Security Act, International Standards and Cyber Resilience Pledge will follow.

2.2.1 The Norwegian Energy Sector

It is beneficial to get a short overview of who owns and dictates the procedure of the Norwegian Energy Sector to outline the structure the sector is contingent on. It is essential to understand which changes the energy sector can implement to strengthen cyber resilience and what falls under the purview of more central authorities.

The public and various stakeholders own the majority of the Norwegian energy sector, whilst a smaller portion is privately owned. Combining all ownership (which is divided between Norwegian counties), the state and other national stakeholders own 90% of Norway's electricity production is owned by the public sector (Ministry of Petroleum and Energy, 2021). The Norwegian Parliament holds the governing responsibility and authority and dictates the political agenda through various ministries, mainly the Ministry of Petroleum and Energy (Ministry of Petroleum and Energy, 2021). The Norwegian Directorate for Civil Protection, now referred to by its official initials (DSB), stated in 2019 that the energy sector is an industrial area highly likely to experience cyber-attacks. Vulnerabilities lie in the possibility of actors accessing sensitive information and conflicting harm to the Norwegian economy, society, and infrastructure strategically by sabotaging oil and gas systems (DSB, 2019). The possibility of these devastating consequences makes it an important area to study.

2.2.2 The Security Act

The Norwegian energy sector is encouraged to follow official requirements and directives as a guidebook and best-practise models to secure organisations. Cyber-resilient strengthening suggestions must align with Norwegian Law; thus, understanding the underlying rules and expectations is necessary before new suggestions are presented.

One of these regulations is implemented through new additions to the Security Act from 2019. According to the Norwegian National Security Authority, from now on referred to by its initials, NSM, the Security Act is meant to prevent, uncover, and protect against security threats (2020). By subjecting energy companies to the Security Act, the intention is to strengthen the collaboration with the state and openly share graded information relevant to cooperating parties

(Hovland & Homes, 2022). Furthermore, the intent is to ensure the industry's safety and security standards are followed.

This change can be seen as a response to preparedness after the two attacks on gas pipes in Østersjøen- the Nord Stream One and Two (NSM, 2022). This attack can be described as the last motivator to get the energy sector included in the Security Act, as it took almost four years from its completion to its inclusion (Moe & Langved, 2022). The intent behind including the energy sector as a national function was to ensure security around the extraction of petroleum and transport of gas through Europe (Hovland & Homes, 2022). Notably, the energy sector requires standards set according to international collaborations and where information systems regarding threats must be sharable with other stakeholders and competitors (Ministry of Defence, 2017). Essentially, the Security Act of 2019 allows for information sharing through a high-security clearance between the energy sector, Ministries and official safety and security authorities to allow for closer cooperation and the generation of a clearer threat picture (Hovland & Homes, 2022).

2.2.3 International Standards and Guidelines:

As the Norwegian energy sector is part of the more significant international sector, there are more than Norwegian laws the sector is subject to. Partnerships across country lines require there to be some standards of security measures to ensure similar procedures between companies. It is essential to be aware of international standards and guidelines to ensure that innovations relating to cyber resilience follow the agreed-upon guidelines. A short overview of the international standards relevant to building security can be found in the ISO/IEC standards, the pledge suggested by the world economic forum and suggestions from the European Commission.

2.2.3.1 ISO/IEC 27000 & DIS 27032 & ISO22301

The International Organisation for Standardization (ISO) collaborated with the International Electrotechnical Commission (IEC) and created ISO/IEC 27000, a set of standards for goals and protection of the security and management of information. One of the primary standards in the series is ISO 27001, which includes the necessary elements and techniques for implementing a functional and robust Information Security Management System (ISMS). The ISO 27000 series is intended to foster a "cyber-resilient" mindset implemented into information systems, the organisation's culture and daily operations (ISO, 2023). This means that cyber resilience has a strong focus in the leading framework for information management and security, highlighting the importance of this research. Though ISMS is not an official requirement for an energy company, they must hold robust procedures for securing information, data, and standards set from the IOS 27000 (Landax, 2021).

Another relevant set of standards is ISO 27032, which will be updated later this year. The 27032 standards offer cybersecurity guidelines relevant to threats, focusing on social engineering attacks and hacking (ISO, 2022). Similar risk management and resilience elements focus on "prepare, prevent, detect/monitor and respond" (ISO, 2022). ISO 27032 is designed to align with the National Institute of Standards and Technologies (NIST) framework for dictating standards within cyber security, with a focus placed on five main functions: identify, protect, detect, respond, and recover, which can be tailored to a distinct organisation (2023).

2.2.3.2 Cyber Resilience Pledge

Notably, significant players in the international energy sector agreed to prioritise the importance of collaboratively building cyber resilience through the cyber resilience pledge (Olsen, 2022). The Norwegian energy sector commonly accepts the pledge, making it an essential component in how cyber resilience is currently viewed. At the 2022 annual global conference for the World Economic Forum in Switzerland, multiple oil and gas companies signed a cyber resilience pledge to "promote cyber resilience against growing cyber threats" (Kagubare, 2022). The intent was to build cyber resilience across the oil and gas industry to withstand damaging and hurtful cyber-attacks by collaboratively protecting critical infrastructure. The sector is complex and interconnected through the value chain "one company working alone, if as effective as locking the front gate while leaving the backdoor wide open" (Raina, 2022). Therefore pledge's objective was to spread collective awareness towards the importance of cyber resilience that would lead to joint action through a global approach (Rania, 2022) of accepted standards (Arghire, 2022).

2.2.3.3 European Commission: NIS2 & CER

With this change to the threat landscape, The European Commission has heightened its efforts to ensure businesses build cyber resilience (2020). Member States have been put on high alert, and all essential infrastructure and constructions are advised to prevent, resist, absorb, and recover from troublesome events ranging from natural incidents to terrorism threats (European Commission, 2020). These essential elements lay the groundwork for how suggested resilience strategies should be targeted and implemented.

More importantly, the European Commission has created a Network and Information System Directive (NIS1), which focuses on establishing strong cyber resilience (2020). An updated version, NIS2, was realised in early 2023. As the Norwegian energy sector are subject to international standards, an alignment with NIS2 standards for cyber security is not uncommon within companies. Members of the Norwegian Parliament have suggested a new law regarding cyber security based on NIS2 (Gjessing, 2023). This includes requirements for risk management and security within IT, similar to the IOS standards and the Cyber Pledge.

Furthermore, to put security further on the agenda, the European Commission (2022) created a directive on the resilience of critical infrastructure (CER). The CER is relevant for 11 sectors, with the energy sector being one of them (European Union, 2023). The main goal of CER is to protect and support critical structures and functions that benefit society in the larger setting (European Union, 2023). Significantly, CER and NIS2 supplement each other.

The Norwegian energy sector falls under all these standards and guidelines, meaning that one of the main objectives of the energy sector should be to understand, build and foster cyber resilience.

3. Theoretical Framework

This section will introduce the theoretical framework to answer the research statement and questions. Risk, cyber resilience, and complex organisations will be examined across significant categories. The first two categories will lay the groundwork for how the first and second research questions can be answered - the understanding of cyber resilience and how the interpretation of risk and security can influence this understanding. The last category will give insight into the third research question, how cyber resilience be enhanced for complex organisations.

Firstly, the basic concept of risk will be explored to form a basic understanding of risk and risk management. After understanding the concept of risk, the interpretation of resilience, cyber resilience, and other cyber-related sections will follow to ensure awareness of the relevant environment. Thirdly, the properties of complex organisations and enhancing mechanisms for cyber resilience through human factors will be examined.

3.1 Risk

Relating to the second research question, how the understanding of risk influences the understanding of cyber resilience call for a throughout examination of how risk is understood.

Engen et al., (2021) and Renn (2010) underline that risk has different understandings according to discipline and context. Within the field of societal safety, risk can be seen as the product of probability and consequences (Aven, 2010; Engen et al., 2021). Risk involves three elements: probability, event, and consequences (Aven, 2012). To understand the term risk practically, Engen et al., (2021) state that risk refers to anything that happens or could with the consequences and active choices that follow. It is important to note that consequences could be positive and negative, and choice inertia is ultimately also a choice (Engen et al., 2021). Furthermore, an incident that carries risk could result from actions with or without intent (Engen et al., 2021).

Notably, the understanding of risk is complex, and there are additional elements that attempt to express risk accurately. To emphasize, risk probability is not necessarily the most accurate measure when evaluating risk when implementing and prioritizing security measures. To illustrate, if one were tasked with evaluating how likely it is for espionage, based on how many times it has occurred in the last ten years, one would have to put the probability at low or not likely. Following this thinking, no resources would be allocated to protect against the threat. Nevertheless, considering the horrendous consequences of successful espionage, valuing the severity (Engen et al., 2021) and strength of knowledge (Aven, 2012; 2010) is highly beneficial in measuring risk. As attacks through cyberspace are an expected threat (Conklin et al., 2017), a high number of occurrences should not necessarily indicate that all resources should be implemented towards every attack, as attack severity holds more weight over the number of occurrences (Engen et al., 2021).

Taking a more holistic view of risk allows a more accurate understanding of describing and calculating uncertainties (Aven, 2012). Risk depiction also idiosyncratically lies in the eye of the beholder and what values they consider essential and worth protecting. In a report based on predicting trends in societal safety-related issues, awareness of which values one wants to protect was mentioned (Sellvåg et al., 2020; NSM, 2023). These can range from life, reputation, operational function and materials (Sellvåg et al., 2020), which all depend on the needs and priorities of the specific organization.

It is beneficial to look for an understanding of risk from the perspective of the Norwegian energy sector. The Norwegian Petroleum Safety Authority (PTIL) evaluates risk for analysis, with the traditional probability x consequence thinking (n.d) suggesting the risk is equal to the consequence of the action with the associated uncertainty. Similarly to Engen et al., (2021), PTIL underlines that all judgements made on risk must be measures against who is conducting the analysis (n.d). The energy sector has implemented this understanding of risk with the understanding that there will always be uncertainty towards future events and, thus, the ongoing presence of risk. Managing risk will allow for a better understanding of uncertainty.

For this research project, *risk* will be defined as the consequence of the action with the associated uncertainty.

3.1.1 Risk Management

As cyber resilience can be seen as a measure to reduce risk, it can also be seen as a form of risk management. Importantly, exploring risk management as a separate concept is valuable to give insight into the second research question regarding how understanding risk influences understanding cyber resilience.

Risk management is the probability of risk and making sound arguments for deciding on a strategy to avoid or reduce risk (Dupont, 2019). Further supported by Annarelli et al., (2020), risk management is about avoiding risk through prevention and protection. Risk management involves awareness of the threat landscape, understanding the why behind the threat, and knowing which resources are available for protection (Allison et al., 2014). An essential part of risk management is to evaluate risk through risk assessments. The three cornerstones of risk assessments are the relationship between "threat, vulnerabilities and consequences" (Linkov & Kott, 2018). However, this view becomes too simplified concerning complex cyber systems, where multiple functions are interconnected and collaborate (Linkov & Kott, 2018).

Can risk reduction through cyber resilience be seen as a strategy for risk management? According to Panda and Bower (2020), the complexity of cyber security requires further steps than traditional risk management. However, cyber resilience should be considered an additional layer (Ferdinand, 2016), not an alternative. With the constant change and upgrade of technology, strong and productive protection for information sharing and critical systems requires more than one form of risk management (Bejarano et al., 2021).

Within risk, one is looking for threats. Generally speaking, a threat is anything that can disrupt operations, people, systems or organisations. Following, whoever or whatever is attempting to inflict harm or damage is referred to as a threat actor (Hausken, 2020). Notably, a trend quickly arising is the use of hybrid threats, which are "a combination of military and non-military measures" to create confusion for the target and understand who is behind the attack (Sellvåg et al., 2020). Another description of hybrid threats is actions in the "grey area" (Sellvåg et al., 2020), whereas uncertainty and doubt cloud decision-making. Examples of such methods are propaganda, fake news, economic pressure, and breaches of safety procedures (Sellvåg et al., 2020; Linkov et al., 2019).

This research project has not had a distinct focus on which type of threats to protect against. Arguably, within a complex organisation, most threats will require multiple layers of attention to be protected against. This research project's findings can apply to hybrid and more traditional threats.

3.1.2 Cyber Risk

Cyber risk is defined similarly to risk in general – evaluating how likely a troublesome event is and the consequences via cyberspace (Linkov & Kott, 2018). This can insinuate that what is known about general risk can be applied to cyber risk (Allison et al., 2014). According to the Institute of Risk Management (Alison et al., 2014), cyber risk is the vulnerability of technology. Though, there is another understanding of cyber risk. It states that cyber risk is the risk of having a conditional need for assets and access to the Internet (Ross et al., 2021). However, a meta-analysis conducted by Strupczewski (2021) combined over twenty academic definitions of risk and concluded that most sectors describe cyber risk as the operational risk that occurs in cyberspace with a threat to goods, information, production disruption, business or reputation. As such, this review confirms that the most used definition of cyber risk aligns with the general understanding of risk.

It is valuable to differentiate cyber threats and cyber incidents for informational purposes, as the two terms are commonly combined with cyber risk. Cyber threats aim at attacking within cyberspace, categorized as cyber incident, that causes cyber risk (Hausken, 2020; Mbanaso & Dandura, 2015). Though this chain of terms is beneficial, threats against cyberspace will be described as cyber risks in this project. Due to the results in the meta-study mentioned above by Strupczewski (2021), *cyber risk* will be defined in the same way as a risk in general, but adding cyberspace as the centuriated area is relevant; the consequence of action within the associated uncertainty within the area of cyberspace.

3.1.3 Cyber Space and Cyber Systems

A clear understanding of cyberspace is necessary for all three research questions, as they all pertain to cyber. In addition to defining cyberspace, defining cyber systems is also relevant to lay the groundwork for what conditions and limitations exist within the system.

Cyberspace is a synonym for the internet (Mbanaso & Dandaura, 2015). When a system becomes digitalized, effectiveness, communication capabilities and safety procedures increase; however, it also opens for vulnerabilities and a weakened security defence (Sellvåg et al., 2020; NSM, 2023). According to the National Intelligence Council's (2021) report on global trends in the next twenty years, the opportunities that cyberspace will allow for are incredible, creating a "hyper-connected world." Urgently, attacks coming from cyberspace are swiftly developing, and there is a need for a framework that can compute the risk of cyber systems (Linkov & Kott, 2018). Linkov and Kott (2018) suggest that the only method of protecting a system against cyber threats is simply disconnecting from the internet, which is not plausible in this modern world. Cyber systems are highly complex and affect most aspects of critical infrastructure (Panda & Bower, 2020), which indicates that a holistic approach is necessary where the components of risk, safety, security, and resilience are involved.

The actors behind a cyber-attack can vary from a single entity to extensive private and public cooperation and even a department of government (Linkov & Kott, 2018). When personal data is stolen or misused, millions can be affected, and the consequences can vary from loss of privacy to fraud (Linkov & Kott, 2018). On a larger scale, when corporations are affected by cyber-attacks, the damage, theft, and misuse of that business's data can be damaging concerning trust between the business and its users and how sensitive and private data is leaked (Linkov & Kott, 2018).

3.2 Cyber Security

Another critical element of the second research question is how understanding security influences understanding cyber resilience. Thus the distinction between safety and security will be explored, and the terms cyberspace and cyber systems will be examined.

The NSM underlines that security needs to be seen and understood within a more extensive system (2023), especially by companies subject to the Security Act, due to their complex structures and the flow of sensitive information. Cyber security is defined as barriers against unlawful entry into a computer system, emphasising protecting users' security properties in cyberspace (Solms & Niekerks, 2013). There are e few general security objectives that should model any strategic decision: availability, integrity, authenticity, nonrepudiation, and confidentiality (Solms & Niekerks, 2013). Furthermore, the Cybersecurity and Infrastructure Security Agency (CISA) states that cyber security is to protect "network, devices and data" from being accessed without permission and for harmful intents (2021). Similar to Solma and Nieker's (2013) security objectives, CISA's (2021) values are "confidentiality, integrity and availability of information."

However, the definition proposed by Galinec and Steingartner (2017) will be used for the understanding of cybersecurity in this paper: "the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries." This definition is highly relevant to a complex organisation as multiple components need to be considered in the equation of security measures. Management, delivery of information, and the relationship between those responsible for informational- and operational technology are elements in a complex organisation.

For this project, *cyber security* will be defined as the governance and use of IT and OT security tools to protect against unlawful disruptions through cyberspace, based on the definitions by Galinec and Steingartner (2017) and Solms & Niekerks (2013).

3.2.1 Security vs. Safety

Separating security and safety are valuable as they hold unique properties, especially concerning the second research question. Further in this project, it will become apparent that even though security and safety differentiate, there is value in keeping the two connected.

At first glance, security and safety have the same goal, to protect. A known challenge is that only some languages have proper translations to differentiate them. The most straightforward distinction between the concepts is that safety deals with risk and uncertainty concerning natural disasters and accidents (Engen et al., 2021). In other words, actions without intent to harm. Security can be seen as the opposite when there is intent to harm or inflict damage, such as criminal acts, sabotage, cyber-attacks and terrorist attacks (Engen et al., 2021). The Norwegian Petroleum Safety Authority (2023) states that the two areas must be seen holistically. Maintenance of platforms and equipment needs to be prioritized on the same level as observing for unwanted attacks, as accidents and malfunction of systems can also be considered a considerable threat (PTIL, 2023).

Safety and security are also divided for the energy sector as to where protective measures are implemented. Safety, which in this case, translates to the Norwegian word sikkring, would be responsible for barriers, procedures, and maintenance on platforms, namely fysisk-sikkring. While security, translated to sikkerhet, focuses on IT and OT elements of protecting information and systems while focusing on business continuity and confidentiality. One argument for holistically valuing and prioritizing safety and security is that the intent behind an incident is often unclear. Secondly, weakness in one area can increase the danger to the other. A lack of security measures can reduce the effectiveness of safety measures as it is required to be more effective in filling the gaps. Thirdly, safety and security work together in a relationship rather than a distinction. Safety is an integral part of resilience, as it is through constant attention and development of the measures, barriers and procedures that are implemented that can build resilience (Bento et al., 2021). Notably, security is also vital for building resilience, as resilience is not achieved but continuously thriving to maintain.

3.3 Resilience

The crown jewel of this project is understanding resilience as it pertains to the first and third research questions. The first research question is how the energy sector understands cyber resilience, which requires a deep dive into how resilience is currently understood. The third research question concerns understanding which elements within a complex organization can enhance cyber resilience. Generally, to understand what cyber resilience is, one must start with understanding resilience.

Resilience has an exhaustive history of meaning, where it has been used to describe various concepts within the fields of engineering, biology, and psychology (Hollnagel, 2016a). As cited by Hollnagel (2016a), it was in 1973 that Holling used the term resilience to describe how an ecosystem could withstand external influences and continue functioning. This is where the term became understood as the ability to endure stressors and traumatic influence and, despite this, continue functioning (Hollnagel, 2016a). This could be understood as corporations' attempts to develop models and systems that continuously strengthen itselves. Though it might be from a different discipline, the way resilience is present in psychology has the same function as in security and risk management; it is all about adapting and continuing to function under distress (Chamorro-Premuzic & Lusk, 2017). Expectedly, the term resilience has undertaken a variety of definitions, from continuing functioning under threat to focusing on the surrounding conditions that had an influence (Hollnagel, 2016a). Hollnagel (2016a) defines *resilience* as having an ability or defence that thrives under threat and not just withstanding risk. Furthermore, there is importance not only being able to counter disruption but also opportunities (Hollnagel, 2016a).

There needs to be a common consensus on how resilience should adequately be defined (Eisenberg et al., 2014), which makes it beneficial to look at multiple definitions to define the construct. According to Tarja (2019), resilience is "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events." Meaning that it is similar to Hollnagel's understanding. Furthermore, The European Commission (2012) and leading researcher in the field Linkov and Palma-Oliveira (2017) has defined the term as (in that order), "ability (…) to withstand, to adopt, and to quickly recover from stress and shocks" and "the capacity to better review how systems may continually adjust to changing information, relationships, goals, threats, and other factors in order to adapt in the face of change and uncertainty – particularly those potential changes that could yield negative outcomes." Furthermore, looking to researchers withing societal safety, Anholt and Boersma (2018), has defined the term as "the ability or capacity to absorb the shock, adapt to the new reality, and to transform to function either as before the crisis or in a superior manner."

It can be concluded that there is a disagreement on how resilience should be defined, but that general themes are repeated. More importantly, there needs to be more understanding of how resilience can be achieved, which will be addressed later. Regardless, accepting that a widely used and relatively new buzzword, such as resilience, might implement a variety of operational definitions (Wied et al., 2019), it is necessary to separate resilience from the terms it is most confused or combined with—mainly robustness, security, and risk.

3.3.1 Resilience vs. Robustness

Two terms, both interconnected and separate, are resilience and robustness. The terms are misused and combined, supporting the complication of the disagreement of official terms. Resilience is often used to describe robustness and vice versa, and the field does not always agree on how (or even if) they differ. According to Engen and others (2021), robustness could be described as the opposite of vulnerabilities, which could signal strength, resistance, or insensibility. Resilience is described as the ability to adapt and resist (Hollnagel, 2016b). So far, both terms hold similar meanings. According to Cambridge Dictionary (n.d), robustness is "the quality of being strong, healthy, and unlikely to break or fall." Taking the words of these definitions literally, robustness means that something will not break because the system will pause or stop. At the same time, resilience can handle being broken because it can continue functioning under an attack and return to its previous state. Creating a distinct difference between the two concepts.

Accepting that the two concepts may overlap in some areas, another clear distinction could be that robustness responds to what has happened, while resilience is more proactive (Hollnagel, 2014). It will be explored how resilience has the underlying understanding that an attack will happen, while security thinking processes that something could happen.

3.3.2 Resilience vs. Security

Pertaining to the second research question, how does one's understanding of security impact one's understanding of resilience? It is beneficial to compare and contrast the two constructs.

Though it can be complicated to separate these terms, evaluating how they can stay strong and benefit from each other is essential, as later in this project, their co-dependency will become apparent.

Security is "preventing a system from degrading and keeping functionality within acceptable levels before and after the adverse event" (Linkov & Kott, 2018). In contrast, resilience is "the capacity to recover quickly from difficulties" (Oxford Dictionary, n.d). Based on this separation, both security and resilience aim at the same goal, for a system to be equipped to handle unwanted events. According to Anhold & Boersma (2018), resilience goes beyond security by accepting that something will happen, not wondering if something happens. Resilience is not necessarily interested in resolving the crisis, which falls mainly to security, but to continue operating despite the crisis. This could indicate that security aims to create as much protection as is deemed necessary to withstand an event, with the goal that the event will be stopped. Resilience, on the other hand, has an innate acceptance that unwanted situations will occur, which puts to focus on strengthening the system to the point that it will not need to rely on what is deemed necessary but simply an overall continuance for the system.

As already established in this project, security is an essential element to combine resilience with, as both systems hold the expertise, value and structure necessary for a complex organization to protect itself against cyber threats.

3.3.3 Resilience vs. Risk

It might be an unusual comparison, as risk happens, and resilience can be a system that ensures the risk does not influence what it is targeting. Relevantly, as an element of the second research question, one's perspective of risk might form one's understanding of resilience; this is a vital comparison and separation. As previously stated in the section about risk, risk management and cyber risk, this section can be seen as an extension of already established theory.

Generally, there is an innate acceptance within resilience, and that risk must be accepted. This makes it a viable option to improve resilience instead of (or in an attempt to) manage risk (Annarelli et al., 2020). Risk and resilience might be seen as complementary concepts where risk management is about avoiding risk, preventing and protecting (Annarelli et al., 2020), similar to resilience. Resilience takes it further than risk assessment by considering the unknown and the unexpected in a complex system rather than analyzing every element itself (Linkov & Palma-Oliveira, 2017). Risk is revolved around endangerment, while cyber resilience aims to preserve high performance in the presence of the given endangerment (Annarelli et al., 2020; Dupont, 2019).

3.3.4 Cyber Resilience

When the distinction of resilience has been established, and the definition of concepts such as risk and security has been stated, it is essential to evaluate the term most relevant for this paper, cyber resilience. The research statement of this project requires an understanding of cyber resilience. All three research questions mention cyber resilience, and this section will serve as the groundwork for further discussions.

As proposed by the approach CCE, Consequence-driven, cyber-informed engineering, the only way to effectively reduce cyber risk is to remove critical functions from the internet (Bochman, 2018; Linkov & Kott, 2018). This is not a plausible defence within a complex organisation, so developing a solid cyber-resilient defence is vital. According to Galmec & Steingartner (2017), cyber resilience is the ability of a "business process to anticipate, withstand, recover from, and adapt capabilities in the face of adversity conditions, stressors, or attacks on the cyber resources it needs to function." Meaning that work should get done regardless of how cyber elements are attacked. Furthermore, *cyber resilience* can be defined as the ability of a system after a cyberattack (Bejarano et al., 2021).

These definitions describe a system that has the capacity to withstand, recover and adapt promptly to reduce harmful consequences from an unwanted event. Kott and Linkov (2021) have created a definition that includes the extension of resilience from security with the acceptance that attacks will occur. "Cyber Resilience is acceptance of cyber compromise as a likely event, and the system suffering as a result; the focus is on the system's ability to recover, adapt and not just resist" (Kott & Linkov, 2021). As suggested by Dupont (2019), cyber resilience is an excellent addition to what is already known and practised within cybersecurity, indicating that cyber resilience is a necessary layer of defence against modern threats and attacks cyber security needs the addition of.

In this master thesis, a definition combining both Kott & Linkov (2021) and Dupont (2019) has been created; *Cyber resilience* will be defined as accepting that cyberspace will be compromised and affecting systems, processes, business continuity and integrity and focusing on the system's ability to prepare against, quickly recover from and adapt to changes, not simply resisting threat.

3.3.5 Resilience Engineering

The current evolution of risk in cyberspace makes it challenging for traditional risk-based approaches to balance the importance of thriving during a cyber-attack. As a valuable addition, resilience-based approaches focus on continuing the system's functioning regardless of disruption. Concerning the third research question, possible measures that can boost cyber resilience, a clear starting point can be found in the theory of resilience engineering. In addition, as the same research questions also include complex organisations, resilience engineering is described as an archetype of how complexity could be tolerated under pressure (Woods & Hollnagel, 2017), making it highly relevant. Moreover, the structure and principles behind resilience engineering contribute to understanding resilience and resilience building, which holds further relevance to the first and second research questions. In further chapters, the valuing of human behaviour and decision-making within resilience engineering will be discussed concerning human factors, but a short introduction will be included in this section.

As described by Hollnagel (2016), "resilience engineering" was intended to offer an understanding and extension of "safety." Meaning that the new goal is not to bypass dangerous threats as the traditional view of safety could be but to endure them. Resilience Engineering analyses an organisation's capacity through the relationship between four levels of competence: "how it responds, how it monitors, how it learns and how it anticipates" (Hollnagel, 2016). Responding entails reacting to anticipated and unanticipated developments by mobilising previously made plans and tailoring responses to new threats (Hollnagel, 2015). This includes adjusting to a new normal in ordinary and unconventional events (Hollnagel, 2011). Monitoring includes being aware of what is happening and knowing what potential effect these changes can have should they develop (Hollnagel, 2015). This is considered a critical part of where ongoing developments are supervised (Hollnagel, 2011). The ability to learn consists of learning from previous events and knowing which information is valuable for future threats (Hollnagel, 2015). This indicates learning from what went right and wrong (Macchi et al., 2011). Lastly, the ability to anticipate includes the attempt to understand what can develop further down the line before it occurs (Hollnagel, 2015). The goal is to identify future threats by deploying defences before it occurs (Macchi et al., 2011). Furthermore, Hollnagel (2015) adds the quality of adapting.

Security measures are typically based on hindsight (Woods & Hollnagel, 2017). The aftereffect of an incident will dictate how to meet the same threat the next time it occurs, meaning that resilience engineering offers a new layer of security (Woods & Hollnagel, 2017). Resilience engineering centres around understanding a system's ability to endure rising pressures and continuing operating at the same level despite the attack (Rankin et al., 2013).

Resilience Engineering is a model of how security could be managed with an intense spotlight on "how to help people cope with complexity under pressure to achieve success" (Woods & Hollnagel, 2017, p. 6). One underlying truth that must be accepted within resilience engineering is that problems rarely arrive through the same path twice, which means that the focus should be on tolerating danger (Hollnagel, 2013), which means that there is no need to establish a step-by-step understanding of how a threat will take place. Resilience engineering reaches its optimal functioning when humans are able to adapt in collaboration with flexible conditions that can do the same (Hollnagel, 2016). This means that instinctively, people working within conditions that allow them to implement changes in how they perform tasks regarding needs and capabilities are capable of creating a resilient system.

It can be suggested that people can adjust to new circumstances and unknown threats. At the same time, the hindering usually falls on what a complex system allows for the freedom to do so. In layman's terms, a system that can meet internal and external pressures without losing capacity can be considered resilient (Bento et al., 2021). Meaning that both the organisational capabilities and the environment it operates in must be understood. Adaptability to circumstances allows for intervening before it is too late (Hollnagel, 2014). It is essential to underline that a resilience engineering approach views unexpected situations as opportunities and not just as threats

(Hollnagel, 2014). As there are often more successful outcomes than unsuccessful in defence of cyber-attacks, there is great value in studying why the system was able to stop the attack.

There are several ways to measure an organisation's resilience. However, as indicated by Hollnagel (2015), the goal should not be to measure how resilient an organisation is but to evaluate what facilitates resilient conduct for that specific organisation. Aligned with the four components that are the building blocks of resilience engineering (how to respond, monitor, learn and anticipate), the Resilience Analysis Grid (RAG) was created. Hollnagel (2015) dictates that the goal of RAG is not to complete a score of how an organisation scored on the four elements but to provide insight into the current state of resilience (Hollnagel, 2015).

A short exploration of the four categories will follow. (1) A system is required to have the ability to respond and function, but more importantly, the response must be both adequate and well-timed (Hollnagel, 2015). The system must be able to identify that a change is occurring and categorise it as a potential threat (Hollnagel, 2015). Furthermore, it needs the capacity to know the length of a response which requires flexibility and freedom for individual tailoring. (2) Notably, a system needs the capacity to monitor internal factors or changes and external elements in its environment (Hollnagel, 2015). (3) As with any complex connection, the ability to learn is highly dependent on the two previous abilities, as the conditions are constantly changing (Hollnagel, 2015). Effective learning requires remembering and learning from previous events, but more importantly, how these events are understood and analysed will lay the groundwork for how well a system learns (Hollnagel, 2015). (4) Anticipating future destructive threats or favourable conditions would create resilience and safety and be both time- and resource-effective (Hollnagel, 2015).

3.4 Complex Organisations

Concerning the third research question, defining complex organisation is necessary, in addition to understanding how the cyber resilience of a complex system is in itself. An overview of the distinct challenges and qualities of a complex system or organisation will follow.

Being able to choose appropriate tools that will function with future updates and be able to adjust to new changes in the threat picture is crucial (Hausken, 2020), especially for organisations with complex systems where communication sharing, cooperation and effective change require the inclusion of multiple layers within the organisation. There needs to be an understanding of the business as an actor, the actors who collaborated with and who are dependent on each other (Hausken, 2020). In a complex system, chains of structures require specific information and tailored cooperation to continue operational function while under pressure from cyber threats seen from a cyber security perspective. Implementing resilience would be highly beneficial if a system is "complex, interconnected and adaptive (Linkov et al., 2019). It is a way of protecting and strengthening the whole defence instead of focusing on one type of attack and building a solid defence. In other words, resilience will protect the whole infrastructure (Linkov et al., 2019).

A continuance from the definition of cyber resilience, from an organisational perspective, resilience is shown in the "systems capacity to absorb and return to a stable state after disruption" (Bento et al., 2021). *Organisational resilience* is a system that predicts, integrates, responds, and adds new knowledge (Bento et al., 2021). A complex system with multiple departments, structural layers, management hierarchies, and multiple layers of supply chains and subcontractors requires strong collaboration and communication. Preparedness must be across sectors (NSM, 2023), as coordinated attacks seem to want to attack multiple companies or sections simultaneously. The more connected cyberspace services and processes become, the more linked together they all get; this can be called "value chains," which are interconnected, complex and often cross international borders meaning outside Norwegian jurisdiction (DSB, 2019). This opens the possibility that secured areas or sectors have defences weakened by another subsector with lower security measures. The complexity of cyberspace is an extreme challenge. As companies are bought by others, new supplies offer a better deal and technology is constantly changing, there is a considerable risk of exposure (DSB, 2019).

Respectively, it is not only an organisation's complexity that has to be considered but the complexity of cyberspace and cyber resilience. As resilience is not considered a property of a system but an ability that must be developed and cared for, as with the environment being ever-changing, resilience measures must follow the paste (Bento et al., 2021).

3.4.1 Building Cyber Resilience Within a Complex Organisation

To answer the third research question of what contributing factors have the potential to build cyber resilience within a complex organisation, an overview of the newest academic findings will follow. Later in this project, relevant frameworks will be analysed and explained, which can be seen in combination with the presented findings from this section.

Some general suggestions and findings can be considered pre-established within security measures, such as being aware of current threats (KPMG, 2018) and being risk-focused (KPMG, 2018; Dickson & Goodwin, 2020); however, these will not be included in this process. Reoccurring suggestions on cyber resilience building are collaborating with other sectors, having management prioritise resilience and educating employees (KPMG, 2018). Though all highly relevant measures, there is a lack of how these could be best achieved within a complex organisation. How should management prioritise resilience, and what is the most acceptable and effective way to educate the different layers of people within a complex organisation? An overview of four direct action-based ideas to foster cyber resilience will be presented. The first is to create an overview of an organisation's needs and functions. Second, to create a shared understanding and definition across the organisation. Third, allow for adaptive capabilities and systems. Fourth, ensure the freedom and authority for actors to react.

Firstly, an overview of where an organisation stands concerning cyber resilience can allow insight into areas that require attention. As Hollnagel (2010) described, being resilient is something an organisation must strive towards. It can be measured by analysing the four essential elements of resilience, as suggested in the RAG. A resilience profile can be attained, giving insight into the organisation's resilience.

Secondly, one of the main issues with resilience is that it is understood differently between sectors (Linkov & Knott, 2018). Without a common understanding of how cyber resilience is built, the go-to method is to authorise new regulations and procedures with every new threat (Gisladottir et al., 2016), as the lack of understanding of knowledge forces companies to react individually. This strategy has, however, been shown to be counterproductive since it results in a rise of stress within the organisation due to too much time and focus being used on the training and familiarity of the new procedures (Gisladottir et al., 2016). Research shows that alternating every defence to the individual case and focusing intensely on readjustment (Hausken, 2020) would help a company to be resilient. This means that there needs to be a great understanding of how the attacked system functions, how the protective measures work and how the company would adjust to the stressors through understanding what cyber resilience is and how it can be achieved for the specific organisation.

Thirdly, an adaptable environment can help a complex organisation build cyber resilience. A cyber-resilient system allows for flexible behaviour with an understanding of the context surrounding these behaviours and how the system reacts (Rankin et al., 2013). This indicates the focus should be on actual reactions and responses under threat, not how they "should" act. Core values of the framework of resilience engineering structures sternly recognised these elements as crucial to achieving resilience, as will be further discussed later in this chapter. Focusing on human capacity and abilities within complex organisations requires mapping. Humans can adapt but need primary resources, trust and autonomy, as Rankin and others (2013) and Hollnagel (2009) stated. Human behaviour can be measured in "motivation, opportunity and ability" (Kleij, 2019). Evaluating how those working within a complex system function in these three aspects can give great insight into how an organisation can foster a secure environment and create opportunities that will result in cyber-resilient behaviours.

Fourthly, human factors greatly influence how cyber resilience is built within complex organisations. It is suggested that people usually choose the most appropriate response when they are experiencing a new threat or uncertainty (Rankin et al., 2013; Hollnagel, 2009). As human factors can be seen as a larger category of influential factors benefiting the building of cyber resilience within complex organisations, it will be discussed in greater detail.

3.4.2 Human Factors & Adaptability

Human factors are defined by the World Health Organisation (2016. p. 3) as "the understanding of the interaction among humans and other elements of a system, and the profession that applies theoretical principles, data and methods to design in order to optimise human well-being and overall system performance." This definition clearly holds transfer value to how vital human factors are in building and strengthening a functional cyber resilience value within a complex organisation.

Comparing a highly resilient person to a highly resilient system creates a clear and symbolic analogy. A meta-analysis by a team of psychologists concluded that a person could be resilient in one area, such as at work, whilst not in personal relationships (Southwick et al., 2014). Comparatively, a system can be great at detecting and protecting itself against one cyber threat but not another. Similarities can also be drawn to different types of environments or threats by those employed in a complex organisation. Furthermore, environmental elements can influence how traits, qualities and values interfere with how one interacts with the environment (Southwick et al., 2014). For an individual person and as a part of a more extensive system, this can be evident in what type of project they are included in and if the way they work matches their preferred work style. When a stressful situation is experienced, the current environment will be influenced by how other people react and respond, what available resources are presented, the work culture and other factors within an organisation (Southwick et al., 2014). This is similar to how a system is designed to base its response on experience, current knowledge, and internal and external circumstances.

Lessons from psychology on human behaviours and coping mechanisms can give great lessons to employees working within a system when developing and adapting cyber resilience behaviour. Additionally, the system's organisation can also draw lessons from this comparison. According to Southwick et al., (2014), continuously attempting to foster a positive manner based on one's experience can accurately describe a resilient person. Furthermore, it is suggested that "the capacity of a dynamic system to adapt successfully to disturbances that threaten the viability, function, and development of that system; and a process to harness resources in order to sustain well-being" (Southwick et al., 2014, p. 12). Importantly, there are comparisons to be drawn, as this description could just as well describe a resilient system within a complex organisation if the word "well-being" is exchanged with "functional capacity."

A resilient person is continuously in the process of building their individual capacity to adapt, just like a system. By attempting to understand the influences that arrive from the environment, social expectations, communities, and subcultures within an organisation (Southwick et al., 2014), an interconnection can be understood and applied to create an adaptive system. If strengthening group A will positively affect groups B to Z, it is possible to raise resilience across multiple layers by starting with smaller sections. Interaction, cooperation, experience sharing and observative learning will naturally spread the growth of adaptive cyber-resilient behaviours within the organisation. There could be a link between human factors and resilience if a highly resilient individual could influence the system to build resilience, as already seen in other operational fields. Bertoni et al., (2022) investigated nurses in a Brazilian intensive care unit and found that resilient individuals can influence the rest of the work environment to think, feel and act in similar resilient-based manners. Respectively, understanding that people react differently to stressors not only based on previous experience and personality but based on the given time, environment, resources, mood, confidence, and other influences, why should a complex organisation function any differently? Understanding systems, processes, themselves, work colleagues and the environmental stressors and expectations are necessary, as coping with one type of hybrid threat might require different resources.

According to Gaskell (2021), four out of five companies mention human factors as an element that is problematic when implementing security in cyberspace. A deeper understanding of how employees work under stressful conditions could give great insight into how to assist in this perception (Gaskell, 2021). Knowing who needs reassurance, a challenge, constant supervision, and so forth creates awareness within the complex organisation. This awareness is fundamental to building cyber resilience and security awareness (Diesch & Krcmar, 2018).

Adaptation is an important quality required to manage a complex system with uncertain conditions (Rankin et al., 2013). This could go a long way in establishing a resilient system, with areas needing attention: understanding context, working conditions and influences it can take on the more extensive system (Rankin et al., 2013). A realistic view of how humans work in the system, not just on paper, is equally important as a complex system often includes inconsistent challenges and new and unknown disruptions (Rankin et al., 2013). It should be underlined that humans are mainly able to successfully adapt given that the system provides room and time for this adaption to occur (Rankin et al., 2013) by allowing for instinct, training and expertise to guide further actions. However, it is essential to note that this does not mean people can fill in and defend against system errors (Rankin et al., 2013).

Importantly, all mechanisms, procedures, attacks, and structures are originally human-made. Ultimately, people design defence and attack methods and security systems, suggesting that there can be lessons in understanding a cyber attack by understanding human behaviours and reasoning. This indicates that human factors can be important when designing resilient systems and organisations (Widdowson, 2022).

3.4.3 Resilience Training

The third research question aims at identified factors that contribute to building cyber resilience within a complex organization. Just like any other skill, training, drills, and preparations will enhance resilient organizational properties (Grøtan & van der Vorm, 2016). There are a variety of frameworks that have methods on how to attain cyber resilience within an organization, that will be discussed shortly. But in addition, training can strengthen cyber resilience.

The TORC – Training for Operational Resilience Capacities is a training program developed by Grøtan and van der Vorm (2016) and is an example of cyber resilience training. The program is based on the principals of resilience engineering. Mainly, the training program is designed to be tailored to each organization, focusing on its operative and managerial capabilities while considering international standards. The program aims to “appreciate, nurture and improve” resilient and adaptive prospects that already exist within the organization (Grøtan & van der Vorm, 2016). In short, there are four aspirations on the TORC-scale recipe; guard the wanted mode of operation, build robustness, rebound and endure over time.

A holistic view of cyber security must be implemented (Gaskell, 2021), as it is not a singular IT or OT problem (Widdowson, 2022). As mentioned in the sections above, human factors significantly impact securing a cyber-resilient mindset within a complex organization. For these cyber-resilient behaviours to grow, training will allow employees to conduct accurate and safe risk management decisions and build trust in their capabilities and the complex system they are working within. As previously stated by Linkov and others (2018; 2019), being adaptive is extremely important for building cyber resilience. As Woods (2015) supported, resilience can thrive because it allows for a system and those who operate within it to foster adaptability.

4. Methodology

The following section provides an overview and justification for the choices made regarding research design, methods, data gathering, and analysis in this research project. The theoretical approach and strategy that structured the making of this project will also be explained. This section aims to justify how the choices made will lead to adequately answering the operational research statement and related research questions. Lastly, possible biases and assumptions will be addressed.

4.1 Purpose

The purpose of this master thesis is to investigate how cyber resilience could be strengthened within a complex organisation. This has been done by gathering and analysing existing research on the given construct in addition to supportive theories and concepts such as risk, cyber security, complex organisations and human factors. Moreover, an extensive investigation of scientifically approved cyber resilience frameworks has been evaluated to identify contributing factors that apply to complex organisations. In addition, interviews conducted with practitioners within a complex organisation were gathered to get insight into the elements through real-life understanding. An in-depth literature review, interviews and document analysis form the theoretical basis for answering the research questions.

4.2 Research Methods and Design

The research method for this project is based on an abductive methodology (Conaty, 2021), where the gathered data drives conclusions. Information on cyber resilience and cyber resilient framework were gathered and compared with the observations and experiences of relevant informants within the cyber field. Arguably, the research method has deduction elements (UKEssays, 2018) due to the data guiding and supporting the constructed pre-determined argument that cyber resilience is a positive supplement to cyber security. The difference between these two approaches, however, is that the goal of this project is not for the data to prove or disprove an applied theory – as is the case in deductive methodologies (UKEssays, 2018) – but to preliminary explore possible connections.

It is accepted that with the unclear definitions of cyber resilience concepts, an exploratory design is taken to drive a better understanding (Erickson, 2019). In further support for an exploratory design, understanding how cyber resilience is built is lacking in the research field (Erickson, 2019); It is necessary to lay the groundwork and let the data lead to outline future use. This research project uses primary and secondary data (Erickson, 2019). The secondary data is the theory of research used in the literature review and document analysis. In contrast, the primary data (Erickson, 2019) was gathered through interviews.

All these aspects strongly support this research project as being qualitative (Erickson, 2019), as data was collected via interviews from a smaller sample size. The interviews were semi-structured with open-ended questions, facilitating the exploration of novel topics, paths and salient topics for each interviewee.

4.3 Case

The international energy company involved in this project has been anonymized, as well as the identity of the participants, to ensure confidentiality (Coffelt, 2017; Bos, 2020). The name of the specific company has no relevance to the project, as the intent is to explore relevant concepts and how these align with a complex organization, broadening its applicability. The company can be considered a sizeable international enterprise within the energy sector. The primary data collection was conducted within one company, and a broad area of expertise was gathered and explored.

4.4 Interviews

Three distinct groups were interviewed for this project. The first was practitioners within the risk function possessing different backgrounds, assignments, positions, and expertise. The second was a Senior Leader of the same energy company. The third was an independent expert in resilience, safety, and security. Though the communications between the researcher and the three groups varied, the general structure of the interview and the guide was uniformly applied across groups.

The benefit of conducting interviews in this study was the chance to explore relevant concepts through practitioners more generally (Majid et al., 2017), with this unique understanding leading to the discovery of gaps and disagreements in fundamental principles, goals, needs and strategic improvement. The only requirement for participating in this study was being employed by the specific company and willingness to contribute. An interview guide was constructed as a collaboration between the researcher, their supervisor and representatives from the company based on interest points and the gaps discovered in the preliminary literature research. The interview guides for each group can be found in the appendix. The informants were given an ID number and will now be called "informant (ID number)."

Table 1: Informant ID

	ID Number		ID Number
1	668	8	147
2	954	9	632
3	318	10	522
4	762	11	813
5	876	12	149
6	498	13	Senior Leader
7	239	14	Expert

4.4.1 Interview with Employees & a Senior Leader

The external supervisor recruited participants in this group. Firstly, a pilot interview was conducted to explore if the proposed interview would be sufficient for the research processes (Majic et al., 2017). The participant was not given any information on the content of the interview but instead told the project was related to resilience, with an allocated one-hour slot. In light of this interview, future interviewees were better prepared by being given the project's four key terms - resilience, cyber resilience, cyber security, and risk – beforehand. The participants were also advised that no prior research would be necessary as the point was to gain their understanding and perspectives and not any official concept definitions. The pilot study also showed that the questions were relevant and easily understood, allowing the participants to answer freely, explore the concepts, and get involved with the content of the themes.

The participants were given a short introduction to the study and the researcher, and the informed consent form was provided. A copy of the informed consent form can be found in the appendix. The interview was not recorded due to anonymity and confidentiality, resulting in the researcher writing notes during and immediately after the interview. These two documents were then combined. If there were any questions regarding what was said or any confusion, the participants were contacted face-to-face, if possible, to clarify any statements.

The test interview was the basis for how the rest of the interviews were conducted, and no changes were made across the 12 interviews from the practitioners. At the same time, the expert informant and a Senior Leader had separate interview guides. Four interviews were conducted via Microsoft Teams, whilst the rest were conducted face-to-face. The interviews lasted from 27 minutes to 3 hours, while most interviews were generally completed within 55 minutes. The interview process was conducted between March and May 2023. All interviews were conducted in Norwegian, except for two in English. The participants chose the language they felt they could best express their thoughts. The interview format was semi-structured but included open-ended questions. The experiences showed that the questions functioned more as themes, and the participant spoke of whatever came to mind. The goal was to explore participants' knowledge, perspectives and understandings of the given constructs to gain new knowledge.

An acceptable translation for "resilience" does not exist in Norwegian, with the closest translation being "motstandsdyktighet." Hence, there was confusion about the meaning and translation of this concept among the Norwegian-speaking participants. This is a known problem and could have affected project results.

There was no compensation for participating in this study, and reassurances were made that submission could be withdrawn at any time.

4.4.1.1 Anonymity and Confidentiality

An essential part of the data collection in this study was to ensure anonymity and confidentiality to protect the identity of the company and participants. In this case, anonymity means that no one other than the researcher can identify who said what in the interviews (Bos, 2020), including confidentiality (Bos, 2020; Erickson, 2019), as identifying markers such as personal information was removed.

One of the measures implemented in this study to protect anonymity and confidentiality was a letter of informed consent (Millum & Bromwich, 2021). The consent form informed the participants of their rights to withdraw from the study at any time and how their data would be stored and used. Another measure taken to ensure participants' privacy was that no interviews were recorded (Bos, 2020). The interviews were written from notes taken during the interview and post-interview researcher memory recall. Another measure was giving the participants a randomly generated ID number from the start, known only to the researcher (Bos, 2020).

4.4.2 Interview with the Expert Informant

The expert was contacted in February to ask if they would be interested in participating in this study. The expert was given a short overview of the project and the researcher's thoughts on how it could progress. They were contacted again in April, and an interview was scheduled for May. One hour was set for the interview. The expert was provided with nine questions three days before the interview, and the instruction that the questions were seen as a loose guide and that their thoughts, perspectives and knowledge were appreciated in whatever form they deemed most relevant for the project. Like all the other interviews, informed consent was provided, and the interview was not recorded. After the interview, the expert was contacted via email for approval of what was used in the interview.

4.4.3 Document Analysis of Cyber Resilient Frameworks

Conducting a document analysis within an exploratory study is a common addition to qualitative research designs (Bowen, 2009). It is considered adequate, easily attainable and does not influence the investigator by other means than the written word (Bowen, 2009; Yin, 2018). Though there is a possibility that the researcher may have been too selective in choosing relevant documents jeopardising data availability and exploring possible biases, comparing the results to the expert testimonies and interviews ultimately triangulates the data and strengthens the reliability and validity of the analysis (Bowen, 2009). A list of all possible resilience-building frameworks was identified and collected. Every framework had to meet the following four criteria to be relevant for this project:

1. It applies to cyber resilience (to a greater extent than simply having resilience as a priority within the cyber security frameworks).
2. It applies to complex organisations.
3. It is relevant to the energy sector.
4. It was accessible through being free of charge.

Forty-nine frameworks were identified, with seven meeting the inclusion criteria, as shown in Table Two.

Table 2. An Overview of Selected Cyber Resilient Framework for Document Analysis

	Name of Framework	Year	Author(s), developer or organization
1	**CCE** - Consequence-Driven Cyber-Informed Engineering	2018	Idaho National Laboratory
2	Conceptual Framework for Developing **Resilience Metrics for the Electricity, Oil and Gas sector** in the United States	2015	Sandia National Laboratories, for the US Department of Energy's National Nuclear Security Administration.

3	**CREF** - Cyber Resiliency Engineering Framework	2011	MITRE
4	**NIST** Cyber Security Framework	2013	NIST - National Institute of Standards and Technology. U.S Department of Commerce
5	**WEF Board Principle Playbook Oil and Gas**	2021	World Economic Forum
6	**Cyber Resilient Scotland**: Strategic Framework	2021	Cabinet Secretary for Education and Skills
7	**CERT-RMM -** Resilience Management Model	2016	Caralli, Allen and White. Carnegie Mellon University

4.5 Possible Biases

Generally, it is essential to be aware of biases that can influence the researcher in the choices they make, the questions asked, and how the data is interpreted (Pannucci & Wilkins, 2010). A *bias* is a conscious or unconscious influence that can skew the outcome (Pannucci & Wilkins, 2010; Šimundić, 2012). It is impossible to remove all forms of bias within the research process (Cristofaro, 2017). However, as a layer of protection, it is beneficial to evaluate the possible biases that could have influenced (Pannucci & Wilkins, 2010) the study or researcher. Two possible biases have been identified as a part of this study, and measures have been taken to actively try to reduce the chance to ensure transparency and accuracy (Šimundić, 2012).

The first bias relevant to this study is selection bias, which is when the participant sample is not entirely randomised (Tripepi et al., 2010). The participants in this study were employed by the same company and had positions related to the fields of risk management, risk analysis, IT, OT or cyber security. Generally, when a sample is not random, that would suggest that the result of the study does not represent the general population (Šimundić, 2012; Tripepi et al., 2010; Pannucci & Wilkins, 2010). However, for the purposes of this study, it can be argued that the sample is representative of the relevant sector, as similar companies have the same values, interests and areas of expertise. The goal was to represent relevant knowledge that would be valuable for complex organisations within the energy sector, so it can be argued that this sample is representative.

Another bias that could influence this project is confirmation bias, when information in favour of what is already believed as the best answer is searched out (Peters, 2020). A favourable view of the term resilience and a firm belief that the potential the construct holds can unconsciously be paired with factors not notable. Such as extreme positive regard while discussing the concept, creating an expectation that the participants should also be positive towards the concept. Furthermore, the interpretation of data could be judged favourably (Nickerson, 1998) by responses that align with what the researcher wanted to find in the study. Efforts were made to be mindful and aware of this bias, which might be the only way to safeguard against it.

4.6 The Relationship Between Researcher and Informants

The researcher and participants' relationship can influence the interview and how information is interpreted (Råheim et al., 2016). The interview format was based on open-ended questions that allowed for exploration, such as "*How do you understand the term resilience?*" This was intended to create an atmosphere where there were no "correct" answers because the essence of the project was to explore current understanding.

All interviews were conducted on the company's premises or via Microsoft Teams during business hours. It is suggested that a good repour between the researcher and interviewee is beneficial to create valuable responses (Miljad et al., 2017; Råheim et al., 2016), but importantly, this was something that naturally occurred and was not designed. All interviews started with a short introduction about the researcher and a more extended introduction of the person being interviewed, which could have influenced the environment for the data collection (Majid et al., 2017). However, this was not intentional, and the social interaction before the interview questions were introduced would have been present regardless.

4.6.1 Assumptions

There were two assumptions made for the concepts of this research project. Firstly, that cyber resilience is a relevant part of cyber security and that there is valuable information to be found in talking to people within the cyber security and risk management field.

Secondly, a few assumptions were taken for granted in regard to the participants of this research project. It was assumed that everyone who participated wanted to contribute to the project based on interest, knowledge and curiosity to improve a relevant field. Furthermore, it was assumed that participants did not do any additional research before the interview other than Google terms they potentially were unaware of beforehand. Lastly, it was assumed that the participant was honest and that the collected data held accurate intel and value to the project.

4.7 Research Quality

Some measures and thresholds must be met to ensure scientific soundness and quality. Two crucial aspects are reliability and validity (Golafshani, 2015). In other words, can the result presented in this research study be trusted to represent facts accurately? The two variables will be discussed shortly in relevance to this project.

4.7.1 Reliability

Reliability refers to how consistently the measures supported the research question (Segal & Collidge, 2018). This means that regardless of how often something is tested, as long as the same measure is used, the results would be similar to the previous. The goal is to reduce the chance of error (Segal & Collidge, 2018). Conducting a study that is deemed high in reliability can significantly help raise scientific acceptance within the scientific community (Brink, 1993), which is one of the goals of this research, valuing cyber resilience framework as an actual strengthening of cyber security. Considering that this is a qualitative study, that is not backed up by statistical soundness or calculations, reliability is of even higher importance (Brink, 1993). As consistency is an essential part of reliability, it usually is a better requirement for quantitative research design, as one would not (and should not) expect the same answer from different people in an exploratory study. However, other measures can be reliable measurements in a study. Reliability also entails that the researcher (Brink, 1993) can collect and interpret data (Segal & Coolidge, 2018). Great importance has been put on accurately retaining the data and interpreting it true to intent. Also, the questions are the same for every group of interviews and are asked in the same manner.

4.7.2 Validity

There are various forms of validity, but three categories are usually relevant to explore in qualitative research designs (Yin, 2018) construct, internal and external validity. Validity indicates if the methodology allowed for an accurate study of what it is indented to (Brink, 1993). In qualitative research, validity can be seen as a subjective measure (Hafeez-Baig et al., 2016; Yin, 2018), which is why construct validity is highly regarded. This includes the initial idea that the reassurer wanted to explore and the research questions that were constructed further to expand the theory (Golafshani, 2015). According to Yin (2018), one way to strengthen the construct validity of a study is to allow for a new understanding of a construct to be compared to official terminology and let that guide how a concept should be defined. This study has done this for three terms: resilience, cyber resilience, and cyber security.

Internal validity includes the understanding that the conclusions drawn in a research project are a true reflection of the collected data (Brink, 1993) or if there were other variables not considered that had a significant influence. As this exploratory study focuses on matching real-life understanding to theory, it can be challenging to judge internal validity as no causal relationship (Yin, 2018) is relevant in this research design. External Validity judges if the results apply to other similar groups (Brink, 1992) or how generalisable (Yin, 2018) the findings are. Reasons and justification for why these criteria have been met can be found earlier in this chapter.

5. Findings

This chapter will present the findings from the interviews and document analysis following the three research questions. The chapter presents one research question at a time and includes all relevant findings from the interviews and the analysed frameworks. The presented findings in this chapter will be used for further interpretations and comparisons with the information introduced in the literature review. The findings and discussion are separated to allow the data to be understood before conclusions are drawn.

The first research question focuses on the basic understanding of cyber resilience within the energy sector. The interviews of practitioners and expert informants serve as the primary source for the presented findings on the research questions. Relevant findings from the analysed framework will also be included, with the main findings being three different understandings of cyber resilience.

The second research question intends to connect the understanding of cyber resilience to the more fundamental aspects of risk and security and evaluate how the three constructs coexist. Findings from interviews and frameworks will be introduced. Notably, the reflections during the interviews about security in the second research question naturally blended in with reflections from the first question, meaning that the two sections should be seen as an extension of each other. The main findings will include how the concepts can be seen as extensions of each other.

The third research question aims to identify elements that reinforce cyber resilience within a complex organisation by presenting findings from the interviews and analysis of existing cyber resilient frameworks. The main findings include four main groupings that correspond between informants and frameworks.

5.1 How does the Energy Sector Understand the Concept of Cyber Resilience?

Through interviews with practitioners within the energy sector with expertise in risk, risk management, cybersecurity, safety, IT and OT, several factors influence how the understanding of cyber resilience is formed. Generally, the perception was based on information provided through the company, previous and current job experience, the media, and personal interest and experience. Two primary groupings can be established that describe what formed people's understanding of cyber resilience: organizational factors and personal experience.

The data gathered in interviews with opened-ended questions naturally allows for more extended reflections, such as "How do you understand the concept of cyber resilience?" Regarding understanding cyber resilience by those working in the energy sector, three more significant categories have been created based on the answers within the two groupings of organizational factors and personal experience. Namely, (1) resilience as more than "motstandsdyktighet", (2) resilience as the new form of security, and (3) resilience as adaptive capabilities. In addition, the understanding and reflections made by an expert informant and a Senior Manager will be included. The mentioned perspective and knowledge will serve as the base for discussion on enhancing measures for cyber resilience.

Notably, every informant answered that the only difference between resilience and cyber resilience was the addition of the word *cyber*, which is why both "resilience" and "cyber resilience" are used in this chapter. All informants had strong reflections on this topic. However, every informant either was unsure of how to define the construct precisely or had trouble narrowing it down to a definition, suggesting how important it is to form an understanding of the concept.

5.1.1 Resilience as more than “motstandsdyktighet”

“*Motstandsyktighet*” is the translation for resilience in the Norwegian language. As already established, the translation does not accurately represent the word resilience. The interview results show an explicit agreement between the informants in this study and current literature that resilience holds a more substantial value to them and their field than is currently the case. Suggesting that it is crucial to divulge this aspect further. As a response to the question, “*How do you understand the concept of resilience?”* the most repeated answers included “*motstandsyktighet, but more.”*

The Petroleum Safety Authority in Norway does not officially define cyber resilience. Though, it can be assumed that each company has an official definition used internally. Introducing a possible caveat to this section, there might be an official internal definition that this project is not privileged to, but the researcher of this project has no information about whether this is the case. Regardless, this makes it difficult to perform any official comparison between the expectation from a company towards the response from those working within the given organisational system. However, a possible definition for one company would not be relevant in analysing a general understanding of cyber resilience within the energy sector; there would have to be an official definition from PTIL. As confirmed by the expert informant, resilience is still understood differently between sectors and people.

Generally, regarding public information on cyber resilience, the energy sector in Norway has been put on alert that they are targeted through cyberspace (PST, 2023; DSB, 2019), and cyber resilience must be prioritized (ISO, 2023). Indicating that it is a current and relevant topic for the energy sector. As stated by informant 318, "*I have no personal definition of cyber resilience; when the company provides me with a definition, I will take responsibility to implement it into the department I work in*." Supported by informant 954, "*Cyber resilience is a hot topic for the company, and expanding the understanding and implication of it lays in the near future."* Signalizing that cyber resilience is valuable to the industry. However, everyday understanding is also valuable and could be used as the groundwork for how cyber resilience works or what function it could serve within a company.

Almost every informant mentioned "motstandsdyktighet" and the metaphor "bounce back." "Motstandsdyktighet" translates into keeping danger at arm's length without affecting operations and production. Most informants mentioned the word "motstandsdyktighet" and added that it was simply not an accurate description of the term and had additional defining words that expanded on the concept. As described by informant 239, "*It does not cover all its properties (...) it is too complex of a construct to be described like that*." Informant 498 stated, "*You should be able to function before, through and after an attack*", in describing why simply resisting a threat was not enough of a description. As added by informant 762, "*the totality of all activities, processes, governance that supports watching, waiting, detecting, protection, response and recovery*," resilience is viewed as a more complex construct than what "motstandsdyktighet" entails. The same tendencies were present in the interview conducted with a Senior Leader. Resilience is more than bouncing back, more than just being able to resist; It should result in a much stronger form than before the experience. "*A new, more suitable and developed form*" (Interview with a Senior Leader).

Terms from the reflections were that resilience included abilities such as: *detecting, awareness, monitoring, protection, learning, responding, recovering, preventing, and adjusting*. All key terms are mentioned more than three individual times, and the terms (one or more) "*detection, prevention and recovering*" were mentioned in every interview. Most informants mentioned the bow tie method, indicating that they imagine the process of cyber resilience through the stages before (prevention) an attack and after (recovery) while reflecting on cyber resilience. Informant 813 attempted to narrow down to a word that expressed what resilience attained and suggested "*survival ability*" and "*endurance*." This was further discussed with the expert informant, who suggested: "*hardfør*" (hardy) or "*tilpassningsdyktig"* (adaptable). Commonly between interviews, the word "robustness" was mentioned. The word was used to describe a property of resilience rather than a synonym or translation and further reflected in the expert interview that resilience entails much more adaptability than what robustness includes. Resilience as adaptability will be further discussed later in this section.

The interviews indicated a maturity further than the industry's implementation of the construct. This leads to the next reoccurring theme concerning the first research question, as introduced by a quote from the interview with a Senior Leader "*Resilience is so much more than security*." Also strengthened by a statement made by the expert informant "Cyber resilience is an advances form of conducting safety."

5.1.2 Resilience as A New Form of Security

As presented in the literature review, cyber security involves the continuance of necessary functions before and after a cyber-attack (Linkov & Kott, 2018); similar to resilience, both constructs want to protect a system from an attack. According to the interviews, when asked to reflect on the distinction or connection, all expressed that both were needed and that they strengthened each other. The intent of the interview guide when trying to define cyber resilience was not to compare the concept to security, as a later part was focused on the connection between the subjects. However, a natural tendency formed in reflecting on what cyber resilience was towards how it correlated with security.

Generally, there was consensus in the interviews that the primary separation between resilience and security was that within resilience, there is an acceptance that an attack or an unwanted event will occur, while security based its principles on the fact that everything could (or should) be prevented. As stated by informant 147, the security field can be considered the fundament, while resilience describes how a situation is handled further.

According to informant 390, if you set the only acceptable outcome to zero incidents, usually the way security is seen from a risk perspective, "y*ou can create an unattainable goal that always will result in something negative.*" The transcendence of resilience in this example would be that the perception changes from zero incidents to withstanding and recovering from that incident that will occur—changing the goal from zero incidents to not being hurt by incidents that occur. Supported by the statement, "*With the climate we live in, it is necessary to expect attacks. It indicates a maturity to see it from a resilient perspective rather than a security perspective*" (Informant 668). Further continued with the understanding that "*resilience is now the umbrella term over security (...) where security is preventive, and resilience recovers and adapt*" (Informant 954). Also, informant 762 adds, "*Resilience involves everything security does, but not vice versa*," supporting the argument that resilience can serve as the umbrella term above security.

More insight can be found in the interview with informant 876 "*Resilience includes a stronger understanding of what is happening, and of critical functions*,“ suggesting a view that resilience can go beyond traditional security patterns to include "*human factors and critical function in relation to people*" (Informant 876). As resilience is seen as more complex, more layers of an organization can be accessed and seen in combination with each other. With the acceptance that all informants still value the need for security, there was a clear trend that cyber security was the fundamental aspect that cyber resilience now has taken over as a continuation of that practice, "*resilience can take over when security meets its limits*" (Informant, 318). Informant 632 added, "*Cyber resilience is how you invest in sound cyber security.*" As stated by a Senior Leader, "*Resilience is important because, generally, it looks at coping.*" As suggested by the interview, in terms of cyber security, it is essential to understand that resilience, cyber or not, will regardless bring improvement to the whole organization and that every layer of an organization is influenced by each other. If you manage to build resilience in one part, it will slowly spread to other aspects as a complex organization is interdependent on each department or layer. As expressed by most informants, resilience takes it further than security by accepting that something unexpected can happen. This indicated the ability to handle unknown and unexpected situations through the skill of being adaptive.

5.1.3 Resilience as Adaptive Capabilities

The literature review states that resilience is about adaptability (Linkov & Palma-Oliveria, 2017). As most informants reflected on what cyber resilience meant and how they understood the concepts, most agreed that resilience was a mature method of handling risk and threats. Though most informants did not mention "adaptable" or "adaptive behaviours," almost everyone spoke about handling the unknown and unthinkable and acting on the spot according to the given circumstances, indicating adaptive features.

As stated by informant 498, "*You have to be able to change or be flexible, and not set in ridged security strategies. You need an understanding of the specific situation*," clearly signifying being adaptable. Informant 149 spoke about thriving despite challenging circumstances, which is highly relatable to adaptability to the given environment and circumstances. Also supported by informant 876, who reflected on how important it was to be able to turn on a whim in crisis management and handle the given situation then and there. Informant 476 added, "*You need to be able to handle what you cannot predict, which is challenging*." Clearly, all these statements reflect adaptable capabilities without using those words. The interview with a Senior Leader clearly stated that evaluating how one could adapt to challenging contexts was essential and that the answer to that could be through resilience.

According to the interview with the expert informant, being adaptable is the main takeaway supporting the trend of being resilient. The informant was asked to elaborate during the interview on a definition of cyber resilience that was not based on any theory but an explanation on the spot, "*cyber resilience is about understanding and developing the practices, management and the organisation have concerning mastering a technology that does not have their trust, but they* *are dependent on*" —also, signalising adaptive capabilities. Furthermore, the expert reflected that, generally, resilience could take form in one of three ways in a complex organisation; failsafe systems, the combination of all assets or human capabilities.

> a.) technical systems and procedures have implemented failsafe and protections that create a flawless system with protective measures automatically activated.
>
> b.) a combination of well-prepared and successful risk management, preparedness and business continuity can create the "perfect" defence that results in resilience. Nothing new is added to the business; it is just a good merge of existing elements that creates a resilient organisation.
>
> c.) people who "know" how to act when facing the unexpected. Capabilities can be innate but also fostered within the culture of an organisation.

Capabilities within an organisation were also mentioned as a strong point in the interview with the Senior Leader and resilience behaviours reflect adaptability; both will be further discussed in the reflection around the third research question. Furthermore, as discovered by the latest pandemic, complex organisations faced challenges they were ready to handle without knowing, and the business and employees could adapt to the situation (Interview, Senior Leader)

According to the data presented by practitioners, senior management and a leading expert, resilience involves adaptive capabilities.

5.2 How does the understanding of risk and security influence the understanding of cyber resilience?

As discussed in the literature section, resilience is rooted in other paradigms like risk and security. Taking into consideration that the participants in this study work within the fields of safety, security, cyber, risk, risk assessment and risk analysis, IT, OT, management and/or engineering, there is a preserved notion that during their education, work experience or current job position they were introduced to the concepts of both risk and security. Intentionally, possible variables that indicate what type of background, education or work experience the participants have not been taken into consideration in this section. Though it could have an influence on how the core understanding of concepts was formed, the value of confidentiality and anonymity falls stronger. Generally, everyone interviewed works within the energy sector, has successful careers in relevant fields and is deemed as having adequate background, insight, skill, and expertise to know these subjects. As previously stated, the relationship between security and resilience has been explored in the reflection on the first research question, so that some additional aspects will be added to the end of this section as an extension.

5.2.1 Risk and Security in Relation to Resilience

Naturally, as the Norwegian Petroleum Safety Authority controls the Norwegian energy sector, the official definition of risk dictates the fundamental understanding in the sector. Risk is the consequence of an action and the attached uncertainty (PTIL, n.d). Most informants started the reflection by stating some form of this definition. "*Probability of a consequence*" (informant 954), and "*vulnerability, probability, and consequences* (informant 239). Also, most emphasise the elements of uncertainty. In addition, most informants mentioned that risk is anything that could go wrong, which requires a risk-based mindset. An extension of a risk-based mindset is a resilient mindset, which can be seen as a natural evolution of security. If resilience is the new security, then resilience-prone thinking should be what leads to a risk-based mindset. As described by some informants, risk indicates danger, and resilience is what reduces the risk of the threat becoming dangerous, "*Resilience is what lowers risk*" (informant, 632). The consensus on how those interviewed describe and understand risk indicates that a solid and recognisable definition of resilience would be applicable for them to include in their work—more on this in the discussion section.

Furthermore, most informants reflected on resilience in relation to risk, with risk being the problem and resilience providing the solution. To illustrate, "*Resilience is to what degree you can handle risk (...) Risk is what activates resilience*" (informant 668). Following that statement, the informant was asked if they believed solid cyber resiliency could eliminate all risks. Most conclude that there will always be risk, so resilience is a state you must fight to attain. This signifies a strong connection between the acceptance that new forms of threats will always be present, and resilience is a solution that is never completed but requires constant activation and attention.

More than one informant saw a strong connection between risk and resilience as solid elements of risk management. Preparing for what can happen is one of the most essential elements of both concepts. Understanding risk can also be described as the core method of knowing where resilient frameworks should be prioritised. The connection between risk and resilience inspired reflections on the value of an acceptable expectation for risk. Accepting zero incidents as that standard leaves out the potential for great learning. More value could be found in how the situation was handled, good or bad, as previously discussed. Strongly supported by reflections made in the expert testimony that within risk management, it is imperative to evaluate what happens after a crisis and not fall back into only valuing the probability assessment that follows a new experience—evaluating what actions were made when an unexpected incident occurred, such as what choices were made, and which behaviours were present. The expert informant reflects that the answers to these statements will be valuable in improving measures leading to a more resilient organisation.

Moreover, multiple informants reflected on how similar the basic principle of risk is to the properties of resilience; if you do not look, you will not find. Accurately preparing for and handling risk to protect business continuity and recovery requires awareness and alertness to own and others' systems, procedures, value chains, communications, and people. Informants drew similarities between these elements within risk, as also being present in resilience, suggesting a similar mindset. Having the reasonableness and integrity to investigate what seems to be working fine indicates the maturity of a company. However, that is an element more present in resilience than risk management.

Interestingly, informant 522 described the safety and security field from a decade ago, where cyber incidents were rare, and little to no knowledge was available. Supported by the statement of a Senior Leader, cyber security has gained more attention in the last ten years, and the progress has been rapid. Previously, there were vital elements of fear and shame connected to cyber threats, as no one wanted to be the first to get hit and suffer the consequences of the media, competitors and the general trust and reputational aspects that would be negatively affected. That influenced how companies evaluated risk, security measures and standards of reporting incidents. The acceptance that incidents will occur that are embedded within resilience made significant changes to risk analysis and risk management within the energy sector. The change in perception included a change in risk and security culture, with an openness to share and report without shame, creating a safer environment. As concluded by informant 522, this led to a more practical focus on business continuity and recovery, elements relevant to security and resilience for a complex organisation.

Adding to the previously concluded relationship between security and resilience in the findings for the first research questions, a few more connections can be drawn.

According to the expert interview, resilience contains some elements that security lacks. The curiosity within resilience to learn from and adapt to positive and negative outcomes creates an opportunity to realise how people react during a threat and how the decision-making process functions under those conditions. The idea is not to put the blame on who did what wrong but learn from how the situation unfolded to attain healthy development (informant 522) in a trusting environment. Furthermore, as discussed by informant 147, resilience within cyber security is not unique from other areas where resilience is beneficial. Similarly, based on reflections made by a Senior Leader, it would be beneficial to view cyber resilience and cyber security from a larger business perspective, as both elements are an essential part of the complex system. Implementing resilience procedures or fostering a resilient mindset in a minor part of a complex system, the effects will expand into other areas. Interestingly, it might be time to strive away from the rigid frames within security, as stated by informant 813, "*Compliance does not foster resilience*," more on this in the discussion section.

Based on the reflections done in the interviews, most informants spoke about resilience concerning risk and security by using the illustrative method of the bowtie, a commonly used tool within those fields "*Prioritise resilience in all stages of the bow tie*" (informant 688) and "*The bow tie must work together to create resilience"* (informant 522). Suggesting that if a new concept should be implemented in a field that focuses security, presenting it in this format might be beneficial, similarly as found with risk—more about this in the discussion section.

5.3 Which elements enhance cyber resilience for a complex organisation in the energy sector?

To accurately answer the third research question, multiple forms of evidence are collected and analysed for descriptive purposes and comparisons. This section has been divided into two categories based on the information's origin.

Firstly, the experience, thoughts and knowledge of those working within the field of cyber security will be presented. This includes the interviewed practitioners, a Senior Leader and the expert informant. These perspectives will represent experiences on resilience enhancing measurements and implementing them into a complex organisation and scientific knowledge.

Secondly, an analysis of accessible and relevant frameworks on cyber resilience was performed, and a summary of key findings will follow.

These data will serve as the key findings for the discussion section, where the answers will be compared to critical concepts such as risk and cyber security, the theory of resilience engineering and other findings presented in the literature review.

5.3.1 Perspectives from Representatives from Complex Organizations and Experts

Between the thirteen interviews conducted with people working within a complex organisation in the energy sector, various measures and implications were proposed. Those interviewed have experience in leadership positions, starting businesses from the ground up, and improving business culture, security, reputation, communication, practices and production. Their views are not necessarily related to their current employer as they were asked to draw from the totality of their experience and are not related to a specific company. The expert informant interviewed for this project is an expert in safety, security and resilience for organisations.

Before the findings can be presented, a critical consensus became apparent during the interviews that are relevant for understanding how a complex organisation can become resilient. A general theme among all interviewed was that many qualified people are usually employed with various expertise within a larger company in the energy sector. However, having an overview of all recourses to collect, combine and corporate people and skills into beneficial tradeoffs or collaborations can be challenging due to organisational complexity. Moreover, this might indicate that resources already lie within a complex organisation. However, a structural or organisational shift would be required to reach its potential. Referencing the second theory of understanding resilience described by the expert informant in the previous research question. A complex organisation already has impressive protective elements; if combined correctly, resilience is the natural result. Making it essential to investigate further which elements would be beneficial in reaching the goal of cyber resilience for a complex organisation.

Regarding the collected data, some measures were repeated by more than half of the representatives, and none were mentioned less than twice—some of the reflections naturally involved more than one element. However, for clarity, suggestions will be grouped as follows: define and standardise, experience exchange and training, the collaboration between units, and human factors and adaptive capacities. Lastly, less-mentioned but important suggestions are grouped at the end.

5.3.1.1 Define and Standardize

There was a consensus that a clear and understandable definition of cyber resilience would be valuable in understanding what it is and, in doing so, knowing how to enhance it (Informant 688, 954, 522, 318, 498, 149 and 632). This is not exclusive to a specific organisation but extends to the more significant sector. More than a few informants underline the importance of international guidelines and standards to ensure a shared understanding and reachable goals. The Security Act (Informant 954 and 522) was spoken of in favour as it opens for an extended collaboration and trust building between government agencies and the energy sector. This could lead to more knowledge, more robust protections, and a clearer understanding of the acceptance that the industry struggles with the same threats (Informant 522). International standards can serve as the groundwork for how the collective fight against cyber threats should entail. It was also suggested that standardized guidance could lead to an openness to sharing information and learning from other mistakes, mishaps or accidents to strengthen cyber resilience. Moreover, the next grouping of suggested measures can be seen as an extension of this factor.

5.3.1.2 Exchange of Experience and Training

As an extension of creating international definitions and guidelines, trust and opportunity for sharing experiences can occur. The main idea expressed throughout the interviews regarding learning from experiences was how companies facing the same issues should exchange experiences and learn from each other. However, the general consensus in the interviews was that even though complex organisations within the sector were facing the same challenges, the complexity of an organisation does not automatically mean that one company's experience can be copied and implemented for another company and result in the same cyber-resilient success. Basically, complex organisations can learn from other companies' attack and threat history but not necessarily apply the same measures to their business structure. "*Learn from their experience but remember your own context*" (Informant 239). Similar reflections can be found in the words of a Senior Leader; it is imperative to know your own business to succeed in improving and protecting it.

Further followed by the expert informant, there is nothing to be learned from other companies' "successes" if you are unaware of your practice and context. Practice, training, and tailoring to organisational needs, requirements, experiences and capabilities are of much higher value in enhancing cyber resilience (Expert Testimony). Moreover, it was mentioned that in combination with international standards, and collaborations with government agencies and similar businesses, there arises a natural need to share and work with other companies down the supply chain (Informant 876), which enhances the awareness of cyber resilience and the importance of enchaining cyber security in all stages, and to multiple companies. As a continued argument made by a Senior Leader, implementing resilience in any area of a complex organisation can spread it to other areas, regardless of how small. In this case, it could spread across the supply chain.

All but two interviews reflected on how necessary training was to raise awareness and enhance knowledge to strengthen an organisation's cyber resilience. Within a complex organisation, training could prepare people on how to foster resilient behaviours, make resilient-based decisions and establish a resilience-based mindset. As stated by informant 688, "*Training to enhance cyber resilience is vital, regardless of the cost*." Both awareness and scenario-based training were suggested in the interviews. Awareness training can be considered the first step to give the construct some attention within an organisation (informant 688), but the training must be taken further (Informants 239 & 954). "*How do you get skilled, experienced, and highly qualified yet, normal people to notice unexpected cyber threats?*" (Informant 239). Scenario training will allow the organisation to see how people react during a cyber threat (Informant 954) and to minimise (at least to some extent) the scary part of the unknown (Informant 762).

The point of training extends into human factors and adaptive capabilities, which will be discussed shortly.

5.3.1.3 Collaboration between Safety and Security, and between IT and OT

As an extension of sharing experiences is the importance of collaborations, nearly all interviews mentioned collaboration between the safety and security domains (Informant 688, 876, 318 & 149) and IT and OT (Informant 688, 875, 239 954, 762, 522, 318). As established in the literature review, there is a separation between the safety and security field, but as suggested by informant 318, "*even though the intent behind an attack varies, which is normally how the security and safety responsibility is separated, is there really a distinction between the two at its core? Both are protecting the organisation.*" A cyber-attack might be with malicious intent, making it a security issue, but the consequences (foreseen or not) can spill into safety operations. As stated by informant 149, the safety field has a strong history and has spent decades perfecting its procedures; why not let security into the secrets so they can adapt? Additionally, as underlined by the expert testimony, theories of resilience, such as resilience engineering, presented in the literature review, are based on safety principles, suggesting a need for collaboration or merging to enhance cyber resilience.

As a security problem can turn into a safety one, the identical inquiry was reflected in the interviews regarding a partnership between OT and IT. As stated by informant 954, operational mistakes can become technical and vice versa. Traditionally, OT and IT are separated to assign responsibility to separate areas within a business, with the intent of solid collaboration. During the interviews, it became clear that without any hostility or ill-intent, it was previously experienced during their work experience by a few that the collaboration between IT and OT did not always function in practice. Ether by lack of understanding regarding the other sections' expertise and prioritisation, values were arranged differently or simply a lack of common language between the two.

Importantly, it was suggested in multiple interviews that feeling responsible for more than the specific task can enhance understanding of the whole process within the larger organisation—creating the grounds to build cyber resilience within a complex organisation. Also, both sections must find a common language (informant 318), where they can share expectations (informant 762), needs, and limitations to their area, so set realistic prospects and fill in the gaps between them (informant 149). More distinctly, building trust between IT and OT (informant 522) could be done by rendering the difference between the two harmless.

As described by a Senior Leader, a cyber threat is never an isolated "IT problem." The difference between the branches is intended to benefit each other to solve problems and strengthen business resilience and security. This is not limited to OT and IT but includes different expertise departments. Knowledge of the system and capabilities outside of what one is personally responsible for can allow for expanding resources and solutions within which limits and boundaries. The expert testimony supports this statement: OT and IT must have genuine collaborations to enhance cyber resilience by creating a common language and an understanding, such as why program X must be used instead of program Y and why a program needs to be able to perform procedure Z even though it decreases the effectiveness of the technical processes—balancing the importance of knowing how and why a program works is challenging but beneficial.

5.3.1.4 Human Factors & Adaptive Capabilities

As already established, training the resources of human behaviour and activity is essential. Informant 147 mentioned that it is critical to understand what lies behind making a decision when faced with a new cyber threat and how adaptive capabilities could be used for their benefit. Importantly, as mentioned by informant 632, a vital part of training would be to mentally prepare people for how they might feel and act in an unexpected situation. Because being adaptable might be people's most vigorous defence (informant 954), but it could also be an organisation's most vital line of defence (informant 498). As underlined by a Senior Leader, adaptability can allow the organisation to see how its complexity is connected.

Further, the Senior Leader reflected that "resilience is not limited to a system, an organisation or the technology employed." The main element of an organisation's capacities lies in human actions. Teaching and allowing the time, resources and space to adapt and cope can massively enhance an organisation's cyber resilience defence (Interview, Senior Leader). An adaptive organisation can create an openness (informant 239) towards reporting accidents and mishaps (informant 239), which is continuous to adaptive behaviours—resulting in a security culture without shame or blame (informant 522 & 498), which leads to an environment that fosters adaptability through openness and trust by establishing good security culture within the complex organisation. As underlined by the expert informant, people are an essential resource. At its core, resilience is about people who are alert and present to see what technology is not yet designed to see. Human factors and adaptive capabilities can be seen in the light of the expert’s testimony’s third explanation for how resilience is built in complex organisations; some people "get" it by implementing a resilient mindset. This will be further discussed in the discussion section.

5.3.1.5 Other Resilience Enhancing Factors

Other measures reflected in the interviews by two or more informants were lessons on crisis communication (informant 688) and communication strategies in general (informants 147 & 149). It was mentioned that to prioritise cyber resilience across a complex origination; it must come from the top. Management has to lead by example by setting expectations and requirements and being open to suggestions as to how this can be implemented and, in doing so, create a safe and adaptable work environment (informant 239 & 149). This was also a point in the reflections done by a Senior Leader; management has to incorporate a resilient focus across the organisation. Supported by reflections done by the expert testimony, people are a great resource, but management has to be interested in learning, implementing, teaching and allowing for resilience change. Significantly, things rarely go according to plan, which requires a system that can adapt to unexpected changes on the fly—enhancing the importance of having a resilient mindset from the top down within a complex organisation.

Another factor mentioned was having one person responsible for seeing the larger scale within the organisation. As established, any change within a complex organisation will be challenging, and people could sit on skills and information that would be hugely beneficial for someone else, but both are unaware of it. Having a person starting to untangle the web of competence, skills and working areas (informant 762) would be beneficial towards building cyber resilience as collaborations, information sharing and responsibility is gathered in one place (informant 138 & 954). The expert informant expresses the complex, challenging element of an organisation as the natural tendency of such an organisation. Relationships and structures naturally originate within this complexity. The system adapts to changes, and going backwards is impossible; only adapting to the new normal is an option. This indicated the need for interest and curiosity, not only about how an organisation is changing but about how the following change can occur unexpectedly.

Both management and front-line workers within cyber security must be interested in how changes from cyber threats X, Y and Z will have a consequence on the organisation as a whole and how to best prepare for being adaptable enough to deal with it. Basically, it is vital not to sit back and be happy with a functioning system but to continue improving it for anything actively (Expert testimony). Collaborations and regular knowledge exchange with those working within academia were also reflected on as e measures to enhance cyber resilience by a Senior Leader. Constantly being aware of new knowledge can create an understanding allowing for correct implications for a complex organisation.

5.3.2 Components Identified in Frameworks

This section includes the findings from document analysis of scientific frameworks intended to strengthen cyber resilience, and key findings will be presented. Each framework will be introduced shortly, with its main elements included. Other than the given name of a framework's categories or phases, all other information presented is reconstructed. After that, a short overview of the essence of resilience-building measures in the given framework follows. The findings from this analysis will be compared to the interviews, expert testimony, and literature review, already presented to identify resilience-enhancing elements to assist in answering the third research question in the discussion section.

A framework is a scientific guide on how to achieve something structurally. If a particular need of a complex organisation can be identified, a tailored and specific design can be implemented to achieve the wanted outcome through a framework (Shahzad et al., 2022). Currently, there are various assessment tools to measure and implement cyber resilience. They vary from having a simple index to a tick-off too explicitly tailored towards a business (Linkov & Kott, 2018). Though the goal of this master thesis is not to match a specific framework to a specific company's structure, there is value in establishing cyber resilience strengthening aspects that could, in turn, be implemented for the given purpose. Suggestions such as "have a solid IT department" and "change passwords regularly" are common knowledge for complex organisations and will not be presented in this study. The idea is to go beyond the statement "be resilient" and analyse which elements within every framework reach that goal. For example, a statement that often came up in this process: "an adaptable mindset will enhance cyber resilience within an organisation," without any suggestion on how this adaptable mindset can be achieved. A general statement without any advice on achieving it does not meet the standard of holding any value in suggesting cyber resilient enhancing measures.

Some of the included frameworks hold the primary function of being assessment tools. However, analysing what would indicate high scores makes it possible to conclude what is considered cyber resilience-enhancing measures. Notably, some frameworks have restrictive access, but still, enough information is publicised to draw importance. With this in mind, the principal elements and substances have been withdrawn from the chosen framework to identify cyber resilience strengthening factors.

The main findings from the seven frameworks will be presented:

1. Consequence-Driven Cyber-Informed Engineering (CCE)
2. Conceptual Framework for Developing Resilience Metrix for the Electricity, Oil and Gas Sector in The United States.
3. Cyber Resiliency Engineering Framework (CREF)
4. National Institute of Standards and Technology, Cyber Security Framework (NIST)
5. World Economic Forum Board Principles Playbook for Oil and Gas

6. Cyber Resilience Scotland: Strategic Framework
7. Resilience Management Model (CERT-RMM)

5.3.2.1 Consequence- Driven Cyber-Informed Engineering (CEE)

The CCE was developed by the Idaho National Laboratory, requested by the U.S. Department of Energy in 2020. The main goal of the framework is to protect critical infrastructure from attacks originating from cyberspace. The CCE consist of four active stages, with the fourth being based on the principles from the NIST framework and developed from the five elements: identify, protect, detect, respond and recover, but separate words and categories have been created within the framework as will be presented in the fourth phase.

The framework is divided into four phases with included focus (in short):

Phase 1 – Consequence Prioritisation: An organisation should clearly define and categorise its limits. Categories cyber threats that would damage the organisation's operations, paired with training scenarios.

Phase 2 – System-of-Systems Analysis: The organisation would create an overview of its system, processes, procedures, and supply chain.

Phase 3 – Consequence-Based Targeting: This stage includes identifying and targeting how an unknown entity would attack and the consequences.

Phase 4 – Mitigation and Protections: Remove the cyber pathways that can give someone access to the organisation. If it is not possible, put in more barriers and reporting systems, the four functions that the CCE wants to achieve in this phase are to protect (remove cyber threat), detect (notice in time), respond (contain hostile opponents), and recover (restore function).

To summarise, within these four phases, the CCE states that cyber resiliency can be enhanced by making cyber resilience a part of security culture, allowing external personnel to create scenarios and assessments to ensure new perspectives, and having management be in charge of deciding, implementing and allocating resources tailored to organisational needs through all stages from the NIST framework.

5.3.2.2 Conceptual Framework For Developing Resilience Metrix for the Electricity, Oil and Gas Sector

The Conceptual Framework for Developing Resilience Matrix for the Electricity, Oil and Gas Sector was constructed for the Energy Policy and Systems Analysis office as part of the U.S. Department of Energy and Defence in 2014. The matrix is rooted in a risk-based mindset, where the understanding of risk is extended to the resilient metrics "probability of consequence, given threat." With the focus on risk, there is substantial importance put on the uncertainty element present in any given threat.

The metrics are meant to be used within the decision-making process. This includes when a system is in its planning stage to when it is in shape to perform operations and tasks. Before implementing the matrix, the organisation must establish a "baseline" of the current situation through a cyber resilience assessment tool. The baseline will allow for exploring areas for improvement and comparative purposes when new adjustments are added to the organisation's resilience building. The results of this baseline will make up the individual company's metrics. The baseline evaluation should include defining and characterising elements such as resiliency goals, the system, threats, disruption level and consequences. This assessment tool used is the Resilience Analysis Process (RAP).

Essential elements that are valued for building cyber resilience are introduced in these seven stages:

1. Define resilience goals: How does the organisation value resilience?

2. Define System & Resilience Metrics: limits, time restrictions, types of consequences

3. Characterise Treats: indicate what the system must absorb; likelihood and capabilities are essential elements.

4. Determine Level of Disruption: scope of damage from threats.

5. Define and Apply System Models: all outcomes from damage to possible domino effect between units.

6. Calculate Consequences: more immense consequences of being unable to distribute energy (societal function, international agreements etc.)

7. Evaluate Resilience Improvements: Modifications can be done to improve resilience.

Moreover, the analysis found that it is recommended to include other stakeholders in the discussion process to get perspectives from multiple points of view and ensure that the whole supply chain is included. To summarise the Conceptual Resilience Matrix, the organisation must analyse current systems to find a baseline for insight and further evaluations. Organisational traits and structures must be understood in addition to resilience, threats and consequences.

5.3.2.3 Cyber Resiliency Engineering Framework (CREF)

The Cyber Resiliency Engineering Framework is created by the research company MITRE. In later years, the CREF has been updated to align with the core elements of the NIST framework. The core value of CREF has not changed; it only updated categorization to match international guidelines better. CREF is based on the four stages: **Anticipate** (alertness to attacks), **Withstand** (continue production despite an attack), **Recover** (revitalize functions after an attack), and **Evolve** (Improve after an attack) to enhance cyber resilience, from the theory of resilience engineering.

Within these stages, CREP has established eight objectives:

1. **Understand**: functions, the business, dependencies, cyber resources, and conditions.
2. **Prepare:** for a cyber-attack by employing all resources and training.
3. **Prevent:** creating barriers to the most damaging or less effective measures to stop when attacked.
4. **Continue:** operations by having them performed by others or on other platforms if one is attacked.
5. **Constrain:** by keeping cyber recourses isolated.
6. **Reconstitute**: by allowing for attacks in an area that is backed up, with no harm to production.
7. **Transform**: by changing how things are done.
8. **Re-architect**: by changing resilience methods after an attack with new knowledge from experience.

To summarise, the core idea of CREF is that resilience is not something that happens; it has to be acquired, tailored and nurtured (or engineered, hence the name). Generally, the thought behind the process is that a complex organisation is interconnected. By improving cyber resilience, a more substantial arsenal of cyber resources will follow, which can improve management and enhance how an organisation deals with accountability. The CREF is three disciplines combined in one: resilience engineering, resilience management (risk-based) and cyber security focused, which means that the core focus is not on identifying and targeting what would make a system crash but keep the focus on how it can be dealt with when it happens. Additional cyber resilient enhancing measures in the CREF include the belief that adaptive human behaviour is necessary to be resilient and coordinate between those involved in cyber defence.

5.3.2.4 National Institute of Standards and Technology, Cyber Security Framework (NIST)

The National Institute of Standards and Technology (NIST) established the Cyber Security Framework in 2004, which was meant to assist organisations in identifying, assessing and managing cyber risk. The framework has been heavily updated since then and is one of the most referred-to structures within resilience-building frameworks. The NIST Framework aims to strengthen cyber security in general but emphasises that solid risk management should improve security and resilience. The core idea is that traditional risk management can be strengthened by focusing on developing elements of security and resilience.

Though this is a cyber security framework, as the core functions are used as the basis for others, it is deemed valuable. NIST consists of five core functions:

1. **Identify** – The organisation must create a shared understanding of how they want to handle cyber risk to functions, systems, production, people and capabilities. This is done by getting an overview of how the system functions, what resources are available, critical functions, needs and strategies.
2. **Protect** – Create barriers that allow for a continuance of delivery of services. Keep cyber threats away from necessary productions and systems by protective measures, information and awareness sharing and training.
3. **Detect** – Have measures that detect cyber threats through monitoring.

4. **Respond** – Actions to implement when a cyber threat is identified by having prepared responses, clear communications and pre-made mitigations.
5. **Recover** – Be a resilient organisation by planning to recover what was stopped due to the cyber threat.

To summarise, the NIST framework suggests that an organisation can establish resilience through how it manages to recover. Other than that, solid cyber security measures will result in resilience.

5.3.2.5 World Economic Forum, Cyber Resilience for the Oil and Gas Industry

This section is based on two documents from the World Economic Forum because they are seen as an extension of each other. The first paper, "Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers," from 2021, can be considered the groundwork that further inspired the creation of a Cyber Resilience Framework presented in "The Cyber Resilience Index: Advancing Organisational Cyber Resilience" from 2022. Both documents include measures to reduce cyber risk by focusing on cyber resilience within the energy sector. These initiatives also resulted in the Cyber Pledge mentioned in the context section earlier in this project, making it very relevant for this master's thesis.

I. **Cyber Resilience Enhancing Measures found in "Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers**"

The World Economic Board Principle Playbook for Oil and Gas results from indebt and honest discussions between more than 40 representatives from senior management in the energy industry to share experience, knowledge and expertise.

The measures identified by The World Economic Forum are based on the notion that companies within the energy sector as extremely complex in business diversity, location of personnel and operatives and with a diverse group of suppliers and customers. Based on this, six energy- sector specific principles have been suggested.

1. Cyber Resilience Governance - This includes a collaboration between all departments: OT, IT, Security, Physical Safety etc. The business has to evaluate which measures have been put in place to ensure trust and collaboration between the department. Furthermore, cyber resilience's definition and principles must be functional and understandable across these departments.

2. Resilience by Design – Security and resilience by design are promoted. Cyber resilience should be embedded into existing structures regarding cyber risk, and the development continently evaluated.

3. Corporate Responsibility for Cyber Resilience – Evaluate how cyber risks are introduced and affect the organisation. Cyberculture and practices should be examined—a collaboration with those affected.

4. Holistic Risk-Management Approach – Cyber risk should be a priority across the originations. Sufficient resources and training should be provided. Evaluate how the whole supply chain can supply cyber risks that might be unknown.

5. Ecosystem-wide collaboration – Management should entrust and nurture collaboration across the organisation.

6. Ecosystem-wide cyber-resilience plans – From the top down, cyber resilience action plans should be created, tested and evaluated. All elements of the organisations should be included.

Furthermore, the Cyber Resilience Playbook suggests that giving authority to individuals to act as cyber resilience officers and tailoring awareness programs to individual units can enhance cyber resilience. Also, scenario training and honest assessments of the business's maturity will be beneficial.

II. Cyber Resilience Enhancing Measures found in "The Cyber Resilience Index: Advancing Organisational Cyber Resilience"

World Economic Forum created the Cyber Resilience Framework (CRF) and Cyber Resilience Index (CRI) in 2022. The tools were meant to allow for the specific origination to create organisational resilience by being aware of how to achieve cyber resilience best. The idea is that it will lead to holistic resilience across the organisation. The framework's methodology is based on experiences and expertise from cyber management, the academic landscape and international standards and frameworks. The goal of the CRF is to serve as a supplement to existing cyber resilience frameworks.

The CRF is divided into six stages paired with relevant actions.

Principle 1: Regularly Assess and Prioritise Cyber Risk.

- Involve the whole "ecosystem" of an organisation when understanding cyber risk
- Those responsible for cyber resilience shall be heard by those making decisions
- Cyber resilience is decided by a risk

Principle 2: Establish and Maintain Core Security Fundaments

- Implement and measure practices against international standards such as NIST, IOS etc.,
- Annually evaluate cyber resilience action plans and initiatives and make improvements

Principle 3: Incorporate Cyber-Resilience Governance into Business Strategy

- Cyber resilience should be holistic for the company
- Cyber Resilience strategies should come from top-down
- Cyber Resilience officers

Principle 4: Encourage Systemic Resilience and Collaboration

- Understanding the complexity of organisations
- Create a collaboration culture with trust, transparency and accountability
- Collaborate with other companies, sectors and agencies

Principle 5: Ensure Design Supports Cyber Resilience

- Processes and operations must be understood and be applicable between OT, IT and other business units
- Resilience testing performed annually (also in collaboration with third parties)

Principle 6: Cultivate a Culture of Resilience

- Cyber resilience training for all employees
- Cyber resilience prioritised by leadership

To summarise, both works from the World Economic Forum suggest that cyber resilience can be enhanced by continue integrating OT and IT, by having management prioritise cyber risk and resilience and by implementing international standards (ISO 27000 or NIST). Prioritising and valuing cyber resilience will enhance awareness, creating small changes that will spread through the organisation.

5.3.2.6 The Strategic Framework for a Cyber Resilient Scotland

The Strategic Framework for a Cyber Resilient Scotland was developed to ensure operational resilience and business continuity by underlining that cyber threats were not an IT-isolated issue but something everyone is responsible for and affected by. The idea behind the framework is that it can be implemented by larger complex businesses and regular people to create awareness and preparation. Though, at first, it might seem that an approach to cyber resilience that takes such a broad approach might not be relevant to complex originations needing to work within international standards and by measurable operation. However, evaluating the general principles of how cyber resilience can be built can indicate broader understandings that might be missing in the stricter frameworks.

The general principles of this framework are a). knowledge and awareness of risk and threat, b.) access to guidance, tools and resources, c). understanding policy and processes, d). learning and skills, e). effective incident management, response and recovery processes.

Generally, the framework underlines that if both businesses and people can recognize a cyber threat, the first step towards managing the risk is achieved, and resilience can develop. An awareness culture has started. This can be achieved by tailoring campaigns towards the individual needs of people, groups and organisations. The aim is that cyber-resilient behaviours will develop across all levels. Then, making reporting easy and safe by creating trust between that reporting and those recording. Regular testing and reviewing must occur after establishing healthy cyber-resilient attitudes and habits. Lastly, open lines of communication towards those affected or involved in a cyber incident to learn, cope and adapt.

To summarise, Cyber Resilience Scotland suggests that awareness and understanding of cyber resilience in all areas is essential and can be accomplished by sharing information, defences and creating trust.

5.3.2.7 Resilience Management Model (CERT-RMM)

The Resilience Management Model (CERT-RMM) is meant to assist in creating operational resilience management by putting it into organisational practice. The CERT-RMM can be used as an assessment tool to guide organisational improvements further to enhance cyber resilience. Notably, the CERT-RMM is establishing resilience within management rather than cyber security. Nevertheless, as with other frameworks, it is beneficial to look for resilience-enhancing factors in various areas to see if there is knowledge that could be implemented into the field of cyber resilience. Moreover, management can be highly complex, just like an organisation. Suggesting that common tendencies can be seen between them.

The model is highly complex, 860 pages long, and includes 26 cyber-enhancing categories. To summarise, the CERT-RMM suggests that resilience in complex organisations is achieved when genuine involvement and collaboration between those operating and monitoring security, information, and data with those responsible for technical support. Also, knowing the organisation's assets and values will establish what needs protection. This can again lead to responsibility and authority for people to act. This can be ensured by focusing on training and learning, where everyone in the value chain is included through clear communication. Lastly, having a baseline is essential.

6. Discission

In this chapter, the findings from the interviews and document analysis from chapter five will be discussed and compared to the literature review included in the third chapter. The discussion will be organised by the research questions, focusing on one question at a time. Importantly, naturally, the discussion of the research question blends, meaning that they should all be seen as an extension of each other.

The first research question focuses on understanding cyber resilience within a complex organisation in the energy sector. Statements from the interviews and resilience-enhancing elements discovered by the document analysis will be compared. Relevant theory from the literature review will be incorporated where it is relevant. The previous chapter organised the findings into three groupings of how cyber resilience was understood: more than "motstandsyktighet," a new form of security and adaptive capabilities. In this chapter, the discussion will be structured similarly, yet differently, to ensure proper arguments flow. Importantly, all findings indicate the need for clear directives from the more extensive authority on how cyber resilience should be understood and worked with. In the discussion on how this can best be accomplished, two more significant categories have been found to need (1) a clear definition and (2) official standards and guides. The two sections spill into each other, as they are similar, meaning that both should be seen as an extension of each other.

The second research question evaluates if understanding risk and security influences how cyber resilience is understood by analysing reflections from the interviews and aspects identified in the framework. Generally, understanding risk and security influences understanding cyber security, offering an additional layer to risk management and cyber security by extending its capabilities and goals. Consequently, cyber resilience can be seen as taking it further than risk management and cyber security practices.

The third research question intends to establish measures that can enhance cyber resilience within a complex organisation by comparing the experiences and perspectives of practitioners and experts to suggestions found in the analysed frameworks. Theories and findings from the literature review are also an addition to answering the third research question. The discussion will be structured similarly to the findings; however, there will not be a separation based on the source of information. Separate groupings of cyber resilience enhancing elements will include (1) defining and standardising, (2) exchange of expertise and training, (3) internal collaboration and (4) human factors and adaptability, as grouped in the findings chapter. Additionally, the importance of understanding organisational properties will be included.

6.1 Understanding Cyber Resilience in the Energy Sector: Key Requirements

Based on all the presented theories and findings in this master thesis, it is necessary to implement directives from more extensive authorities to assist in the understanding of cyber resilience for complex organisations in the energy sector. This will further explain how cyber resilience can be enhanced for the given sector. Directives from the more extensive authority must include a clear official definition and standards and guides.

6.1.1 Clear Official Definition

To understand how the Norwegian Energy Sector understands the concept of cyber resilience, it is crucial to draw attention to an essential element lacking for the sector to accomplish this: a clear definition to work from. Though the Norwegian Energy division collaborates with the more significant international oil, gas and energy sector, making them reliable for following international standards and pledges commonly accepted, there is no official definition or reflection of cyber resilience from the Norwegian Petroleum Authority or the Norwegian government. Moreover, there are no official incentives or recommendations for how these companies can start implementing changes to their corporations to achieve cyber resilience.

This trend became apparent in interviews with those working within the Norwegian energy sector. There is a lack of official definitions, reflections and expectations to indicate how cyber resilience should be valued or worked with. Notably, the lack of information and direction is from a higher perspective than the management of specific energy companies. The need lies with the Norwegian government, Ministries and Petroleum Authorities before it can be expected to be implemented by boards or management within specific companies. Cyber resilience must be understood collectively as a precise point in multiple frameworks (WEF, 2022; CREF;

Hollnagel, 2010; Linkov & Kott, 2018). It became apparent during the interviews that all but one informant reflected on resilience and expressed a necessity and want for the construct, even as needed by the industry.

However, the expressed need, commonly in the interviews, for a clear understanding of the construct and the tools for strengthening it was unclear, mainly because there was a lack of knowing where to draw information from. This was also apparent in the interview with the outlier, who showed little interest in cyber resilience. The scepticism came from a lack of understanding and available information, which meant that the person did not know if resilience was needed or if the more traditional elements of risk management and cyber security were "enough" for an organisation to focus on. All these reflections indicated organisations and experts that are matured further than the more significant sector, and the need for a clear definition of cyber resilience is a much-needed and welcomed improvement.

This is illustrated by comparing the responses when the informants were asked how they understood risk. Risk is a clearly defined concept by highly relevant scholars (Aven, 2010; 2012) and The Norwegian Petroleum Authority (n.d). A clear understanding of what risk is and how it should be understood exists for individual companies to draw their understandings and definitions. Everyone interviewed described risk in the same way. This indicates that if a clear and direct definition is given, it will be considered seriously as to how it could form risk management and risk assessment within the given organisation. Because most cyber resilience frameworks are risk-based in nature (Resilience Matrix; CREF; WEF; Cyber Resilience Scotland), this should only strengthen the benefit of this comparison. This will be further discussed in the section regarding the second and third research questions.

Also, as most interviewed are highly skilled in risk management, risk assessment and security, the bow tie method was a symbolic tool most used when reflecting on cyber resilience. Suggesting that introducing cyber resilience into an existing assessment could be beneficial to connect cyber resilience to existing understandings of security and risk. This is also one of the main points in the suggestions done by the World Economic Forum (2021; 2022). By implementing cyber resilience into existing practises, the organisation connects the dots that are already there. It makes the transition more accessible; they can tailor it based on the official definitions.

A framework that most other cyber resilience building framework has taken inspiration from is the NIST Cyber Security Framework. The NIST is one of the frameworks that most corporations are encouraged to follow internationally. However, the definition of resilience stated by NIST contradicts the substance that most relevant scholars have stated.

In the fifth and last stage of the NIST Framework, resilience is mentioned as a part of the stage recovery "Be resilient (…) by planning to recover what was stopped due to cyber threat" (NIST). That definition more accurately defines the properties connected with robustness. When a system has to pause or stop (Hollnagel, 2016a) production to endure the threat if a system is truly resilient, it can continue thriving while under attack (Linkov & Kott, 2018). This has been apparent in the literature review on resilience and in statements from informants that resilience is meant to operate despite an attack (CREF; Conklin et al., 2017; Anholt & Boersma, 2018; Rankin et al., 2013). The literature review states that robustness has been described as a property of resilience (Woods, 2015). This trend was also seen in the interviews with employees. The "robustness" arose in the resilience reflections but was always thrown aside for better descriptive words.

Luckily, most frameworks that take inspiration from the NIST framework do so to have a starting line within cyber security—indicating that the substance in other relevant frameworks arising from NIST can contain elements much more suited for the energy sector. Both the CREF Framework and the playbook from World Economic Forum underline that for cyber resilience to be effective, the system must be able to do better than "waiting out" the cyber threat. Interestingly, this suggests that the Norwegian energy sector might have to look further into other frameworks more focused on a cyber-resilient mindset rather than cyber security thinking. Moreover, it still can since it seems the extended sector has not yet reached the stage of creating (or adapting) an official definition or suggested framework, for that matter. An adequate framework will be suggested in discussing the third research question.

A clear definition from authorises is required for the energy sector to implement cyber resilience into their complex organisation.

6.1.2 Standards and Guides

As established, cyber threats towards the energy sector are expected (DSB, 2019; PST, 2022; Conklin et al., 2017). Further acknowledged by the Security Act, the law intends to "prevent, uncover and protect against security threats" (NSM, 2020), especially concerning international collaborations. The inclusion of the energy sector in the law was intended to give the sector a wanted requirement to align according to international standards (Ministry of Defense, 2017). Commonly, international energy companies usually are subjected to follow the ISO/IEC 2700 Standards, advice from the European Commission (NIS2), The NIST Cyber Security Framework and the Cyber Resilience Pledge created by the World Economic Forum.

The Norwegian Government has suggested the inclusion of NIS2; however, for the time being, only the content of the Security Act is a requirement for operations for the Norwegian Sector, which publicly states nothing about resilience. The suggested inclusion of the European Commission's "Network and Information System Directive" (NIS2) as a requirement for the energy sector (Gjessing, 2023) will be evaluated in the discussion of the third research question. Nevertheless, some more applicable frameworks or directives could supplement the Norwegian Energy sector on the need for official standards and guides.

As established in the empirical findings, cyber resilience was described in general as (i) more than withstanding an attack, (ii) a new form of security, (iii) and adaptive capabilities. These reflections are accurate representations of cyber resilience. This is an essential part of the reflections on cyber resilience done by Galmec and Steingartner (2017) and Anhold and Boersma (2018); resilience is more complex than security, and resilience is the ability to be adaptable (Expert Interview). As suggested by a Senior Leader, resilience has to be seen as a larger perspective and not limited to cyber, but rather as business resilience. Hinting at elements found in cyber resilient frameworks such as the Strategic Framework for Cyber Resilience Scotland, the Resilience Index from WEF and the CERT-RMM, further suggesting that there are more relevant frameworks that better align with the maturity of the energy sector. This can also indicate a resilience mindset, which will be further discussed in the third research question in combination with reflections from the expert testimony regarding understanding how complex organisations can attain cyber resilience.

Another essential element to draw attention to in exploring how the energy sector understands cyber resilience compared to the current development in Norway is how deep the construct is implemented into the nature of cyber protective measures. The Cyber Resilience Index created by the World Economic Forum comprises experiences and expertise inside and outside the fields and positions of board members, management, cyber, security, academia, and other experts. Cyber Resilience was in 2022 (year of publication), so clearly an imbraided construct in the industry that it was defined in the margin on the summary page; no more discussions or introductions of explanations were needed. In one of the interviews, it was reflected on how impressive it was to listen to academics hold discussions in their fields, where every construct was so well understood and established within the discipline that nothing was explained. The term was said, and everyone understood its implications. Cyber resilience is as well understood globally in the energy sector by adapting standards and guides.

The interview with a Senior Leader clearly expressed interest, curiosity, and an awareness of its importance, to implement and integrate cyber resilience into the business as a larger concept than just connected to cyber. However, this relies on a standard and a guide to develop. The expressed wish to be further educated and instructed on cyber resilience, occurring in most interviews, is another indication that some energy companies might have matured beyond the constitutions that regulate them. To conclude, all interviewed attempted but struggled to define cyber resilience because there is a lack of understanding to base it on concerning the field of cyber security.

It can be speculated that if the informants were asked how to be a resilient person, parent, or college, the responses might have been easier to reflect on. Regardless, reflections showed maturity beyond the more extensive field, and impressions from senior management are equally the same. A definition and suggestions on how it can be implemented and enhanced must be provided to the energy sector.

However, based on these findings, the energy sector might be perfect for creating the definition and suggesting standards.

6.2 Cyber Resilience: An Extension of Risk and Security

As expected, when interviewing people skilled and experienced within the fields of risk and security, a solid and clear understanding of the two fields is present. The substance of the interviews and the results of the reflections on how the constructs were in relation to each other will be presented and combined with the literature review. Supplements from the frameworks will also be presented. Naturally, reflections relevant to this research question also occur in the third research question, which prominently holds a more substantial relevance to the larger argument. Also, elements discussed in the first research question pertain to this section. To avoid repetition of findings, reflections from all research questions should be seen as an extension of another. Generally, cyber resilience can be seen as an extension of risk and security.

All informants had a similar and clear definition and understanding of "risk," suggesting that when a concept is strongly defined and valued within a complex organisation, people make it a part of their work life. Decisions are made with the concept in mind, and the construct is an active part of the decision process within work related to risk management and cyber security. As previously stated, all informants wanted a distinct and understandable official definition of cyber resilience, as with risk and cyber security. Supported by a statement made by a Senior Leader, correctly understanding a construct would be beneficial for understanding how to best implement it into existing complex systems, such as risk and security.

6.2.1 The Relationship between Risk and Resilience

During the interviews, it became clear that risk was more straightforward to divulge than resilience, but their relationship was relatively easy to reflect on. Most informants indicated that cyber resilience was a method of reducing, handling, working with or hindering risk. This aligns with what was stated in the literature review, and the risk is the threat, and resilience is the protection (Annarelli et al., 2020; Dupont, 2019). As the informants were asked if they believed it possible that a solid, strong, and robust cyber resilience mechanism could remove all risk, everyone answered no. The common consensus was that risk will always be present, as new ways, forms, methods, or implications can carry risk to an organisation. Also supported by

Bochman (2018) and the expert informant, the cyber domain makes a "risk-free" environment impossible.

This reflection further suggests a deeper understanding and correlation between resilience and risk, as by accepting that risk can always be presented (Panda & Bower, 2020) in unexpected threats, the "state" of resilience is fluid. As stated in multiple interviews, a resilient organisation is not a title to achieve; it is a state to fight to attain progressively. As could be said about a "risk-free" organisation, further strengthening the relationship between risk and resilience. Interestingly, this also indicates how adaptable cyber resilience defence has to be and how aware human cognitions are of this understanding, which will be discussed further in the third research question.

The separation between risk management and cyber resilience lies within the complexity of cyber systems (Panda & Bower, 2020), as theoretically, the end goal is the same, to protect against a threat. However, resilience does not necessarily want to "manage" a treat. The innate quality of a cyber-resilient system is that it is not affected by the cyber threat. Hence, no need for action. Importantly, as suggested by one of the expert informants, three origins of a resilient organisation, it was proposed that well-constructed and functional risk management combined with business continuity and preparedness would result in a strong defence, thereby reaching resilient standards. Risk management is a crucial element that must work correctly for this to be achieved.

Leading the way to another relevant similarity between how risk influences the understanding of cyber resilience, as most frameworks on enhancing cyber resilience originate from a risk-based mindset. The Resilience Matrix for the electricity, oil and gas sectors is rooted in risk management, where uncertainty is highly valued and prominent within resilience. Also, CREF states that implementing a risk-based mindset is one of the major elements of building a strong cyber resiliency through their measures. Also, NIST is firmly rooted in risk management. Most predominately within, The Cyber Resiliency Index created by WEF states that how cyber risk is understood, evaluated, and valued layers the whole groundwork for how cyber resilience can be built.

Cyber resilience is risk-based, suggesting that implementing measures to attain resilience could be effective and appropriate within a field where a risk mindset is predominant. Combining the understanding of a known construct, such as risk, can make the transition more assessable for practitioners within the sector. Furthermore, by adding the importance of cyber resilience to risk management, the construct is placed within an existing system already highly functioning by the industry.

Another essential correlation between risk and resilience that strengthens the connection between the two concepts is the importance of uncertainty. Within risk management, the elements of uncertainty are essential (Ptil, n.d; Aven, 2012; Engen et al., 2021; Strupczewski, 2021), which is also the case within resilience (Anholt & Boersma, 2018; Linkov & Palma-Oliveira, 2017). Furthermore, the individual influence of who is making decisions that is present in any decisions being within risk (Aven, 2012; Ptil, n.d); Sellvåg et al., 2020; NSM, 2023) or resilience as of human factors (Southwick et al., 2014; Diesch & Krcmar, 2018; Rankin et al., 2013). Suggesting a natural acceptance within the two concepts that align for similar processes.

Based on the results of this study, resilience is a natural and applicable extension of risk management that would strengthen and enrich the protective value of a complex organisation.

6.2.1 The Relationship between Security and Resilience

Predominately present in the interviews was the notion that cyber resilience and cyber security were concepts that worked together and were similar but held different properties. Clearly, both cyber security and cyber resilience aim to protect a system or an organisation from harm. What became apparent as one of the main differences between the two in the reflections was that security assumes that the presented measures might stop an attack. At the same time, resilience accepts that an attack will happen, regardless of what barriers are created. This is also found in Anhold and Boersma (2018); there is a clear shift in the possibility of attack from if (security) to when (resilience)—creating a difference in where efforts should be prioritised. Within security, the avoidance part is highly focused on in the preparation stage (Solms & Niekerks, 2013; CICA, 2021), while within resilience, adaptive capabilities are valued most (European Commission, 2012; Linkov & Palma-Oliveira, 2017). This shift in perception of how to think about protective measures can reflect the maturity within cyber resilience, seen as a growth from cyber security.

In terms of the understanding of security concerning resilience, an extension is necessary. As suggested by this research, cyber resilience might be the absolute goal of cyber security. This indicates that resilience adds essential elements to the already established protection within security. The idea that arises with resilience is that preparation involves more than withstanding (Hollnagel, 2014), as is the main objective of security. Referring to the distinction between resilience and robustness, a robust system will shut down until the danger is over (Hollnagel, 2014; 2016b); It would align with traditional cyber security thinking. As can be found in the previously mentioned use of the word resilience in the NIST framework, which predominately constructs cyber security. The definition used on resilience has been concluded in this paper not to be sufficient and only reaches the value attained to the quality of robustness. This is further evidence that a solid cyber security framework is necessary but that an additional framework for extending security till resilience is necessary. Cyber security is complex regardless due to the properties of cyberspace (Mbanaso & Dandaura, 2015; Sellvåg et al., 2020; NSM, 2023) and the complexity of an organisation (Galinec & Steingartner, 2017; Hausken, 2020) resilience is necessary to fill the gaps between the high rise of uncertainty and threats, with an additional layer of protection (Fernindand, 2016; Woods & Hollnagel, 2017).

Cyber resilience has the potential to raise the bar for traditional cyber security, to expect and want more from protective measures. Resilience is a continuance of security and risk management; by accepting that unexpected threats will arise for the energy sector (Conklin et al., 2017; NSM, 2023; PST, 2022), both security and risk can adopt an improved culture of adaptability and human factors necessary to meet the uncertainty of threats.

6.3 Cyber Resilience Enhancing Measures

Combining the findings from the literature review, all interviews, and the analysed framework, measures indented to enhance cyber resilience for complex organisations have been established. The findings will be presented in the four groups containing relevant suggestions on strengthening cyber resilience as stated in the findings, to ensure flow between the chapters: (2) defining and standardising, (3) exchange of expertise and training, (4) internal collaboration and (5) human factors and adaptability. Though the previous chapter has specifically pointed out relevant measures, this serves as extended conclusive remarks on the resilience-enhancing proposals. However, there is an additional inclusion to signalise the starting point that needs to be executed before the suggested measures can be implemented. Namely, (1) accurately understanding the uniqueness and individual factors of the specific complex organisation. This category will be presented first to lay the groundwork for other measures.

6.3.1 Understanding Organisational Properties

Notably, an in-depth understanding and knowledge of the relevant organisation's structure, values and functions (Hollnagel, 2010; Linkov & Kott, 2018; Diesch et al., 2018) are considered the minimum starting point for implementing strong resilience defence within a complex organisation. The CERT-RMM, Cyber Resilient Scottland, WEF, CREF, Resilience Metrix, and CCE recommend this. The challenges paired with being a complex organisation are also an element that supports the necessity of understanding own organisational properties (Huasken, 2020; Hollnagel, 2010). Interconnected departments with expert knowledge, individual responsibilities, and a larger supply chain (Linkov et al., 2019; Dooley, 2002) create a complex challenge requiring attention. Furthermore, establishing a baseline for where the organisation is currently concerning cyber resilience—is often done by an assessment tool such as the RAG (Hollnagel, 2015; Resilience Metrix; CERT-RMM). Creating a baseline will allow the organisation to evaluate their effectiveness and current successes or challenges of measures, in addition to having a result that can be compared for effectiveness after measures.

Staying aware that the complexity of such organisations can make it challenging to collaborate on compelling implications of change, it is essential to implement a security culture deemed safe by those working with the structure (CERT-RMM). This includes giving the proper authority to act (CERT-RMM) and a trusted environment to be allowed to get to know the reasoning for the relevant changes (Cyber Resilience Scotland).

Realising that different units within complex organisations require unique tailoring to how the addition of cyber resilience should be introduced and worked is important (Cyber Resilience Scotland). This reflects another challenging element with a complex organisation; knowing your workforce and the humans behind the actions is essential. (CERT-RMM; Cyber Resilience

Scotland). Sufficient allowance for authority and knowing the people included in the process can be challenging in a complex organisation. Nevertheless, as suggested by works analysed by The World Economic Forum, appointing cyber officers with specific responsibilities within smaller groups can be effective for the organisation. It allows people to attain individual knowledge of specific people in smaller groups and learn their qualities, needs and challenges. Breaking down the responsibility of tailoring the environment to be most productive and supportive in developing cyber resilience.

Furthermore, as a barrier against the complexity of an organisation when implementing cyber resilient measures, it makes the understanding of resilience attainable and relatable. According to the framework proposed by Resilience Scottland, CREF and the World Economic Forum, small changes can quickly spread, even across the complexity of an organisation in the energy sector. A slight difference in one department, group or even in an individual can successfully influence other aspects of the organisation. This supports the notion that having cyber officers be responsible for smaller groups within a unit can create the necessary environment for implementing cyber resilience and enhance the chances for positive change to spread across the organisation after successful adaptation within the smaller groups. As underlined by the expert informant, the unique qualities of a complex organisation are that connections and relationships are formed naturally. As an extension of making cyber resilience relatable, implementing the principles into already trusted and relatable structures, such as within safety and security or risk management (WEF, CEE). As solid correlations have been drawn with the practices of risk management and even cyber security, these can be considered excellent structures to further build in cyber resilience.

Relevantly, the addition of cyber resilience into a complex organisation must come from management. As stated by the Senior Leaders' experience, effective change is shown by trustworthy respect and value from management. Leading by example is essential for change to spread successfully across complex organisations (WEF, CCE).

6.3.2 Define and Standardise

A common understanding and definition of cyber resilience are fundamental for an organisation to implement (Glasdottir et al., 2016; Linkov & Knott, 2018). As illustrated by being a point of the highest importance by every analysed framework, there must be e collaborative definition of cyber resilience to measure, implement, and understand. As collaboration and a shared understanding are greatly important for this to happen, it is suggested that inspiration is found in tested, scientific, and peer-reviewed frameworks (Cyber Resilience Scotland). The Cyber Resilience Pledge suggested by The World Economic Forum and the combined Cyber Resilience Framework and Index are relevant, updated and clear standards the Norwegian Government or Petroleum Authorities could use to create a standard for the Norwegian Energy Sector to follow and develop from. With an official definition and framework, it can be implemented across organisations and the more significant sector (WEF, NIST). Another suggestion is to implement changes based on the ISO 27000 standards (Landax, 2021; ISO, 2023), as the goal is to foster a resilient mindset, and a resilient culture established can develop from adaptability, flexibility and human factors.

6.3.3 Exchange of Expertise and Training

Learning from others, sharing experiences and expertise, and continuous training are highly beneficial measures to enhance a complex organisation's cyber resilience. As established, sharing expertise is only beneficial if not directly copied into other organisations, as the transfer value does not function in that sense. It is necessary to know the uniqueness of each organisational structure and complexity, to evaluate whether lessons and knowledge hold valuable transfer value. If this is kept in mind, learning from others' experiences to strengthen cyber resilience benefits a complex organisation (CERT-RMM, CREF, CCE, Cyber Resilience Scotland).

Grøtan and von der Vorm (2016) state that training benefits a complex organisation. Three forms of training were highlighted by practitioners, experts and in frameworks: instinct training, awareness training and scenario training. Instinct training (Rankin et al., 2013) can be beneficial in pinpointing resilient individuals within an organisation or establishing resilience-enhancing behaviours to be fostered across the organisation. Awareness training can serve as a gentle reminder to refocus or sharpen the importance of resilience (Cyber Resilience Scotland, WEF), as the informants express as a successful tool. Scenario training, such as via the TORC, will take the specifics of a complex organisation and tailor relevant scenarios to those needs (Grøtan & van der Vorm, 2016). This is suggested as highly relevant in the CERT-RMM, The World Economic Forum, the CREF and the CCE. All are supported by the argument that resilience is a state an organisation must fight to foster; continuous training and exposure are needed. As suggested by principles from Resilience Engineering, such training can enhance a resilient mindset.

6.3.4 Internal Collaboration

Based on the real-life experience of the informants and suggestions found in cyber resilience enhancing strategies, internal collaborations are significant in building organisational resilience—mainly the successful collaboration between the safety and security domains and between IT and OT. As established, they have intended collaboration, but the division might be too strong for a successful relationship.

Those working within safety and security must work holistically (PTIL, 2023) for cyber resilience to be fostered within a complex organisation, similarly, for collaboration between those who work within OT and IT. Both internal collaborations face the same challenges. Indicating that what would work for Safety and Security is also valid for IT and OT. However, the different responsible areas dividing the two "opposites" make this complexity even stronger. As Resilience Engineering has a great impression on how a complex organisation can be resilient, it is essential to remember that those principles are based on safety (Hollnagel, 2016a). Also, the framework suggested by the World Economic Forum and the CERT-RMM strongly suggests a holistic collaboration between safety and security for successfully implementing cyber resilience within an organisation's complexity. Building trust and a common language between the two needs to be built, and extending where those working within feel responsible for what (WEF, Expert testimony), similarly with IT and IT (CERT-RMM, Cyber Resilience Scotland, WEF).

6.3.5 Human Factors and Adaptability

A flexible and adaptable work environment fosters a positive security culture (Rankin et al., 2013; Southwick et al., 2014; CEE), fostering a resilience-based mindset and behaviours. Based on reflections made by informants and their own experiences and observations, people are adaptable. They can cope with changes if there is a culture of trust within the organisation. This adaptability is strongly suggested as an influential human factor by Woods (2015). Seeing adaptable behaviour concerning how small changes can influence more extensive changes over time is relevant for cyber-resilient behaviour (Southwick et al., 2014). As it has been experienced that cyber threats rarely take the same path twice (Hollnagel, 2016b), adaptive behaviours are essential in resilience building. As illustrated by the latest pandemic, the employees of a complex organisation showed great adaptability to new and unexpected changes (Interview Senior Manager). Suggesting that resilience-prone thinking and behaviour are innate for people or that the complex organisation allows adaptation. Further supported by the fact that people usually know how to act in situations (Ranking et al., 2013; Hollnagel, 2009). This distinction is essential, as human behaviour is one of the most critical factors in building resilience for complex organisations (Widdeson, 2022; CREF).

The theory of resilience engineering is designed to cope with complexity (Woods & Hollnagel, 2017), making it highly relevant as a baseline for complex organisations. Within the theory, it is firmly believed that the optional function of an organisation is when those working within it can be adaptable to a flexible work environment (Hollnagel, 2016a). A clear and honest overview and understanding of own organisation is essential for this to happen. The principle of resilience engineering states that a system must be able to notice a change that can signalise a threat (Hollnagel, 2015). This requires alertness and curiosity that goes beyond security protocols. There must be freedom to individually tailor responses, suggesting adaptive behaviours and a flexible environment.

7. Conclusion

This master thesis aimed to explore the concept of cyber resilience to enhance understanding of the construct and to identify measures that could strengthen cyber resilience for a complex organisation in the energy sector.

It can be concluded that the first step is that those in the authority of the Norwegian Energy Sector must create and implement an official definition of cyber resilience and align the industry to an international standard such as the World Economic Forums, Conceptual Framework for Developing Resilience. With these steps, cyber resilience can be built within complex organisations.

Focusing on the complex properties of such an organisation results in a need to be aware of fostering cyber-resilient behaviours and mindset by creating a work environment that fosters trust, learning, and training. This can result in valuing and enhancing both personal and organisational qualities of adaptability and human factors.

To summarise, the more prominent categories that include resilience-enhancing measures for complex organisations are; understanding the qualities and uniqueness of an organisation, clear definitions and guidelines, trust and collaboration between internal units, contentions, learning and training—also understanding human and organisational capabilities through adaptability, human factors and flexibility.

8. Reference List

Allison, A., Chatzilia, A., Canham, D., Hillyer, M., Roberts, D., Seale, H., Willsher, M., & Williams, C. (2014). Cyber Risk Resources for Practitioners. The Institute of Risk Management (IRM).

Anholt, R., & Boersma, K. (2018). From security to resilience: New vistas for international responses to protracted crises. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of Cyber Resilient Systems. Computers & Industrial Engineering, 149. https://doi.org/10.1016/j.cie.2020.106829

Arghire, I. (2022, June 10). *38 tech leaders sign Cyber resilience pledge*. SecurityWeek. Cybersecurity news, insights and analysis. https://www.securityweek.com/38-tech-leaders-sign-cyber-resilience-pledge/

Aven, T. (2010). On how to define, understand and describe risk. Reliability Engineering & System Safety, 95(6), 623–631. https://doi.org/10.1016/j.ress.2010.01.011

Aven, T. (2012). The risk concept—historical and recent development trends. Reliability Engineering & System Safety, 99, 33–44. https://doi.org/10.1016/j.ress.2011.11.006

Bejarano, M. H., Rodriguez, R. J., & Merseguer, J. (2021). A vision for improving business continuity through cyber-resilience mechanisms and frameworks. 2021 16th Iberian Conference on Information Systems and Technologies (CISTI). https://doi.org/10.23919/cisti52073.2021.9476324

Bento, F., Garotti, L., & Mercado, M. P. (2021). Organizational resilience in the oil and gas industry: A scoping review. Safety Science, 133. https://doi.org/10.1016/j.ssci.2020.105036

Bertoni, V. B., Saurin, T. A., & Fogliatto, F. S. (2022). How to identify key players that contribute to resilient performance: A Social Network Analysis Perspective. *Safety Science*, *148*. https://doi.org/10.1016/j.ssci.2021.105648

Bochman, A. (2018). The End of Cybersecurity. Technology & Operations: Harvard Business Review

Bos, J. (2020). Confidentiality. In *Research Ethics for Students in the Social Sciences* (pp. 149–173). essay.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/qrj0902027

Brink, H. I. L. (1993). Validity and Reliability in Qualitative Research. *Society of a Nurse Researchers Workshop*.

Chamorro-Premuzic, T., & Lusk, D. (2017, August 16). The Dark Side of Resilience. Harvard Business Review. Retrieved March 13, 2023, from https://hbr.org/2017/08/the-dark-side-of-resilience

CISA. (2021, April 21). What is cybersecurity? Cybersecurity and Infrastructure Security Agency CISA. Retrieved April 23, 2023, from https://www.cisa.gov/news-events/news/what-cybersecurity

Coffelt, T. (2017). Confidentiality and anonymity of participants. *Iowa State University - Digital Repository*, *4*(1).

Conaty, F. (2021). Abduction as a methodological approach to Case Study Research in Management Accounting — an illustrative case. *Accounting, Finance & Governance Review*, *27*. https://doi.org/10.52399/001c.22171

Conklin, A. (2016). It vs. OT security: A Time to consider a change in CIA to include Resilienc. 49th Hawaii International Conference on System Sciences (HICSS), 2642–2646. https://doi.org/

Conklin, W. A., Shoemaker, D., & Kohnke, A. (2017). Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture. In Proceedings of the 12th International Conference on Cyber Warfare and Security(pp. 105–118). essay, Air Force Institute of Technology.

Cristofaro, M. (2017). Reducing biases of decision-making processes in complex organizations. *Management Research Review*, *40*(3), 270–291. https://doi.org/10.1108/mrr-03-2016-0054

Diesch, R., Pfaff, M., & Krcmar, H. (2018). Prerequisite to measure information security - a state of the Art Literature Review. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0006545602070215

Dickson, F., & Goodwin, P. (2020). Five Key Technologies for Enabling a Cyber-Resilience Framework. *International Data Corporation*.

Dooley, K. (2002), "Organizational Complexity,"International Encyclopedia of Business and Management, M. Warner (ed.), London: Thompson Learning, p. 5013-5022

DSB. (2019). Analysis of Crisis Scenarios 2019. *The Norwegian Directorate for Civil Protection*.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 5(1), 1–17. https://doi.org/10.1093/cybsec/tyz013

Eisenberg, D. A., Linkov, I., Park, J., Bates, M. E., Fox-Lent, C., & Seager, T. P. (2014). Resilience Metrics: Lessons from Military Doctrines. Solutions: For a Sustainable and Desirable Future, 5(5), 76–87.

Engen, O. A. H., Pettersen, A. G. K., Kruke, B. I., Lindøe, P. H., Olsen, K. H., & Olsen, O. E. (2021). Perspektiver på samfunnssikkerhet. Cappelen Damm.

Erickson, G. S. (2019). Chapter 2: Exploratory Reserch Design. In *New methods of market research and analysis* (pp. 27–50). essay, Edward Elgar Publishing.

European Commission. (2020, December 16). The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU. Migration and Home Affairs. Retrieved April 2, 2023, from https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en

European Commission. (2022, October 18). Critical Infrastructure: Commission accelerates work to build up European resilience. European Commission: Critical Infrastructure. Retrieved March 3, 2023, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

European Union. (2023). DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance). *European Parliament*.

Ferdinand, J. (2016). Building organizational cyber resilience: A strategic knowledge-based view of cyber security management. Journal of Business Continuity & Emergency Planning, 9(2), 185–195.

Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defence to achieve Cyber Resilience. 2017 IEEE 14th International Scientific Conference on Informatics. https://doi.org/10.1109/informatics.2017.8327227

Gaskell, A. (2021, September 28). *Cyberchology: How the human factor affects cybersecurity - cybernews*. CyberNews. https://cybernews.com/editorial/cyberchology-how-the-human-factor-affects-cybersecurity/

Gisladottir, M., Treasure, J., & Svavarsdottir, E. K. (2016). Effectiveness of therapeutic conversation intervention among caregivers of people with eating disorders: Quasi-experimental design. *Journal of Clinical Nursing*, *26*(5–6), 735–750. https://doi.org/10.1111/jocn.13412

Gjessing, M. (2023, May 5). *Vil endelig innføre NIS-direktivet*. Digi.no. https://www.digi.no/artikler/vil-endelig-innfore-nis-direktivet/530666

Golafshani, N. (2015). Understanding reliability and validity in qualitative research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2003.1870

Grøtan, T. O., & van der Vorm, J. (2016). Training for Operational Reislienece Capabilities. *Safera*.

Hafeez-Baig, A., Gururajan, R., & Chakraborty, S. (2016). Assuring reliability in qualitative studies: a health informatics persective. *20th Pacific Asia Conference on Information Systems*.

Hausken, K. (2020). Cyber Resilience in Firms, Organizations, and Societies. Internet of Things, 11. 10.1016/j.iot.2020.100204

Hollnagel, E. (2009) The Four Cornerstones of Resilience Engineering. In: Nemeth, C.P., Hollnagel, E. and Dekker, S.W.A., Eds., Resilience Engineering Perspectives, Volume 2: Preparation and Restoration, Ashgate, Surrey, 117-133.

Hollnagel, E. (2010). How Resilient Is Your Organisation? An Introduction to the Resilience Analysis Grid (RAG).

Hollnagel, E. (2013). A tale of two safeties. *Nuclear Safety and Simulation*, *4*(1).

Hollnagel, E. (2015). Introduction to the Resilience Analysis Grid (RAG) RAG – Resilience Analysis Grid.

Hollnagel, E. (2014). Resilience engineering and the built environment. Building Research and Information, 42(2), 221–228. https://doi.org/ 10.1080/09613218.2014.862607

Hollnagel, E. (2016a). Resilience Engineering. Erik Hollnagel Ph.D., Professor, Professor Emeritus. Retrieved February 1, 2023, from https://erikhollnagel.com/ideas/resilience-engineering.html

Hollnagel, E. (2016b). Resilience engineering: A new understanding of safety. *Journal of the Ergonomics Society of Korea*,*35*(3), 185–191. https://doi.org/10.5143/jesk.2016.35.3.185

Hovland, K. M., & Holmes, M. C. S. (2022, September 28). Equinor og Gassco lagt under Sikkerhetsloven: – naturlig at VI Skjerper Beredskapen. E24. https://e24.no/energi-og-klima/i/xg8Awn/equinor-og-gassco-lagt-under-sikkerhetsloven-naturlig-at-vi-skjerper-beredskapen

HSD. (2021). Implications of OT and IT Integration for Cyber Security. Security Delta. 10.1109/hicss.2016.331

ISO. (2022). Cybersecurity — Guidelines for Internet security. ISO/IEC DIS 27032.

ISO. (2023). How tech giants are building cyber resilience. The International Organization for Standardization .

Kagubare, I. (2022, May 25). Global oil and gas companies join Pledge for Cyber Resilience. The Hill. Retrieved March 29, 2023, from https://thehill.com/policy/3501324-global-oil-and-gas-companies-join-pledge-for-cyber-resilience/

Kleij, R. V. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In R. Leukfeldt (Ed.), *Advances in Intelligent Systems and Computing* (Vol. 960). Essay.

KPMG. (2018). Building Cyber Resilience In Asset Management. *The Investment Association*.

Landax. (2021, August 31). *Hva er ISMS?* Landax. https://landax.no/2021/08/30/hva-er-isms/

Lindkov, I., Baiardi, F., Florin, M.-V., Greer, S., Lambert, J. H., Pollock, M., Rickli, J.-M., Roslycky, L., Seager, T., Thorisson, H., & Trump, B. D. (2019). Applying Resilience to Hybrid Threats. IEEE Computer and Reliability Societies, 78–82.

Linkov, I., & Kott, A. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In Cyber resilience of systems and Networks. essay, Springer International Publishing.

Linkov, I., & Palma-Oliveira, J. (2017). Resilience and risk: Methods and application in environment, cyber and Social Domeins. In NATO Science for Peace and Security Series C: Environmental Security (NAPSC). essay, Springer. *Sciences*, *7*(4). https://doi.org/10.6007/ijarbss/v7-i4/2916

Macchi, L., Reiman, T., Pietikäinen, E., Oedewald, P., & Gotcheva, N. (2011). DISC model as a conceptual tool for engineeringorganisational resilience: Two case studies in nuclear and healthcare domains. *Proceedings of the Fourth Resilience Engineering Symposium*, 179–185. https://doi.org/10.4000/books.pressesmines.1049

Majid, M. A., Othman, M., Mohamad, S. F., Lim, S. A., & Yusof, A. (2017). Piloting for interviews in qualitative research: Operationalization and lessons learnt. *International Journal of Academic Research in Business and Social*

Maleh, Y. (2021). IT/OT convergence and cyber security. Computer Fraud & Security, 2021(12), 13–16. https://doi.org/10.1016/s1361-3723(21)00129-9

Mbanaso, U. M., & Dandaura, E. S. (2015). The Cyberspace: Redefining A New World. IOSR Journal of Computer Engineering, 17(3), 17–24.

Millum, J., & Bromwich, D. (2021). Informed consent: What must be disclosed and what must be understood? *The American Journal of Bioethics*, *21*(5), 46–58. https://doi.org/10.1080/15265161.2020.1863511

Ministry of Defence. (2017). Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven). Regjeringen.

Ministry of Petroleum and Energy, 2021. General Overview Navigation. Accessed 23. April, 2023. https://www.regjeringen.no/en/dep/oed/id750/ https://energifaktanorge.no/en/om-energisektoren/eierskap-i-kraftsektoren/

Moe, I., & Langved, Å. (2022, October 2). Viktig Sikkerhetslov kom for tre år siden. Først i juli I år ble Equinor Underlagt Loven. Aftenposten. https://www.aftenposten.no/norge/i/ve5eqV/loven-skulle-ta-nye-trusler-paa-alvor-foerst-etter-tre-og-et-halvt-aar-ble-oljebransjen-innlemmet

NIC. (2021). Global Trends 2040 - A more contested world. National Intelligence Council.

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, *2*(2), 175–220. https://doi.org/10.1037/1089-2680.2.2.175

NIST. (2023). Cybersecurity Framework. National Institute of Standards and Technologies

Norwegian Intelligence Services. (2022). FOKUS 2022 - Etterettningstjenestens vurderinger av aktuelle sikkerhetsutfordringer. Etterettningstjenesten, 3–68.

Norwegian Intelligence Services. (2023). FOKUS 2023 - Etterettningstjenestens vurderinger av aktuelle sikkerhetsutfordringer - Viten om verden for vern av Norge. Etterettningstjenesten, 3–70.

Norwegian National Security Aagency. (2020, June 10). Sikkerhetsloven og forskrifter. Nasjonal sikkerhetsmyndighet. https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-forskrifter/

Norwegian National Security Aagency. (2023). Risiko 2023 - Økt uforutsigbarhet krever høyere beredskap. Nasjonal Sikkerhetsmyndighet.

Norwegian Petroleum. (2023, January 9). Companies with production licence. Norwegianpetroleum.no. https://www.norskpetroleum.no/en/facts/companies-production-licence/

Olsen, D. (2022, May 26). *18 oil and gas companies take Cyber Resilience Pledge*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/oil-gas-take-cyber-resilience/

Panda, A., & Bower, A. (2020). Cyber security and the Disaster Resilience Framework. International Journal of Disaster Resilience in the Built Environment, 11(4), 507–518. https://doi.org/10.1108/ijdrbe-07-2019-0046

Pannucci, C. J., & Wilkins, E. G. (2010). Identifying and avoiding bias in research. *Plastic and Reconstructive Surgery*, *126*(2), 619–625. https://doi.org/10.1097/prs.0b013e3181de24bc

Peters, U. (2020). What is the function of confirmation bias? *Erkenntnis*, *87*(3), 1351–1376. https://doi.org/10.1007/s10670-020-00252-1

PTIL. (n.d.). Risiko og risikoforståelse. Risiko og Risikoforståelse. Retrieved March 23, 2023, from https://www.ptil.no/om-oss/rolle-og-ansvarsomrade/risiko-og-risikoforstaelse/

Raina, S. (2022, May 22). *Global CEOs Commit to Collective Action on Cyber Resilience*. World Economic Forum. https://www.weforum.org/press/2022/05/global-ceos-commit-to-collective-action-on-cyber-resilience-ffa0ba5f56/

Rankin, A., Lundberg, J., Woltjer, R., Rollenhagen, C., & Hollnagel, E. (2013). Resilience in everyday operations. *Journal of Cognitive Engineering and Decision Making*, *8*(1), 78–97. https://doi.org/10.1177/1555343413498753

Renn, O. (2010). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.

Ross, R., Pillitteri, V., Riddle, M., & Guissanie, G. (2020). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. National Institute Of Standards and Technology (NIST), 2. U.S Department of Commerce. https://doi.org/https://doi.org/10.6028/NIST.SP.800-171r2

Ross, R., Pillitteri, V., Bodeau, D., & Mcquaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. National Institute of Standards and Technology, U.S. Department of Commerce, 2. https://doi.org/10.6028/NIST.SP.800-160v2r1

Råheim, M., Magnussen, L. H., Sekse, R. J., Lunde, Å., Jacobsen, T., & Blystad, A. (2016). Researcher–researched relationship in qualitative research: Shifts in positions and researcher vulnerability. *International Journal of Qualitative Studies on Health and Well-Being*, *11*(1). https://doi.org/10.3402/qhw.v11.30996

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. The Journal of Digital Forensics, Security and Law, 12(2), 53–68. https://doi.org/10.15394/jdfsl.2017.1476

Segal, D. L., & Coolidge, F. L. (2018). Reliability. In *The SAGE Encyclopedia of Lifespan Human Development*. essay, Company: SAGE Publications, Inc.

Sellvåg, R. S., Brattekås, K., Bruvoll, J. A., Buvarp, P. M. H., Fardal, H., Fykse, E.-M., Hellesø-Knutsen, H., Kirkhorn, S., Nystuen, K. O., & Seehuus, R. A. (2020). Samfunnssikkerhet mot 2030 - utviklingstrekk. Forsvarets Forskningsinstitutt (FFI).

Šimundić, A.-M. (2012). Bias in research. *Lessons in Biostatistics*.

Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. (IJCSIS) International Journal of Computer Science and Information Security, 14(1), 129–135.

Shahzad, S., Qiao, L., & Joiner, K. (2022). Need for a cyber resilience framework for critical space infrastructure. *International Conference on Cyber Warfare and Security*, *17*(1), 404–412. https://doi.org/10.34190/iccws.17.1.52

Solms, R., & Van Niekerk, J. (2013). Information Security to Cyber Security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Southwick, S. M., Bonanno, G. A., Masten, A. S., Panter-Brick, C., & Yehuda, R. (2014). Resilience definitions, theory, and challenges: Interdisciplinary perspectives. European Journal of Psychotraumatology, 5(1). https://doi.org/10.3402/ejpt.v5.25338

Strupczewski, G. (2021). Defining cyber risk. Safety Science, 135. https://doi.org/10.1016/j.ssci.2020.105143

Tarja, R. (2019). "Applicability of Resilience Metrics in the Context of Telecommunications Services." European Conference on Cyber Warfare and Security, July, 845.

The Norwegian Police Security Services. (2022). National Threat Assessment 2023.PST, 2–28.

The Norwegian Police Security Services. (2023). National Threat Assessment 2023. PST, 2–43.

Tripepi, G., Jager, K. J., Dekker, F. W., & Zoccali, C. (2010). Selection bias and information bias in clinical research. *Nephron Clinical Practice*, *115*(2), c94–c99. https://doi.org/10.1159/000312871

UKEssays. (November 2018). Difference Between Deductive, Inductive and Abductive Research. Retrieved from https://www.ukessays.com/essays/data-analysis/difference-between-deductive-inductive-and-abductive-research.php?vref=1

Wangsness, C. (2023, April 2). It vs ot: How information technology and operational technology differ. OnLogic Blog. https://www.onlogic.com/company/io-hub/it-vs-ot-how-information-technology-and-operational-technology-differ/

WEF. (2021). Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers. World Economic Forum.

WHO. (2016). Human Factors - Technical Series on Safer Primary Care. World Health Organization.

Wied, M., Oehmen, J., & Welo, T. (2019). Conceptualizing resilience in engineering systems: An analysis of the literature. Systems Engineering, 23(1), 3–13. https://doi.org/10.1002/sys.21491

Widdowson, A. (2022, May 29). *How to enhance resilience by addressing human factors*. Cyber Magazine. https://cybermagazine.com/network-security/how-to-enhance-resilience-by-addressing-human-factors

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of Resilience Engineering. *Reliability Engineering & System Safety*, *141*. https://doi.org/10.1016/j.ress.2015.03.018

Woods, D. D., & Hollnagel, E. (2017). *Resilience Engineering Concepts and precepts*

Yin, R. K. (2018). *Case study research and applications: Design and methods*. SAGE.

9. Appendixes

9.1 Appendix A: Interview Guide for Practitioners

Interview Guide for Practitioners

Background

1. ID number
2. What is your current position / job?

   How would you describe your job to a 10-year-old?

3. What is your previous background / jobs / experiences / positions?

Part I: Resilience

4. What is your understanding of the term “resilience”?
5. What is your understanding of the term “cyber resilience”?

Part II: Building Resilience

6. Can you identify areas or knowledge or expertise that would strengthen an understanding of building cyber resilience in the energy sector?
7. Can you name any collaborations that would be beneficial to strengthening the expertise to build cyber resilience?

I. Internal collaborations

II. External, same industry

III. External, different sector

Part III: Risk

8. What is your understanding of the term “risk”?
9. How would you describe and define “cyber risk”?
10. How would you describe risk in relation to resilience?

Part V: Cyber Security

11. How would you differentiate between “resilience” and security”?
12. How would you define and/or describe “cyber security”?

Closing Remarks

13. Any comments, questions, or remarks

9.2 Appendix B: Interview Guide for Senior Leader

Interview Guide for Senior Manager

1. Who are you? What is your role at the company? Previous experience?

2. How do you understand the concept of resilience and cyber resilience?

3. Does resilience building benefit companies in the energy sector? If so, how and why.

4. Is resilience building valuable within the security field?

5. What elements would you want to see (or require) from a cyber resilience framework?

6. For a complex organisation, how do you think the best way to implement cyber resilience is? Based on our experience or goals.

7. Is there anything regarding cyber resilience that could be clearer, more defined and better explained

9.3 Appendix C: Interview Guide for Expert Informant

Interview Guide for Expert Informant

1. Who are you? What is your educational background? Expertise? Job? Previous experience?

2. How do you understand the concept of resilience?

3. How do you understand the concept of cyber resilience?

4. What is your definition of cyber resilience?

5. What are your thoughts on the relationship or connection between resilience and security?

6. How do you think cyber resilience could be built within the energy sector?

7. Any collaborations that would benefit from sharing experience and knowledge to build cyber resilience?

8. Any frameworks you could recommend? If so, why?

9. What are your thoughts on resilience engineering towards understanding cyber resilience for complex organizations?

9.4 Appendix D: Informed Consent Form

Cyber Resilience

Purpose of the project
You are invited to participate in a research project where the primary purpose is to explore different understandings of cyber resilience. Furthermore, to explore frameworks and/or further develop relevant frameworks that are beneficial for building resilience. This is a Master's dissertation, and the collected data will only be used for this project.

Which institution is responsible for the research project?
The University of Stavanger is responsible for the project in collaboration with your organisation.

Why are you being asked to participate?
You are asked to contribute due to your cyber and/or security role within the organisation.

What does participation involve for you?
You will be asked to participate in an interview about resilience and your understanding of it, in addition to any reflections you may have related to building resilience for the future. The interview should take 30 to 60 minutes, depending on your contribution.

Participation is voluntary
Participation in the project is voluntary, and you can withdraw your consent at any time without an explanation. All information about you will then be deleted. You will have no negative consequences if you choose not to participate or later decide to withdraw from the project.

Your privacy – how we will store and use your data
I will only use your data for this research project and process your data following data protection legislation, the GDPR (General Data Protection Regulation). Your anonymity will be ensured. Your data will be stored till the end of the project **on the 17th of July, 2023**.

Where can I find out more?
If you have questions about the project or want to exercise your rights, contact:
- The student responsible for the project: Marlene Svela Øvrebø via marlene.svela.o@gmail.com or +47 46474152

If you have questions about how data protection has been assessed in this project by Sikt, contact:
- email: (personverntjenester@sikt.no) or by telephone: +47 73 98 40 40.

Yours sincerely,

Marlene Svela Øvrebø

Consent form

I have received and understood information about the "Cyber Resilience" project and have been allowed to ask questions. I give consent:

• to participate in an interview

I consent for my data to be processed until the end of the project.

(Signed by participant, date)

9.5 Appendix E: Cyber Resilient Framework: Document Analysis

Primary documents on Cyber Resilient Framework used in the analysis. All documents were accessed and checked no later than the 15th of July, 2023.

1. Consequence-Driven Cyber-Informed Engineering (CCE) https://inl.gov/wp-content/uploads/2021/01/CCE-Phase-1-4-Reference-Document.pdf
2. Conceptual Framework for Developing Resilience Metrix for the Electricity, Oil and Gas Sector in the United States https://www.energy.gov/oe/articles/conceptual-framework-developing-resilience-metrics-electricity-oil-and-gas-sectors
3. Cyber Resiliency Engineering Framework (CREF) https://apps.dtic.mil/sti/trecms/pdf/AD1108457.pdf
4. National Institute of Standards and Technology, Cyber Security Framework (NIST) https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
5. World Economic Forum Board Principles Playbook for Oil and Gas: Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers https://www.weforum.org/whitepapers/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers/ **and** The Cyber Resilience Index: Advancing Organizational Cyber Resilience https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf
6. Cyber Resilience Scotland: Strategic Framework https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/
7. Resilience Management Model (CERT-RMM) https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf