UNIVERSITETET I AGDER

Project Master Thesis

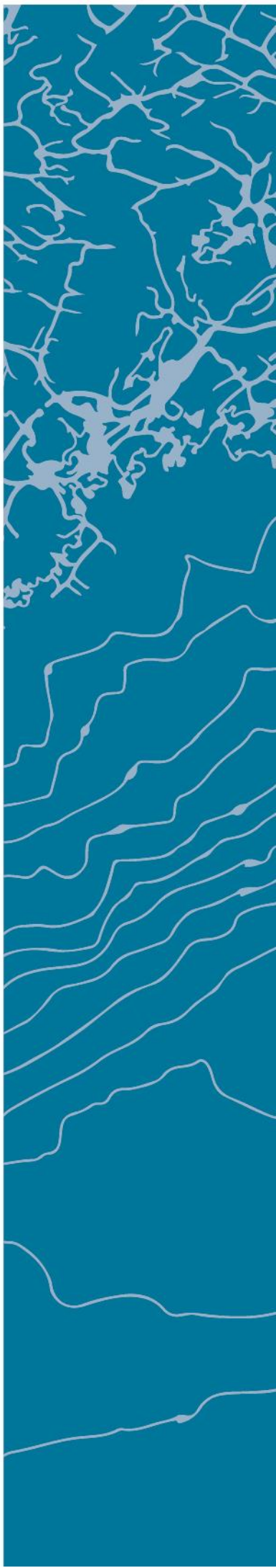
Resilience in Critical infrastructure within the energy sector of Norway

EIRIK ANDRE STÅLESEN
SHIWAN HASSAN

SUPERVISOR

Nadia Saad Noori
Devendra Bahadur Thapa

University of Agder, 2021
Faculty of Social Sciences
Department of Information System



Preface

This master thesis is a completion of master's program (MSc) in Cybersecurity management at the University of Agder (UIA). The study was conducted by and written by two master students that had several courses about critical infrastructure system (CIS) and how the different sectors deal with cybersecurity, where they found a common interest in resilience within the energy sector.

The objective of this exploratory qualitative study was to look at the energy sector's security and find what characterizes resilience and how do they achieve it. Additionally, find out how resilience is achieved through various best practices and other methods. The choice of this research area was proposed by the students themselves with the assistance of their professors and NC-spectrum that specializes in network and information security. We decided the security and resilience of CIS with the energy sector in mind is relevant and worthy of investigation, and our interest in the subject made this decision easier.

We would like to thank our advisors, Professor Devendra Thapa and Associate Professor Nadia Saad Noori at the Department of information systems at UIA, for providing great feedback, guiding us in the right direction, and encouraging us. We would also like to thank Eva Brekka and Mari Aarland, from NC-Spectrum for assisting us in creating a topic and taking it to the direction in our research. This immense task would not have been possible to complete without the help we got from them.

Lastly, we would like to thank all the research subjects that contributed to the interviews and decided to share their expertise and knowledge regarding the findings.

Kristiansand,
June 4th, 2021

Eirik A. Stålesen _____ Shiwan hassan _____

Eirik A Stålesen Shiwan Hassan

Abstract

This thesis investigates what are the characteristics of resilience within the energy sector, as well as what are the "best" known practices being used to increase awareness of the employees. By looking at the existing literature and finding differences between how the energy sector in Norway vs other nations approaches resilience. There is a difference in Norway's more decentralized power grid, where many smaller power stations supply energy, compared to other nation with single large power station. This influences how they will approach resilience.

The study uses a qualitative research approach, with semi-structured interviews to gather data from several organizations within the energy sector of Norway.

The results are then analyzed, and compared to existing research, to achieve a theoretical understanding of the result.

The study identifies what are the characteristics that can be used to define resilience within the energy sector. And defines how these characteristics can be used to achieve resilience within an organization. Furniture more this study analyzes what constitutes “Best-practices” and if they truly are “best,” before investigating how such practices are used to increase awareness of resilience to the employee of the energy sector. To achieve this, we create a list of questions through semi-structured interviews, which are based on our hypothesis, and what was discovered in the literature. To potentially discover what are the best practices used, what resilience is in the energy sector, and how resilience can be achieved in this area.

The findings of this study shows that the understanding and awareness of resilience in Norwegian energy sector share some similarities with existing literature, but the process and how they achieve it is different. One of the more known and often referred framework such as The National Institute of Standards Technology (NIST), is vastly limited in Norway, and they have had the need to make their own version of frameworks.

The road ahead for this paper would be to have a more extensive study with an increased number of organizations and different stakeholders about resilience and the awareness of it. A quantitative study that investigates resilience within the energy sector could provide a more generalizable result to further the understanding of resilience within the critical infrastructure in Norway.

Table of Content

Figure and Table List

Table 1: List of Abbreviations

List of Abbreviations	
CIS	Critical Infrastructure Systems
DSB	Direktoratet for samfunnssikkerhet og beredskap (Directorate of Civil Protection and Emergency Planning)

CIPSEC	Enhancing Critical Infrastructure Protection with Innovative Security Framework
ESCO	European Cybersecurity Organisation
NAS	National Academies of Sciences
FFI	Forsvarets Forskningsinstitutt (Norwegian Defence Research Establishment)
NVE	Norges Vassdrags- og Energidirektorat (The Norwegian Water Resources and Energy Directorate)
KBO	Energy Supply Preparedness Organization
RMI	Resilience Measurement Index
NIST	National Institute of Standards and Technology
HRO	Highly Reliable Organizations
CIP	Critical Infrastructure Protection
CISR R&D	National Critical Infrastructure Security and Resilience Research and Development Plan
ISO	International Organization for Standardization
DLP	Data Loss Prevention
SIEM	Security Information and Event Management
ICS	Industrial Control Systems
SWOT	Strengths, Weaknesses, Opportunities and Threats
GDPR	General Data Protection Regulation
SCADA	Supervisory control and data acquisition
KBF	Kraft Beredskapsforskriften (Power preparedness regulation)
IDS	Intrusion Detection System
NSM	National Security Authority
ICT	Information Communication Technology
HSE	Health, safety and environment

1.0 Introduction

The society we live in is becoming more dependent on critical infrastructure services. Rinaldi et al. (2001) refers to these services as the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole". The dependence of these services is both on the technology used in the infrastructure and on the organization that manages these infrastructures. These infrastructures manage to provide significant social and economic benefits that modern society is dependent on being available, reliable, safe, and secure. Nickolov Eugene. (2005). So, any disruptions caused to the infrastructures could have a significant impact on all aspect of modern society such as proper functioning of government and industries, losing essential services to the community, operating ability of business will be reduced, and other adverse effect, which makes the importance of CIS crucial and must be functioning ag least at minimal level for survival of society. (Nickolov 2005). With several recent attacks on the energy sector, such as the Indian nuclear power plant in 2019, where a malware infected the network (Thomas, 2019). In addition, the U.S. Pipeline shutdown in the early year of 2021, where a ransomware attacked caused disruption to a large part of the east coast of USA (Eaton et al. 2021). These recent attacks show the impact an attack on critical infrastructure can have. To reduce the impact and frequency of threats and attacks against critical infrastructure, an increased attention is being directed at improving the resilience of critical infrastructure. (Brown et al. 2017). What is resilience and how can it be used to increase the resilience of an organization. In modern times the term resilience can have a variety of meanings, depending on context it can be about people, diseases, nature, cyber, structure etc. However, the concept generalized in the context of crisis and disaster management in the mid 2000's. When used it is important to specify in which area the term will be used, in this thesis we will look at resilience in a specific area of critical infrastructure in Norway.

The topic will look at what the energy sector does to achieve a resilient system, and what has been settled on to train the employee to have more understanding of security and how well the training works.

By using qualitative interviews this thesis will investigate what defines resilience in the energy sector, and how employees can become aware of their own role, to increase the overall resilience in their organization. Since frameworks and different practices have an essential role in how security and resilience are implemented, we will investigate what these frameworks have and what are the best practices to use to achieve resilience. This study looks at 7 organizations within the energy sector of Norway, and from these organizations we have interviewed 11 employees to discover what is true about the existing literature, and what has differed from the energy sector in Norway.

1.1 Energy sector

James Chen (2020, p1) states in his article that "*The energy sector is a large and all-encompassing term that describes a complex and interrelated network of companies, directly and indirectly, involved in the production and distribution of energy needed to power the economy and facilitate the means of production and transportation."* The objectives of the energy sector are to produce an uninterrupted supply of energy for the society that completely relies on it to function. For this, the energy sector is involved in exploring and developing oil, gas reserves, oil and gas drilling, and refining.

The energy sector empowers products and services that help with enhancing and extending life through powering computers, transportation, communications, and innovative medical equipment. Therefore, it is essential for the energy sector to operate in a way that ensures the safety and security of the whole associated energy chain all the way from generation to supply Melchiorre (2018).

These requirements have led the energy sector to undergo undeniable changes, particularly electricity infrastructures. The massive digitalization of the energy infrastructure has led to another evolution where systems can be controlled remotely, and the supervision or monitoring of such complex infrastructure has become more optimized. European cybersecurity organization (ECSO 2018).

The digital transformation has given the energy sector many benefits which are envisioned to be a more economical, reliable supply of energy and sustainable.

However, it has led the energy infrastructures to be more exposed to cyber threats. The number of attacks is increasing due to new data interfaces that are used today

such as new connection-oriented meters, other smart devices, and collectors. Which in turn offers new ways of entry for attackers. Therefore, reducing the vulnerabilities and increasing resilience of the systems within the energy sector is essential. ECSO (2018).

1.2 Problem statement

There is a lot of research that exists, which looks at how the energy sector is one of the top five most targeted sectors for attacks worldwide (Wueest, C. 2014). Thus, understanding what type of threats and/or challenges exist, and how they are dealt with in a security and resilience manner is of importance to this research work. When investigating some of the attacks which has happened, and how they have been prevented, Wueest summed it up best with:
"*Most of them could have been prevented by following best practice guidelines for protecting the IT infrastructure and the industrial component.*" (Wueest, C. 2014, p.1).

Therefore, this research work will look further into what methods the energy sector implement/practice to increase or maintain their Cybersecurity and resilience. We have a preliminary research to understand the problem and conducted a qualitative exploratory study to investigate the following questions.

1. What is the role of training to increase cyber awareness and encourage best practices for cybersecurity measure in the energy sector?
2. What are the rules and regulations followed and applied by the different stakeholders in the energy sector or across the supply chain?
3. What are the various levels of resilience awareness among the distinct categories of employees?

1.3 Research questions and objectives

The goal for this qualitative research is to study what challenges the energy sector faces, what are the best countermeasures in the form of practices that could be deployed, and how well these practices work.

We have conducted several interviews with individuals that work in the energy sector to gather as much necessary data as possible. By having these interviews, we should be able to answer the research questions mentioned below:

"What are the characteristics of resilient critical infrastructures within the energy sector, and how can this be achieved?"

"What are the best practices used to achieve resilience within the energy sector, and how are they carried out to increase the awareness of their employees?"

The research questions look at what resilience means for the energy sector, and how well practices are implemented to maintain resilience. By looking into the connection between practices and employees, we seek to understand how beneficial these practices really are. Therefore, the main objective of this exploratory study is to:

1. Examine and understand resilience in the energy sector.
2. Identify best practices used to achieve resilience.
3. How these best practices affect employees.

1.4 Rationale and contribution

The motivation of researchers behind this study is to explore the understanding and awareness of resilience within the energy sector. This study identifies challenges that affect the energy sector and looks at what practices are used to combat these challenges, to understand the relationship between resilience and practices.
Our empirical findings start by discovering threats and challenges that exist within the energy sector today and how they are addressed. It then leads to finding what characterizes resilience and how that is achieved when working in the energy sector. Lastly it shows the different practices used to both achieve and increase the awareness of resilience amongst the employees. We focus on organizations that work with CIS within the energy sector and reflect on what resilience is and how they achieve it.

1.5 Research approach

This study implements a qualitative research approach and exploratory research perspective to examine and uncover the phenomenon in depth. The technique for gathering data is primarily used though semi-structured interviews, supported by documents and frameworks used in the research. The study started by having a literature review which was performed between January February 2021. Followed by several meetings to decide what type of research approach to apply. Eleven interviews were then carried out between March and April 2021. It is important to point out that the selected research subjects are limited to Norwegian context and commenced from NC spectrum's network.

We analyze the data gathered from the interview based on the structure of existing literature review, where we start by looking at security, framework, resilience, and other best practice methods that the energy sector implements to achieve desired level of resilience.

NC spectrum, a Norwegian organization that works with different stakeholders in the energy sectors and specializes in cybersecurity, is the key stakeholder in this research work. One of their employees held a lecture about security within the energy sector in the third semester, which motivated us to contact them and ask if they had any research area or question, they would like us to examine. After a thorough meeting with NC spectrum and our supervisors, it was decided to investigate the two research questions mentioned above. With their help we managed to contact several organizations within the energy sector and set up interviews with our research subject.

1.6 Scope and limitation

This study looks at what characterizes a resilient critical infrastructure within the energy sector and how it is achieved. In addition, the study looks at what best practices are used to achieve resilience. The objective was to examine and explore how critical infrastructures operate, deal with security, and achieve a desired level of resilience, focusing on organizations that work in the energy sector.

When working with critical infrastructure, there is always the issue of confidentiality where we might not be able to get the information that we need to get a conclusion to our result or validate our findings.

Contacting employees within the energy sector and asking about security measurements used within their organization, how well and on what level it is implemented, may result in them not wanting to answer the questions. Not only is the possibility that they are not willing to answer it, but how well does their honest opinion translate into the reality of the situation. If we only interview a few select members of each organization, do these few people reflect the actual situation within the organization, or did we just sample on the end of a scale. Another factor is if an employee has a negative opinion about their organization and will not express their honest opinion about the situation in fear of being traced back to the individual.

1.7 Thesis Overview

Chapter 1 - Introduction covers an overview of the problem and represents the research questions.

Chapter 2 - Related Research discusses related research that yields further understanding of 1) what characterizes resilience and 2) what best practices are used to achieve resilience.

Chapter 3 - Research Approach explores the choice of a qualitative study with an exploratory approach. Moreover, data selection, analysis, validity, and ethical consideration are presented.

Chapter 4 - Empirical Findings addresses the findings collected from the fieldwork. A thematic mapping of the interviews has been performed to collect these findings.

Chapter 5 - Discussion researchers discuss the findings collected from their perspective and academics.

Chapter 6 – Conclusion and contribution whatthis research has Summerizes the project work and contribution to IS. It provides a conclusion and a brief reflection on future work.

2.0 Background and related research

To gain a better understanding of state of the art of the energy sector's security and resilience. We organized a literature review to get an overview of the security challenges, resilience, and other best practices that are used within the research field. We decided to follow Kitchenham's guidelines (kitchenham & Charters, 2007), the objective was to get an understanding of existing research related to our research questions. Kitchenham, (2007) states that these guidelines have been made with the following intentions:

- Assist researchers in conducting empirical studies.
- Summarize the existing evidence concerning technology.
- Identify any gaps in current research to suggest areas for further investigation.
- Provide a background to position new research activities appropriately.

The literature review serves as a foundation to develop the research question by finding gaps and issues emerge or have been highlighted by researchers in the field. To that end a further investigation in this research work will be conducted. In the literature review phase, a total of 33 articles were reviewed consistently and relevant to our research. The research was conducted based on search string and criteria explained in Appendix 2: which provided a method in finding these articles. The following categories and literature themes emerged: CIS, resilience, security challenges within the energy sector, framework, and practices. These categories and themes in Table 2 were reviewed so that we could find more information about our research work and how they were tied together. The research work started by doing the following:

- To discover what defines resilience and how it is achieved in CIS, we first had to uncover what is CIS and the importance of it.
- That led to learning about the security of CIS and what challenges it faces.
- Afterwards we looked at the term resilience, what characterizes it, and how it is achieved in the energy sector.
- Framework was then the next thing to be covered due to the importance of it in CIS.

- Lastly, the research focused on finding as many best practices implemented in the CIS that are related to security and resilience.

Table 2: Article Reference and quotes from them

Theme	References	Quote
Category 1: Critical Infrastructure Systems		
Identification and designation of CIS	(EU Directive 2008/114/EC, 2008)	"'Critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."
Improving Critical Infrastructure Systems	(Croope, S. V., & McNeil, S. 2011).	"The objective of the decision support system is to reduce the vulnerability of places and infrastructure systems through the use of mitigation strategies that increase system resilience and resistance to the stresses imposed by disasters."
Critical infrastructure interdependencies	(Rinaldi et al., 2001)	"What happens to one infrastructure can directly and indirectly affect other infrastructures, impact large geographic regions and send ripples throughout the national a global economy."
Critical infrastructure protection.	Nickolov, E. (2006)	"The best practices and resources on cyber security policy developed in the last years provide valuable guidance both to industrialized and developing countries."
What is Critical infrastructure systems	(Jensen, C. 2019)	"Critical infrastructure consists of "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."
Critical infrastructure review	Xiao-Juan, L., & Li-Zhen, H. 2010	critical infrastructure is of the first rank, it comprises of some fundamental infrastructures for daily production and living, so the vulnerability and interdependency of critical infrastructure systems (CIS) is a hot issue for exploration.
Hva er kritisk	Sikkerhetstoppmøtet, (2014)	"«Kritisk infrastruktur de anlegg og

infrastruktur		systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner, som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.»"
Critical infrastructure & Cybersecurity	European Commission, (2007)	"Stakeholders must share information on CIP, particularly on measures concerning the security of critical infrastructure and protected systems, interdependency studies and CIP related vulnerability, threat and risk assessments."
Importance of critical infrastructure	(Melchiorre. 2018)	"It is shown that the protection of critical energy infrastructure is essential for states because the well-being of their societies depends on its good functioning."
Category 2: Resilience in critical infrastructure		
Resilience management	(Herrera, et al., 2018)	"A model provides traceability and meaningfulness for tools in view of different contexts of application, which becomes a fundamental support to decision-making in the scope of resilience management."
Factors and elements of resilience in CIS	(Rehak et al., 2018)	"Factors determining the resilience of these elements are identified, both in terms of technical resilience (i.e., robustness and recoverability) and organizational resilience (i.e., adaptability)."
Understanding resilience and safety	(Hollnagel, E. 2016)	"New types of accidents have, historically speaking, always led to new types of causes but without challenging the underlying assumption of linear causality. We have therefore become so used to explain accidents in terms of cause - effect relations that we no longer notice it."
Enhancing resilience of CIS	(Jensen, C. 2019)	"Enhancing security is, perhaps, the most fundamental component of critical infrastructure protection."
Resilience of interdependencies	(Rinaldi et al., 2001)	"Cyber interdependencies are relatively new and a result of the pervasive computerization and automation of infrastructures over the last several decades."
What is resilience, and how can it be integrated.	Stavland, B., & Bruvoll, J. (2019)	"Resilienshåndtering tar utgangspunkt i resultatene fra resiliensevalueringen og benytter dem til å utvikle planer for å modifisere resiliensnivået."
Enhancing resilience of energy system	National academies of science,	"For decades, the planners and operators of the system have taken care to assure that the electric system

	engineering and Medicine (NAS. 2017)	is engineered and routinly operated to achive high levels of reliability. Increasingly, the system's planners and operators are focusing on resilience as well."
Resilience in various countries.	(Gjesvik, 2019)	"The Finnish approach to cyber security has been primarily defensive, focused on measures of resilience."
Resilience Management Guidelines for Critical Infrastructures.	(Herrera, et al., 2018)	"Targeted at policy makers, it provides an overview of essential resilience concepts, methods and techniques to attain results from these Projects and to work towards an integrated guideline which could be implemented EU wide."
Resilience management index	(F.D petit, et al., 2013)	"The main benefit of the RI was to give the critical infrastructure owners/operators a performance indicator of the resilience of their facilities that could support their decisions in risk and resilience management."
Resilience: Designing for the unexpected	(Boumphrey & Bruno, 2015)	"In parallel to this, rapid technological change can provide both opportunities and threats to resilience."
Understanding landscape of resilience	(Juliet Mian et al., 2018)	"The changing energy landscape, through decentralisation of energy supplies and the forming of microgrids is making resilience and integrated systems approaches increasingly importance. "
Highly reliable organizations	(Gifun, J. F., & Karydas, D. M. 2010)	"The model proposed herein was developed and derived from acomprehensive examination of the following organizational models: the High Reliability Organization, the Disaster Resistant University, the Resilient Enterprise, Enterprise Risk Management, Risk-Based Process Safety, Reactor Oversight Process, Hearts and Minds, and Business Continuity Planning."
Enhancing resilience through emergency planning	(Ramsay, & Kelly, T. 2009)	"This extension of thinking, planning, and anticipation is vital, because the assessment of the residual risk may, as in these accidents, ultimately be proven to have been significantly flawed."
HRO managing the unexpected	(Gebauer and Kiel-Dixon 2009)	"HROs can teach managers in more traditional organizations a great deal about preparing themselves – and their companies – for extreme situations."

HRO and CIS resilience	(Fritts et al. 2017)	"In contrast, however, academic and practitioner evidence did suggest implementation strategies and tactics. Although never formally validated, High Reliability Theory (HRT) has been suggested as an implementation approach to CI protection (CIP)."
Category 3: Frameworks		
Identify the frameworks used specific within the energy sector.	(u.s. department of energy office of electricity delivery and energy reliability 2015), (Kwasinski, A. 2016).	"This proposed framework is built on fundamental concepts that serve to quantitatively represent power grids' performance during natural disasters and other extreme events."
Identify the frameworks used within CIS generally including the energy sector.	(Barret. M. 2018), (Sedgewick (2014) (European Commission. 2007), (NSCI. 2019),(CPNI. 2021), (European Commission. 2013), (Xiao-Juan, L., & Li-Zhen, H. 2010), (Yusta et al. 2011), (Department of Homeland Security. 2013), (Rinaldi et al. 2001), (Nickolov, E. 2006).	"The National Plan builds upon the critical infrastructure risk management framework introduced in the 2006 NIPP." "The Framework identifies principles of cooperation (i.e. responsibility, comprehensiveness, partnerships, coherency of action, risk-based, all-hazards, resilience, clear communications, and continuous improvement) and it recognizes that emergency management is comprised of interdependent risk-based functions: prevention, mitigation, preparedness, response and recovery."
Category 4: Practices		
Practices used in CIS or energy sector.	(Wueest, C. 2014), (Department of Homeland Security 2013), (M.T., Ramsay, C.G., & Kelly, T. 2009), (Lykou et al. 2018), (Gjesvik, L. 2019), (Jensen, C. 2019), (EU Directive 2008/114/EC, Identification and designation of European critical infrastructures 2008), (Sabino, V. 2020), (Bailey et al. 2020), (u.s. department of energy office of electricity delivery and energy reliability 2015), (Labak et al 2016), (Skandsen, H. 2020), (Miron, W. Muita, K. 2014), (European Commission. 2013), (Kallio et al. 2016),(NSCI. 2019), (Barrett, 2018), (Vilnius, 2018).	"For all regular client computers, the well-established best practice guidelines apply. These computers are often the first ones to be attacked." "Utilities should leverage their best practices to ensure that all employees are aware of the specific threats facing the organization and the specific indicators they, as employees, should be looking for in order to contribute to the overall security of the company and its customers." "It is concluded that organizations can become wiser by looking at incidents outside their own sector and by using these recurring themes to explore the resilience of their emergency plans. Recommendations are also made for best practices to improve the learning of lessons within organizations."
Forskrift om fordeling	(Olje og energidepartementet, 2019)	"Forskriften kommer til anvendelse ved planlegging, bygging, eierskap og

og bruk av energi		drift av anlegg for produksjon, omforming, overføring og fordeling av elektrisk energi, varmeenergi produsert i fjernvarme- og fjernkjøleanlegg, samt ved omsetning og bruk av elektrisk energi."
Security information and event management (SIEM)	(Bhatt et al., 2014)	"Security information and event management (SIEM) systems are an important tool used in SOCs; they collect security events from many diverse sources in enterprise networks, normalize the events to a common format, store the normalized events for forensic analysis, and correlate the events to identify malicious activities in real time."
Addressing energy sector vulnerabilities	(Bailey et al., 2020)	"These vulnerabilities first came to light as early as 2010, when a Puerto Rican utility estimated that tampering with wireless smart meters could result in revenue losses as high as $400 million per year."
Energy sector Cybersecurity is achievable.	(Sabino, 2020)	"Effective cybersecurity awareness training is another essential action that organizations can take to keep corporate users safe on the network."
Cybersecurity measures	(Lykou et al., 2018)	"Which reveals the need for security reinforcement with suitable measures to increase cybersecurity protection."
Category 5: Security challenges		
Security of CIS	(Jensen, 2019)	"Similarly, in the cyber realm, security means identifying virtual vulnerabilities and addressing those vulnerabilities."
Analysis, evaluation of CIS protection	(Nickolov, 2006)	"Analyzing of the current reaction abilities of network elements and systems based on their reaction to possible attack scenario."
Monitoring and security of CIS	(Kyriakides & Polycarpou, 2014)	"In particular, this monitoring system is based on a novel hybrid architecture, in which different sensors, architectures and physical phenomena under monitoring coexist and cooperate to provide different views of the same physical phenomenon."
Cybersecurity of smart energy sector network	The European Cybersecurity Organisation (ECSO, 2018)	"These services rely on interconnected smart devices, such as sensors and actuators, widely deployed in households to measure energy use

		and reduce energy equipment consumption to prevent overload."
Energy sector attacks	(Wueest, C, 2014)	"To stop this self-inflicted DDoS attack, part of the monitoring and control network had to be isolated and disconnected. Fortunately the situation was resolved without any power outages."
critical infrastructure protection	(Lars Gjesvik, 2019)	"For the protection of critical systems, the concern is not necessarily espionage and criminal activity per se, but the risk that digital technologies would be used to destroy and disrupt their functionality."

2.1 Critical infrastructure systems:

Critical infrastructure systems are essential for their continued service to maintain the nation's socioeconomic systems, (Croope & McNeil. 2011). Critical infrastructures are defined as "*assets, systems, or parts thereof, essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being*" (EU Directive 2008/114/EC p.43). (Rinaldi et al. 2001 p.13) refers to this definition of CIS in his article:" The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole". Furthermore, in the report "Society's critical functions," published by Direktoratet for samfunnssikkerhet og beredskap [1](DSB) in 2015, there is a list of systems/functions that are deemed critical. According to the list made by DSB (2015), say that a system is critical if, within seven days after the system has failed, society is no longer able to satisfy one or more basic needs. CIS consists of electrical power plants, telecommunication, transportation network, oil and natural gas systems, water distribution system, banking and financial, healthcare service and security services (G. Ellinas et al. 2014). These infrastructures manage to provide significant social and economic benefits that modern society is dependent on being available, reliable, safe, and secure, (Nickolov, 2006). In addition, Nickolov (2006) mentions if CIS is damaged it would have a serious impact on citizens, the functioning of government and industries, or other adverse effects. This makes the importance of CIS crucial and

[1] The Norwegian Directorate for Civil Protection

must be functioning at least at a minimal level for survival of private and public sectors. To ensure the survival of private and public sectors, CIS needs to have proper protection from the challenges and threats it faces. These threats can be categorized into three classes: human error, natural threats and accidental or technical threat (Robles et. al 2008). Additionally, Kröger (2008) mentions five factors that affect the risk of failure in critical infrastructure:

1. System-related factors related to complexity and interconnections.
2. Technological factors related to innovation and operation.
3. Environmental factors such as resource access and Climatic conditions.
4. Institutional factors such as market liberalization, regulation, and legislation.
5. Societal factors such as the public's risk perceptions, urbanization, and exposure to terrorist acts.

The increased connectivity and interdependencies between such systems increase the complexity of managing critical infrastructure and modelling the risk of cybersecurity threats (Rahman et al.,2011; Xiao-Juan & Li Zhen, 2010). Therefore, the essentiality of CIS cannot be understated and the protection and resilience of it is paramount, (F.D Petit et. al 2013).

2.2 Security challenges of the energy sector

Cybersecurity could be seen as a complicated practice that varies from being a nuisance all the way to high-level national security threats. Protecting critical infrastructure such as the energy sector has been a concern for states for well over a decade and it still faces challenges that could be problematic for many reasons (Gjesvik, 2019).

Some of these challenges have become more prominent over the years such as *increased complexity*, a natural phenomenon with digitalization where more and newer integration of the system improves it and makes it more complex. Going back a few years ago the threats were tangible and focused a lot on being physical threats, such as floods, wildfires, and hurricanes (Jensen, 2019). The impact of a natural disaster can have a dire effect on the energy sector, even when they are not physically

impeached sudden demand surges during crisis can provoke blackouts, leading to loss or denial of service" (Nickolov, 2006).

Nevertheless, today the energy sector is susceptible to other frequent threats (e.g., fault of equipment or software, human error, and insider attack), which does make it more difficult to operate, secure, and ensure that the system is robust (Kyriakides & Polycarpou, 2014). In addition, one of the biggest threats or challenges that have increased throughout the years are cyberattacks, which can harm systems by shut it down, disrupt operations or giving remote access to attackers. Cyberattacks could leak sensitive information, critical equipment, and harm third party partners, which makes it particularly important that these challenges are addressed. Based on a study by European Cybersecurity Organization (ECSO) in 2018, about cybersecurity for the energy sector, there have been several major attacks targeting the energy sector, like Stuxnet in Iran or Black Energy in Ukraine, (ECSO, 2018) Attacks on the energy sector have become an ever-increasing issue, and measurements must be taken to prepare this sector for these threats. Table 3 shows the possible threats CIS with the energy sector included.

Table 3: List of attacks and threats based on CIS studies. (ECSO 2018)

Nr.	Attack / Threat	Number of studies per sector									
		Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

Table 4: Projected losses/hour for various industries during IT outages. (Kyriakides & Polycarpou, 2014)

Industry	Typical hourly cost of downtime (in US dollars)
Brokerage service	6.48 million
Energy	2.8 million
Telecom	2.0 million
Manufacturing	1.6 million
Retail	1.1 million
Health care	636,000
Media	90,000

Kyriakides and Polycarpou (2014) mentioned based on estimates from studies and surveys performed by IT industry analyst firms that the assessment cost of cybersecurity incident and downtime that affect the energy sector is one of the three most impacted sector and has the highest incident and downtime cost as seen in Table 4.

Wueest, (2014, p1) stated, "*The energy sector has become a major focus for target attacks and is now among the top five most targeted sectors worldwide*".

Since the energy sector is such a clear target by hacktivists, espionage, or foreign governments there is a need to protect it. Wueest mentioned when talking about attacks against the energy sector "*Most of them could have been prevented by following best practice guidelines for protecting the IT infrastructure and the industrial component.*"

Other security challenges within various sectors (energy sector included) that are smaller states such as Norway could have restrictions on how to deal with incidents due to the size of organizations, where their resources could be limited, and practices provided on a European level might not be implemented fully. In his article Lars Gjesvik (2019), identifies that the regional and European cooperation is not at the desired level, while some of the initiatives might be implemented, they are unfortunately too recent and too limited to have any significant impact. He additionally mentioned that cooperation and collaboration are essential for states, and these are not at the extensive level that it should be.

2.3 Maintain security & resilience.

Resilience has in recent years increased in popularity and can be used in several different definitions, these can be the city, social, disaster, ecology, and more. The multitude of definitions can be viewed in the paper of Herrera. et al. (2018) where Five European projects conducted literature reviews on resilience, and one of these identified over 300 different definitions.

Hereafter in this thesis the term resilience is defined as the system's ability to maintain function during stress and exertion, and that there is an element of learning.

The purpose of increased resilience is to improve future handling of issues both known and unknown, which can impact a system or function. In this respect, resilience plays a crucial role in ensuring the security and reliability of systems within the CIS (energy sector included) and is understood as a cyclic process based on the continual enhancement of system prevention, absorption, recovery, and adaptation (Rehak, et al. 2018). Erik Hollnagel states "*A system is resilient if it can adjust its functioning prior to, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions.*" (Hollnagel, E.2014, pg 376)

Jensen, (2019, pg 1) further states "In *cyber-centric environments, resilience builds on security to round out a comprehensive cyber defense program that addresses all*

phases of preparation and implements steps to prepare for, and respond to, any cyber threats."

Due to interdependencies of these systems, Rindali (et al. 2001. Pg 11 - 25) mentions that if one of these infrastructures or sectors were to be disrupted, it could create a cascading effect that could damage or destroy others with them, which in return makes each sector as important as the other.

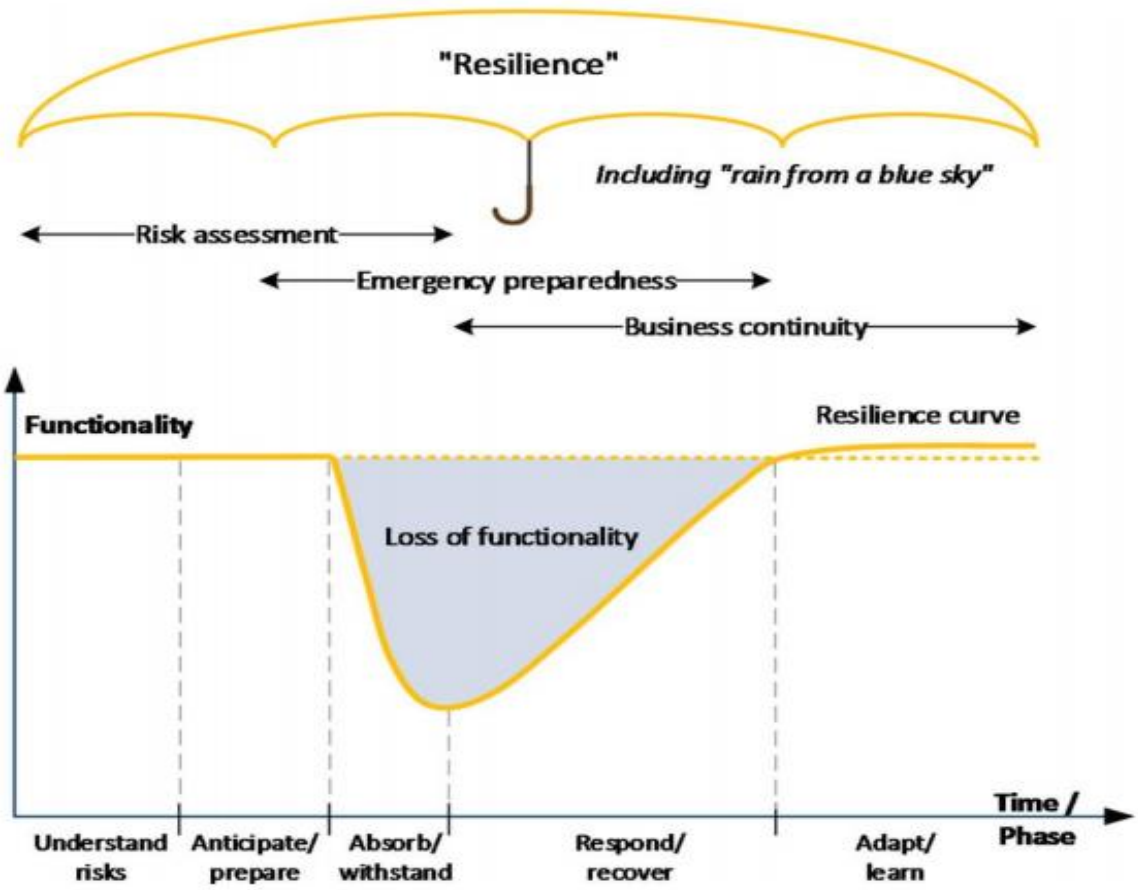


Figure 1: Umbrella concept (Øien m.fl., 2018)

In Figure 1, the resilience is set in the context of risk assessment, emergency preparedness, and business continuity, and shows how resilience can be seen as a process in time, with different steps of before, during, and after an incident has occurred. During the two first steps, understanding risk and anticipating/preparing shows the resilience curve as it is or its normal stage. When an incident occurs, we move over to the absorb/withstand and respond/recover steps. These define the time of loss of functionality and where the resilience is tested. If the resilience is strong then the curve will not change to much from its normal state. After the incident is

resolved, the next steps are adapt/learn which are where progress can occur, as seen where the resilience curve has risen higher than before the incident. Thus, improvement has been made, and the system is stronger than it was before the incident, (Stavland, B., & Bruvoll, J. 2019).
Figure 1 illustrates how resilience functions, and how it can arch to visualize a potential loss of functionality. Creating, maintaining, and improving resilience can massively impact business economics, its level of continuation, and its capability to handle threats, (Stavland, B., & Bruvoll, J. 2019).

A report written by the National Academies of Sciences, looked at resilience related to the energy sector in the USA, and how to achieve a resilient system (Figure 2, NAS, 2017).

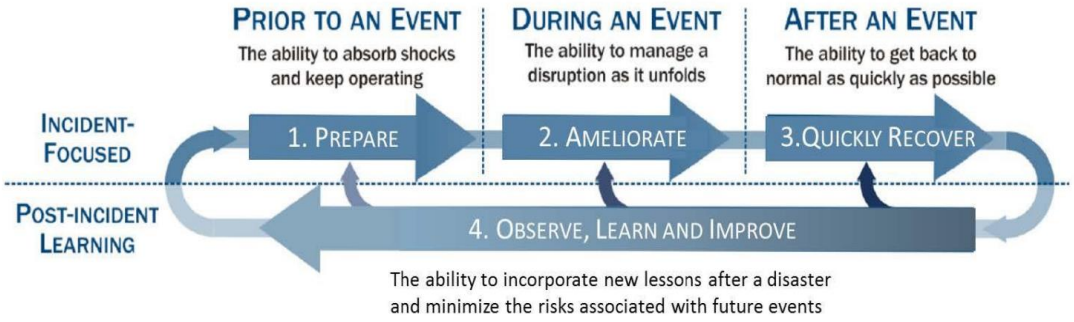


Figure 2: NAS Achieving resilience (NAS 2017)

A resilient system can withstand sudden attacks/incidents and continue to work, it can also, deal with interruptions, and have the ability to rapidly recover and bring functionalities of the system back to normal. The NAS report explains it as follows:
"*It's not just about reducing the possibility of power outages, but also about limiting the extent and consequences of this happening, rapid recovery, and learning lessons from what has happened. A resilient system must minimize power outages, but recognize that it may occur and prepare to deal with them and learn from it*" (NAS, 2017: p,1)

Different states and organizations could measure their resilience by using the following four indicators (kwasinski, 2016).

1. The ability to resist both internal and external attacks/threats.
2. The ability to recover after an incident.
3. Capacity for planning and preparation.

4. The ability to adapt.

By following the indicators above the maintenance of systems within the energy sector and other CIS, can become more thorough. The energy sectors could look at historical events and decide on how to isolate and control upcoming events. This will lead to having a system that works as intended where nothing unexpected could occur, (FFI-rapport, 2019).

Countries such as Norway deal with resilience and cybersecurity of their systems by giving the responsibility to the Norwegian Water Resources and Energy Directorate (NVE). NVE helps the energy sector by supervising their systems, write a regulation and advise on how to approach cybersecurity to become a resilient CIS, (Lars Gjesvik, 2019). NVE works as well with KraftCERT, which is a private company owned by most energy operators. KraftCERT's functions as an advisory body and provides information to several organizations, where they specialize in industrial control system (ICS) however, with security they have a limited role and capacity (KraftCERT, 2019). Additionally, KraftCERT has been added along to the energy supply preparedness organization (KBO) so that the security and resilience of the energy sector are prepared in a sufficient manner (Energilovforskriften[2], 2019). Lars Gjesvik, (2019) mentions in his report that there is another approach towards resilience management. This focuses more on the measurement of resilience that is built on existing approaches to security. Including the history of cooperation between public and private actors that aimed at enhancing resilience by having the whole of society contributing to overall security. Figure 3 shows that Norway has a joined cyber coordination network of a response and management of cyber security. The Figure represents both the complexity of the response system to cybersecurity incidents in Norway and if an attack happens it would impact different level of organization within the ecosystem due to its connectivity.

[2] The Energy Regulations

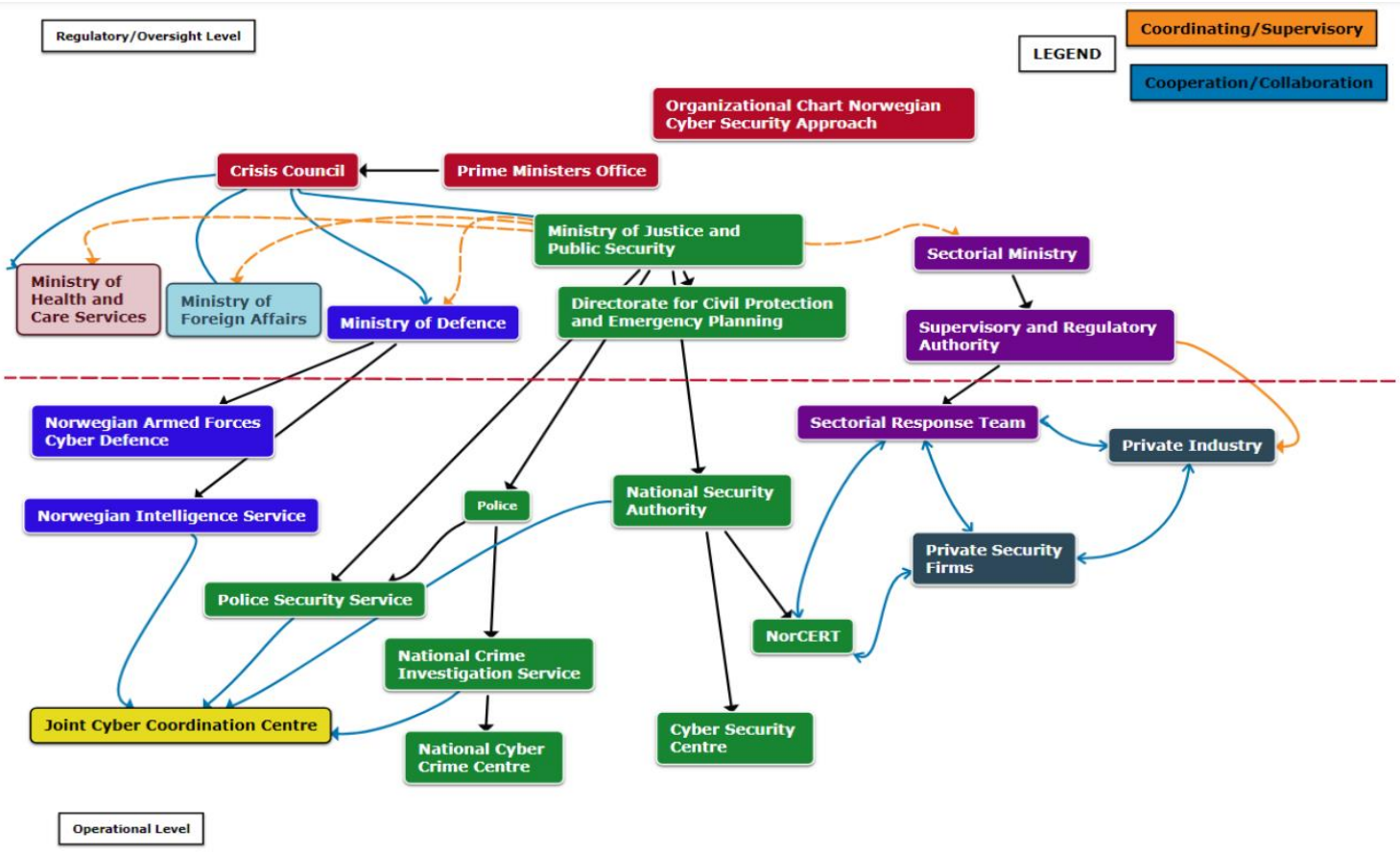


Figure 3: Norwegian Cybersecurity Approach (Gjesvik, 2019)

Enhancing the resilience of critical infrastructures has been a priority for many countries due to the consequences it could have if they are not prepared sufficiently. To achieve resilience, the system must be able to withstand threats, mitigate impacts of a threat/attack, and be able to return to normal operations as soon as possible. Looking at these "requirements" the U.S Homeland security (DHS) decided to partner up with Argonne National Laboratory to develop a methodology that would assist CIS on how to make decisions for risk management, business continuity, and disaster response F.D Petit, Et. Al. (2013). The methodology developed was called Resilience Measurement Index (RMI), It was formulated to capture the aspect of resilience for critical infrastructure and can be combined with other tools so that CIS could be able to reduce the significance and duration of impacts of attacks by looking at the following four groups in figure 4.

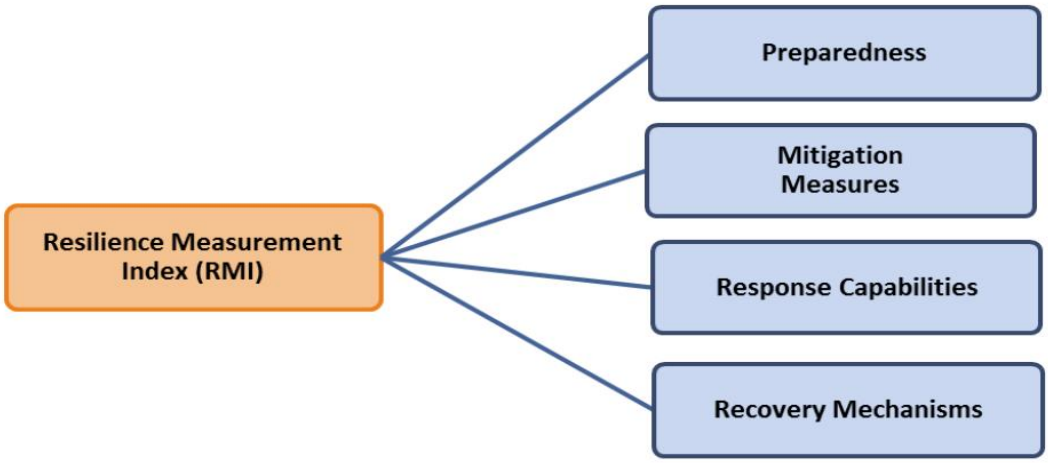


Figure 4: Resilience Measurement Index (RMI) (Petit, Et. Al. 2013).

To increase the specificity of how CIS could achieve a wanted level of security and resilience, RMI looks at each group and adds subcomponents that would be relevant to the contribution of the given component, such as the one shown in figure 5. F.D Petit, Et. Al. (2013).

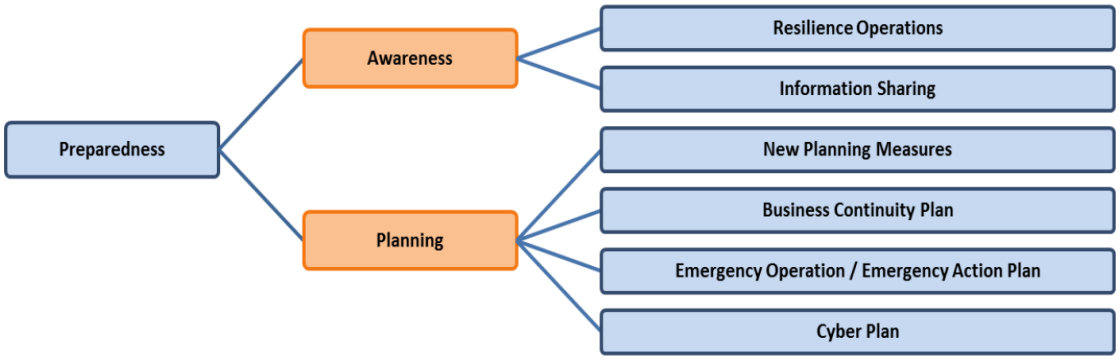


Figure 5: RMI Preparedness (Petit, Et. Al. 2013).

Having a resilience-based approach when it comes to CIS security is essential, and it needs to be considered as an inherent part of a project, as opposed to an afterthought (Boumphrey & Bruno, 2015). Furthermore, Juliet Mian et. al. (2018) reports that there are additional ways of achieving/enhancing resilience. The focus lies on looking at policies, practices, and sharing of information. The paper argues that the best way of achieving resilience is by having a combination of different approaches, and that no single policy instrument is the answer to resilience challenges. The study further states that sharing information and experiences between sectors, cities, and

countries has been a powerful tool to engage people in thinking more broadly about the benefit of resilience.

2.4 Frameworks

To further increase the resilience and security of CIS, there is a need to develop frameworks that can assist in monitoring and, controlling the security of such systems, (Kyriakides & Polycarpou 2014). NIST published a framework (Sedgewick, 2014), whereas according to them the framework created is "*A Prioritized, flexible and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security*." Croope & McNeil (2011) argue in their paper that a framework they created could be implemented in the aftermath of a disaster by having a set of rehabilitation tools which will help both repair and improve the resilience of CIS.

To handle the security risks within the various CIS, at least twelve countries or regions have defined criteria for security standards and the way to implement them (Yusta et al., 2011). Table 5 shows that the European Union (EU) has created a critical infrastructure regime through the European Program for Critical Infrastructure Protection (EPCIP). The United States has a cooperative framework that has been created with the assistance of Homeland security. As for Canada and the United Kingdom, Cooperative frameworks are in place as well. (Miron & Muita 2014)

Table 5: Frameworks created by countries or regions. (Miron & Muita 2014)

Region	Regulation	Model
European Union	European Program for Critical Infrastructure Protection (EPCIP)	Regulation
Canada	National Strategy for Critical Infrastructure (NSCI)	Cooperative Framework

United Kingdom	Centre for the Protection of National Infrastructure (CPNI)	Cooperative Framework
United States	National Infrastructure and Protection Plan (NIPP 2013)	Cooperative Framework

Furthermore, based on a paper released by the U.S. Department of energy (2015), which focuses heavily on cybersecurity resilience that is built upon the framework produced by NIST (Barrett, 2018). Meaning that different sectors not only use the frameworks provided by their region/country, but they add other frameworks such as NIST (Barrett, 2018). This framework contributes to creating a set of activities where the goal is to achieve specific cybersecurity outcomes and provide examples/guidance on how to make the systems resilient. The paper specifies that the core of this framework is not a checklist, but as essential outcomes that are determined by the industry as helpful in managing cybersecurity. NIST (Barrett, 2018), states that the framework helps different types of CIS sector with the following:

1. Describe their current cybersecurity posture.
2. Describe their target state for cybersecurity.
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
4. Assess progress towards the target state.
5. Communication among internal and external stakeholders about cybersecurity risk.

NIST (Barrett, 2018) further states that "*The framework enables organizations - regardless of size, degree of cybersecurity risk, or cybersecurity sophistication - to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure*".

The way to improve and maintain a resilient CIS, the framework focuses on five core functions that are performed concurrently and continuously shown in table 6 which

is used to improve the resilience and cybersecurity of critical infrastructures within the energy sector. Function and Category Unique Identifiers

Table 6: Function and Category unique identifiers (Barrett 2018)

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

2.5 Highly Reliable Organizations

Pettersen and Schulman (2016) implies that resilience and reliability are equally important, and explicitly identified that HRO's are associated with critical infrastructures.

The definition of Highly reliable organizations (HRO) was originally made by Roberts (1989) who stated the following:

"There is a class of organizations that can do catastrophic harm to themselves and a larger public. Within this larger set of potentially harmful organizations there is a subset which has operated extraordinarily reliably over an extended period. Operational reliability rivals short term efficiency as major goals in these

*organizations. Extraordinary attention is paid to operational reliability both because of the inherent dangers of the situation and because outcomes reliability is impossible to realize without operational reliability. Hence, we call these organizations "high reliability" organizations" (*Roberts, 1989, *p. 112).* This definition means that HRO are organizations that manage to anticipate, resist, and recover from incidents by following specific policies, and practices they have which focus on reliability, disaster resistance, high organizational quality, and resilience (Gifun, & Karydas, 2010). Crichton, Ramsay, and Kelly (2009) argue that organizations could enhance their resilience and share the knowledge with other CIS by having an emergency planning approach. Hassel, and Zio (2013) recommended that the energy sector systems need to have reliability and are essential for their systems. Gebauer and Kiel-Dixon (2009) suggested that CIS should look at all the HRO's hallmarks and implement them, so that they have the capabilities needed to improve their security and resilience. From the articles mentioned above, reliability, organizational resilience, and critical infrastructure, we can see that the concept of using HRO hallmarks in CIS can be beneficial and will improve or provide resilience. In addition, the US Department of Homeland security implies in their publications (2013, 2015) that a successful critical infrastructure protection (CIP) needs to have resilience as an anchoring concept. Furthermore Fritts et al. (2017) concluded that the five HRO hallmarks and the five DHS CISR priority areas may not have the same construct, but they have a conceptual convergence, where both aim to achieve the same goals.

Table 7 shows the similarities with the DHS priority areas. Thus, HRO can be combined with other CIP to achieve resilience.

Table 7: Comparison of HRO hallmarks to DHS priority areas. (Cantu 2020)

HRO: Hallmarks	DHS National CISR R&D Plan: Priority Areas
Preoccupation with Failure: Be alert to failures, especially as indicated by weak signals. Prepare for and prevent failure where feasible, and respond and recover from failures when they do occur.	Develop integrated and scalable risk assessment and management approaches.
Reluctance to Simplify: Don't overlook subtle aspects of complex problems, and avoid classifications of conditions into convenient categories.	Develop the foundational understanding of critical infrastructure systems and systems dynamics.
Commitment to Resilience: problem events may be unavoidable but an organization can identify, plan for, and execute recovery and service-restoral measures to ensure continued delivery of products or services.	Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.
Sensitivity to Operations: HROs realize that potential problems can lie in little-recognized location in a process or system. They acknowledge that failures usually are the result of more than one source or cause.	Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action
Deference to Expertise: Ensure that those with the specific problem-solving knowledge, skills, and abilities are engaged in providing solutions and avoid restrictions caused by hierarchy and chain-of-command constraints.	Build a crosscutting culture of CISR R&D collaboration.

2.6 Other best practice methods

In addition to these regional regulations and frameworks, some countries have made their legislation and frameworks specifically for each of the sectors that need to be implemented in every CIS sector. Norway has the energy contingency regulations which is a framework that will provide better security against espionage, sabotage, and terror at a time when the threat and risk picture is constantly changing. (Energilovforskriften[3] 2019). Several organizations combine different frameworks to achieve the best possible security, (U.S. Department of energy, 2015).

When it comes to maintaining security and achieving the highest level of resilience, most energy sectors use best-practice guidelines provided by NIST, ISO standards, and or the European Commission to provide the "how-to" solution to achieve security. "Prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services." (Barrett, 2017)

When it comes to protection and mitigation against attacks within the energy sector, Wueest, (2014) mentions several countermeasures that can be used such as:

A) Email filtering which can help prevent certain spear-phishing attempts can be beneficial for untrained personnel.

[3] The Energy Regulations

B) Data loss prevention (DLP) can track the flow and access of critical information and prevent it from leaving or encrypting the information.

C) Security information and event management system (SIEM) provides a main area that collects alerts into this place, by gathering and analyzing data from several systems, to detect any abnormal behavior or to find potential attacks (Bhatt et al., 2014).

While having protection may not fully stop the attacks, the implementations can still be worthwhile to slow and mitigate attacks. Additionally, Wueest, (2014) states "*Industrial control systems (ICS) should be specially protected and monitored. The control system and control network should be secured. Where possible, ICS should be separate from the Intranet. Isolating these networks alone is often not enough to protect the control network, but it can make it more difficult for attackers to succeed.*

Most organizations use analytic teams that monitor threats and provide a holistic view on threats and other factors such as legal, geopolitical, and economic) which shape the threat environment they need to defend against, (Bailey et al., 2020). Additionally, t e analytic team provides an effective cybersecurity awareness and by having this, the organizations teach employees to identify what kind of threats exist and how they can keep their information secure and mitigated from attacks like Phishing, ransomware, and social engineering (Sabino,2020). Organizations as well as create and practice incident response plans to build confidence, muscle memory, and process clarity so that when an actual incident happens the organization is prepared to handle these situations (McNeil 2011).

Another way of increasing security is by looking at the importance of reducing third-party risk and understanding their security posture. Sabino, (2020) states "*Ask questions to identify their potential exposure areas, technical controls to data and systems, network segmentation practices and authentication tools used.*"

There are many different methods an organization can implement to improve their resilience, and the choice of methods may depend on the organizations themselves. By looking at different practices used in different organizations and sectors and how they conduct their method, we can look for patterns.

Figure 6 shows "The *identified practices for smart airports have been categorized into three main groups: i) Technical; ii) Organizational and iii) Policies and Standards.*" (Lykou, G, et al. 2018)

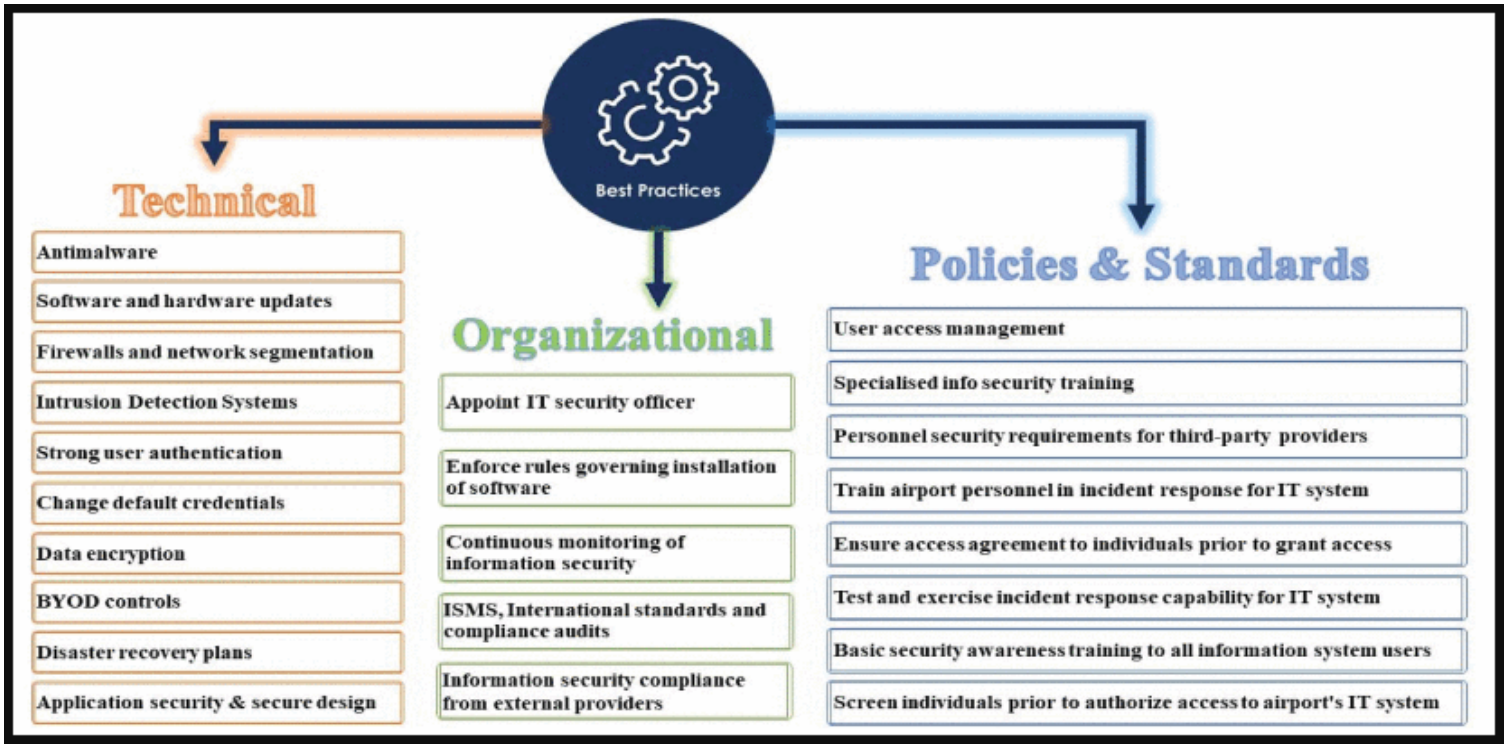


Figure 6: Cybersecurity Good Practices Classification (Lykou, G, et al. 2018)

Figure 6 shows an example of a smart airport. It shows clear goals for the several aspects within the airport, and while some systems and functions may be specialized for airports, much of these best practices are used in many organizations, such as disaster recovery and incident response for IT systems. This is an example of how looking at practices in other sectors may help uncover improvements that can be used in other sectors such as the energy sector.

Physical security is an essential part that proves to be a critical element in maintaining the security of the Energy sector (Weingart, H. 2000). The location of Data centers and distribution sites could prove sensitive and will require protection. Bailey, Maruyama, & Wallace (2020) stat that

"*Access panels for wind turbines are sometimes left unsecured, allowing attackers physical access to both internal device controls and a segment of the broader OT (Operational Technology) network. Recent security research at a wind-turbine farm indicated that physical vulnerabilities (an easily picked lock) and a lack of*

network security allowed researchers to traverse the entire wind farm's network within minutes—with access privileges that would have enabled them to cause anywhere from $10,000 to $30,000 of revenue losses per hour or even destroy the turbines entirely."

Maintaining security is not just performed on a company level but on a national level as well, where different priorities can provide great benefits to maintain security and resilience such as the priorities stated in Nickolov (2006).

"*1. Establishing a national cyberspace security response system.*

2. Developing a national cyberspace security threat and vulnerability reduction program.

3. Creating a national cyberspace security awareness and training program.

4. Securing government systems.

5. Strengthening national security and international cooperation on cybersecurity."

3.0 Research Approach

The objective of this study is to investigate and gain a better understanding of what characterizes resilience in CIS within the energy sector, how to achieve resilience in this area, and how organizations manage to increase awareness of their employees. To address that, the study introduced the following two research questions:

- *RQ1:* What are the characteristics of resilient critical infrastructures within the energy sector, and how can this be achieved?
- *RQ2:* What are the best practices used to achieve resilience within the energy sector, and how are they carried out to increase the awareness of their employees?

This chapter represents the chosen research approach for the thesis which is shown in figure 7 and illustrates how the process of doing research and creating research questions goes through several steps of research progress. The first step is to design an interview protocol, based on research questions, and identify what question needs to be asked to potentially answer the research question. The next step is data collection where information gathered from interviews is used to provide data.

Which moves into the last step, where data analysis is performed, and where potential answers to the research question can be discovered.
We will consider any ethical or validity issues during each step.

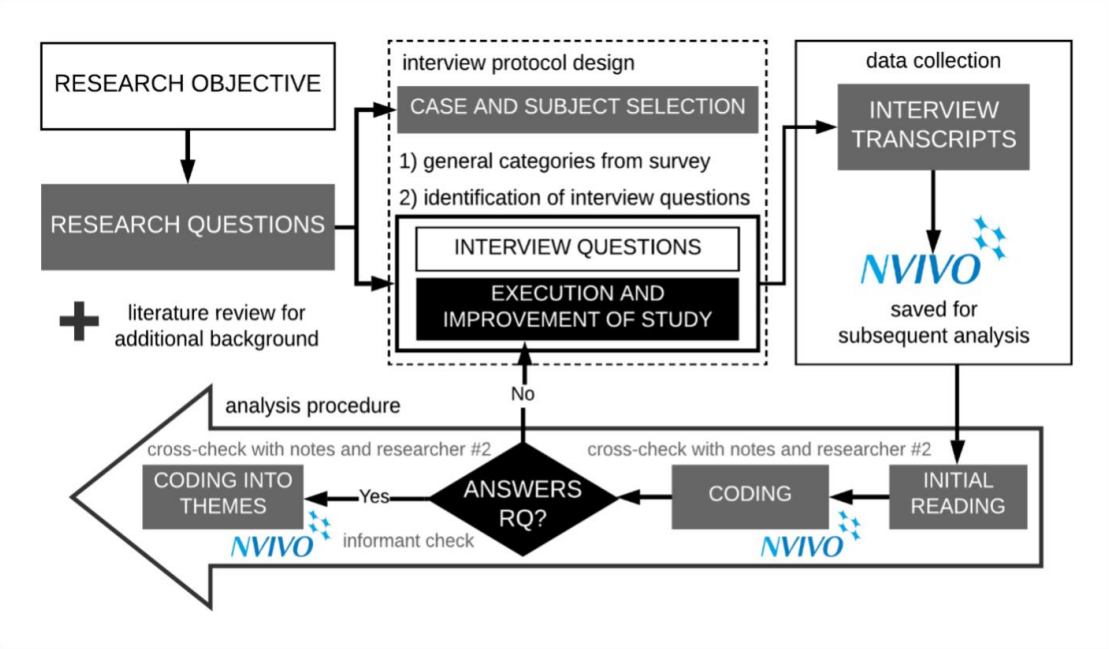


Figure 7: Research Process based on Thomas (2006), Cruzes & Dybå (2011), Berg et al. (2020), Andersen & Pettersen (2020).

3.1 Qualitative approach

The term qualitative research can be used in many forms of methods or techniques, each with its own benefits or challenges. It does however have a common goal, and that is to explore and examine a person's experience in detail, using different methods to achieve this. This method could be interviews, observation, content analysis, biographies, focus group discussion or visual method. (Hennink, M., Hutter, I., & Bailey, A. 2020).

Taking a few examples on how to achieve qualitative information we can use interview, where conducting an interview with an employee within the energy sector related to the power grid. The interview subject can provide experience, personal opinion and information regarding power grids and problems that can occur, and what they do to prevent it or what they lack in order to mitigate it.

Another method could be observation, where you follow a person around their work environment without interacting with the employee, gathering information by looking and listening, allowing them to collect data as it is happening rather than through someone else's opinion or emotions (Kolb, 2008).

3.2 Quantitative approach

When using a quantitative approach to gather information, there are some methods that could be used in this research, such as data analysis or desk research. While both methods are similar in that they both take a lot of raw data and analyze it, there are some differences in the two methods. The data analysis would consist of Strengths, Weakness, Opportunities, and Threat analysis (SWOT), where the goal would be to get a better understanding of power grids and information to use in this report (Tugrul 2016). The desk research is simple to look at the information that is out there, such as data on the internet and government/non-government sources. (Quantitative Research: Definition, Methods, Types and Examples)

While a quantitative approach is good for collecting substantial amounts of data, it can as well be a challenge in itself. How much data do you need to consider it viable, if using questionnaires, how many participants is enough, and can you still use it if the amount is smaller than you expected?

3.2.1 Qualitative VS Quantitative

In the book "Qualitative Research Methods" written by Hennink et al. in 2020, they state that the following difference between qualitative and quantitative research can be summed up by following some key differences.

Table 8: Qualitative VS Quantitative aspects (Hennink et al. 2020)

	Qualitative research	Quantitative research
Objective	To gain a contextualized understanding of behaviors, beliefs, motivation.	To quantify data and extrapolate results to a broader population.
Purpose	To understand why? How? What is the process? What are the influence or context?	To measure, count or quantify a problem. To answer: How much? How often? What

		proportion? Which variables are correlated?
Data	Data are words (called textual data)	Data are numbers (called statistical data)
Study population	Small number of participants; selected purposely (non-probability sampling)	Large sample size of representative cases.
Data collection methods	In-depth interviews, observation, group discussions.	Population Surveys, opinion polls, exit interviews.
Analysis	Analysis is interpretive.	Analysis is statistical.
Outcome	To develop an initial understanding, to identify and explain behavior, beliefs or action.	To identify prevalence, averages and patterns in data, To generalize to a broader population.

These key differences can further validate our choices for the selected method we choose, by looking at what type of information we want, and what method can provide it.

3.3 Research design

Depending on the information needed to provide knowledge to the research question, a method should be considered to best provide this information. The goal of this study is to find out about resilience in the energy sector, practices used to implement it, and how this can increase awareness among employees. As shown in sections 3.2.1 the various aspects of qualitative and quantitative, this helps us determine which method is best to get the information needed to find a potential answer to our research question. In this case we look to identify what information exists that can be used to improve certain aspects of the energy sector, and the

behavior of people towards these improvements. The method chosen for doing the research will be performed through qualitative methods, as we seek to investigate how people respond to new events that could affect their daily routine.
"*Qualitative research is the systematic inquiry into social phenomena in natural setting*" Teherani, A. et al. (2015).
These phenomena can be about people's experiences, how an individual or a group behaves, and how the organizations function. The research allows for the examination of what happens, how it occurs, and what these are meant to the people involved. Teherani, A. et al. (2015). Using qualitative data, we can learn more, and better describe the phenomenon, by providing a more detailed insight to the participant, and the world they experience. Hoepfl, M. C. (1997).
Thus, using a qualitative interview is considered both the most common and important method for gathering data. Myers, M. D., & Newman, M. (2007).
When it comes to the purpose of the research Robson classified four diverse types (Berg et al., 2020; Robson, 2002):

- Exploratory - Understanding what is happening: to seek new insight.
- Descriptive - Portraying a situation or phenomenon.
- Explanatory - Seeking an explanation of a situation or a problem, mostly but not necessary in the form of a causal relationship.
- Improving - Try to improve an aspect of the studied phenomenon.

In this research work, the context of our interviews, and the goal of our research is to look at potential factors that can help increase resilience within the energy sector.
The result is that this is an exploratory study.

3.4 Research subject Selection

Subjects were collected primarily through NC-Spectrum who worked as a medium between us and other organizations, a minor few were contacted directly by us. We provided NC-Spectrum with a brief list of criteria of the type of informant we were after, as well as a maximum number of respondents per organization.
The people we contacted and interviewed were limited to three members of the organizations and had to fulfil one of the three different categories.

1. They have some sort of leadership role within the organization.
2. They have some sort of responsibility for IT and Cybersecurity.
3. They have other responsibilities within the organization where IT/Cybersecurity is less of a priority.

several organizations were contacted about being interviewed for this study. We managed to get 7 different organizations that were willing to be interviewed. The pie chart shows the general fields the organizations work inn. Several of the organizations do function in more than on field.

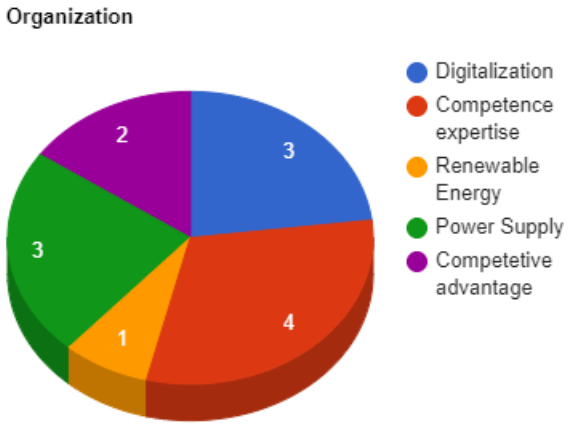


Figure 8: Organizations fields

Table 9 shows the general profession of our 11 respondents that fulfill the criteria and area that they are representing.

However, to ensure that the informant to be anonyms the category “Area” of the table below, is a looser description of their job area, Therefore the “Area” represents a “sum up” part of their work. Our informant was divided among who had more technical background, and those who had a more organizational background, while this is a particularly good balance, this has also led to some questions were not or insufficiently answered due to lack of knowledge in the specific questioning, depending on background.

Table 9: Interview's object

ID	Profession	Area
1	Leadership	IT security
2	Leadership	IKT
3	Leadership	IKT
4	Leadership	IKT
5	IT/Cybersecurity	IT security
6	Leadership	IT security
7	IT/Cybersecurity	IKT
8	IT/Cybersecurity	Consulting
9	Leadership	IKT
10	Leadership	IKT
11	IT/Cybersecurity	Consulting

We were determined from the beginning to ensure anonymity to our respondents as well as the organizations we contacted. The reasons for this are that we investigate sensitive areas of the organization, and we also investigate what aspects of certain security or resilience practices do not work or function optimally within the organizations. Therefore, anonymization was of high priority to us, to ensure that our respondents were comfortable answering as honestly as they could without negative consequences.

3.5 Data collection

When it comes to qualitative interview questions there are three different forms of interviews one uses to gather information. Structured, unstructured, and semi-structured interviews.
Different types of methods have their advantages and disadvantages, depending on what you are after concerning information.

Structured interviews are when the questions are planned and non-deviant, the interviewer all asks the same question in the same order, and the interviewee must

answer just the question. This is usually what is used in job interviews when you are comparing the different interviewees with each other (Myers, 2007).

Unstructured interviews are the opposite of structured interviews where the questions are not planned. This results in more open and spontaneous questions, and different interviewees may get different questions. This is a more personal approach, and the interviewee can answer freely. This method is good to get experience from an individual (Myers, 2007).

Semi-structured Interviews are a combination of the other two, where a few pre-made, questions are asked to get the interview going, but interviewers can ask off-scripted questions, and the interviewee are free to answer as they please (Myers, 2007).

3.5.1 Semi-Structured Interviews

Geoff Walsham, (2006) mentions that interviews are used very commonly in most studies and are an essential technique for gathering data. While both unstructured and semi-structure are a variable method for conducting interviews in our research, this study has chosen to use semi-structure to both have the possibility to ask about existing issues, and solutions, as well as still having an open interview where we can learn more about the employee personal experience. In addition, a semi structured interview will have a list of questions but the sequence of asking those questions is flexible. This could lead to us having the opportunity to talk or ask about other subjects that are related to the study and could create other categories that might assist in broadening the analysis. If you do not slip out in relation to the topic and time you have available, this is entirely possible in this form of interview (Myers & Newman, 2007). Furthermore, Semi-structured interviews could allow researchers to understand how individuals interact and react to their context, but reduce the risk of bias as well (Iyamu, 2018; Tsan, 2014; Marshall et al 2015). Another reason this method was preferred was that we needed to define some questions that could be used to further understand our knowledge about the area of interest and to confirm or disconfirm some aspect about our research problem. In addition, using the semi-structure method allows us to learn more about the interviewee's own experience,

opinions, and perception and how they viewed the work tasks. Furthermore, a semi-structured enables the respondents to speak in a free form and then later we can ask for more specific details, where we feel that a more concrete answer is required. Having this form of qualitative approach will increase the amount of information we could get that could help answer our research question.

In order to ensure this procedure was accomplished correctly, we decided to follow a review paper "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide" by Kallio et al. (2016) on how to set up an interview guide using semi-structured interview.

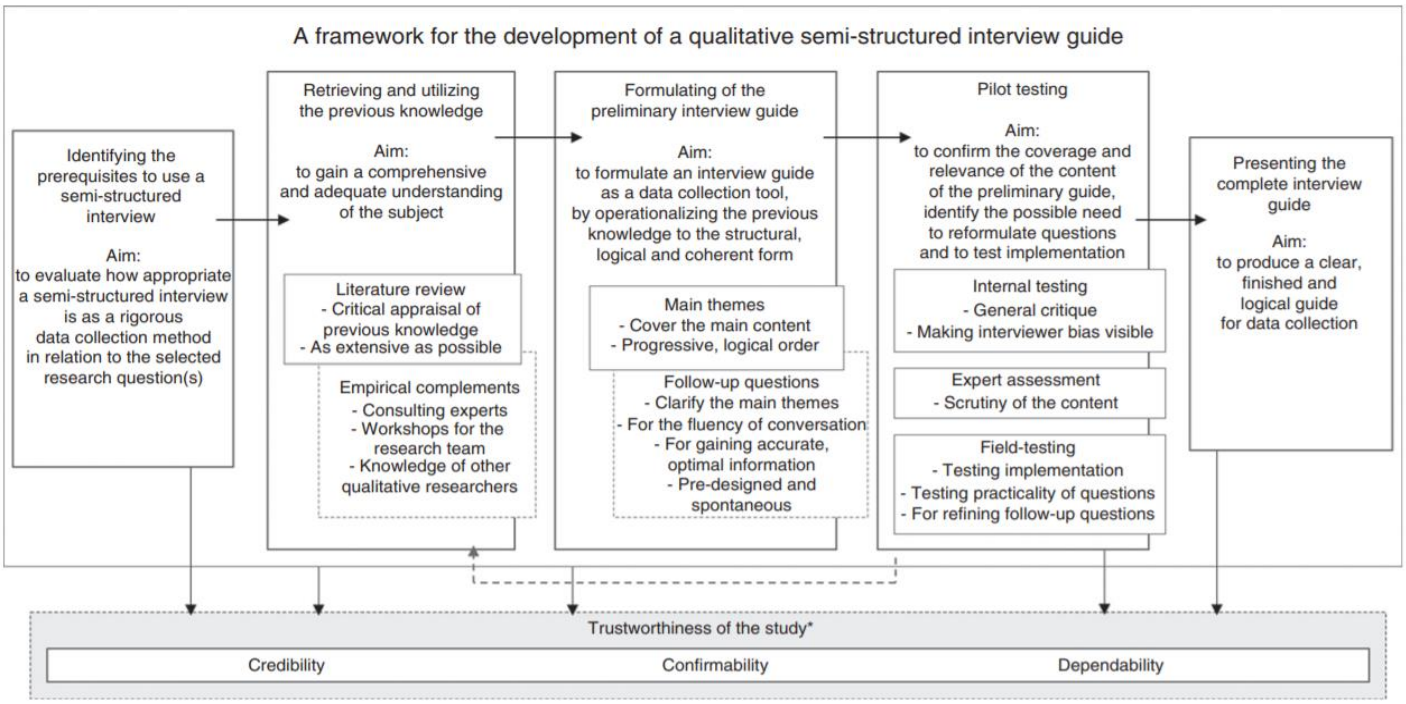


Figure 9: Framework for development of a qualitative semi-structured interview guide (Kallio et al. 2016)

By following a developed framework, we can further justify how and why we use our method and ensure that our interview questions are relevant to the research questions.

Several of these goals have been met previously within this paper, and we intend to follow this guide as closely as possible, however considering work and time limits some aspects may not be able to be completed or used within this paper. These limitations were mostly on refining the research questions and having some testing to see how well formulated they were for a potential research subject.

The interview will open with a brief introduction to what we are trying to accomplish here, and then inform the respondents about data processing and consent (See Appendix 4: Consent Form). We made the questions both in English (shown below) and Norwegian (Appendix 1: Interview questions in Norwegian). Which one will be used will be decided by what the respondent is most comfortable with? The following questionnaire was used for the data collection procedure.

The semi-structured interview will allow us to ask follow-up questions at each phase about anything we might find relevant to the study or if we identify something that needs to be explained in detail. We decided to have both researchers in each interview due to the following reasons:

1. enables direct contact with the respondents.
2. creates a demanding first-degree data collection technique.
3. one of the researchers could produce a relevant question the other did not think of (Runeson & Höst, 2008).

Lastly all interviews have been recorded and transcribed so that we can provide data for the analysis stage.

3.6 Limitations of interviews

When using interviews regardless of form and structure there are some limitations that can affect the outcome. There is also a possibility that differences in social and cultural understanding can shape the interview. (Fontana and Frey, 2000) Myers & Newman point out that there are several other aspects that could become potential problems when conducting interviews such as (Myers & Newman, 2007):

- Lack of trust - when an interviewer is a stranger, and the interviewee may have doubts about how much they can trust the interviewer and may not want to give out certain information they consider sensitive, which can lead to the data gathering being incomplete.

- Constructing knowledge - interviewers may think that they just absorb the data or information that is already there and may not realize that they are

actively constructing knowledge. (Fontana and Frey, 2000) This can happen when an interviewee responds to a question, they never have considered before, and reflect on the issue, while the interviewer takes this reflection and makes it into something that is logical and consistent, but not what the interviewee reflected on.

- Ambiguity of language - words can often be ambiguous, and what the interviewer asks, may not be what the interviewee hears, and vice versa, as such misunderstanding can occur during an interview. (Fontana and Frey, 2000)

- Specific targets, that may be limited in number and availability for interview, such as having a specific group, in a certain area, where not all may be valid for interview.
  In our research work we interview members within CIS, therefor there may be a limited number on how many interviews object that are willing to share experience with us.

Using qualitative methods can be an extremely useful tool for gathering data but understanding the limitations and pitfalls of using such interviews is important to be able to use it to its full potential. (Myers & Newman, 2007) When we go forth with the interviews these limitations and others such as the Hawthorne effect or elite bias are necessary to be aware of, to best avoid them.

"*The qualitative interview is a powerful tool, but those using it should have an appreciation of its strengths and weaknesses.*" (Myers & Newman, 2007, p5)

The limitation above was analyzed and together with the supervisors found ways to deal with them. To build trust between the interviewer and the subject, an interview guide and consent form were created and handed to every subject. The guide and consent form gave the subjects information on how any data given then will be handled, stored, and deleted. In addition, everything they said will be anonyms and cannot be tracked back to them. The interview subjects then knew what they were signing for and had time to prepare for these interviews. To avoid misunderstanding both interviewers and interviewees agreed on that, anything that is not

understandable should be highlighted to make sure there are no misunderstandings. In addition, there were two interviewers in every interview to make sure that if there were any misunderstanding, one of the interviewers would notice it. Lastly, the specific targets were our biggest concern due to covid 19 and the number of targets available for interviews. This was addressed by asking NC-spectrum and our supervisors to assist with finding the specific subjects we could interview. However, this limitation was not addressed to a satisfactory level, seeing how we managed to have 11 interviews when the goal was to conduct 15.

3.7 Data analysis

This study looked at a variety of data and analyzed them structurally. The analysis was based on interviews, where we wrote down notes during the meeting, as well as going through the recording of the interview and transcribing for further analysis. In addition, the analysis of result data was performed in an inductive approach where we had decided to explicitly use the form of thematic analysis (Thomas, 2006). A general inductive analysis approach contains three objectives (Thomas, 2006)

1. Summary format is created from raw data.
2. Text is familiarized with, and an understanding of themes and events is gained.
3. Create categories that can be subdivided into new categories/themes each with its own segment of data.

Thomas, (2006) mentions that there are some fundamentals to how a general inductive approach is carried out. The analysis starts by having evaluation objectives guiding it, however having multiple readings that interprets the raw data will satisfy the inductive component. Focus will then be provided by the objectives, but no expectations about findings. Additionally, the researcher will then develop a model containing themes and processes which is taken from categorizing the raw data. Later, the findings will then be framed from the researcher's perspective, by arriving at results from the several interpretations that have been finished. That is when decisions will be taken from the researcher about the importance of inadequacy of the data. Furthermore, the researchers could end up with findings that are distinct

and not overlapping each other. Lastly Thomas, (2006), mentions that the trustworthiness of this type of analysis evolves from other qualitative analysis.

The combination of inductive approach with the thematic analysis will attempt to answer our research questions by providing a model of themes and events that will describe what characterizes resilience in CIS and how do they achieve it. The NVivo software given to use by the university will assist in analyzing and coding the data we will gather. An explanation of the analysis procedure is shown below.

Initial reading:
We will start by having the raw data files cleaned up, and then start reading it so that we can find patterns and get some general ideas. In addition, during the interviews one of the researchers (us) will be taking notes that might help during the initial reading phase.

Coding Process:
We plotted our transcriptions from the interview into NVivo, from there we could code each section of the interviews with the corresponding answer from all respondents to that section. Through this process we could compare similarities and differences of each informant to the related interview question.

Coding into themes:
After that we coded our transcriptions, we started to code into themes to avoid having to use terms that were too general. This made it easier to find specific phrases or keywords to further clarify what our respondents had said.

Translation
The interviews were conducted in Norwegian with all respondents, The information gathered from this interview were then translated into English. The quotes are translated to be accurate conveyed from Norwegian to English.

3.8 Validity

When it comes to qualitative research validity, usually the researchers refer to qualitative research that is plausible, credible, trustworthy, and defensible. Johnson (1997). Stated, “We believe it is important to think about the issue of validity in qualitative research and to examine some strategies that have been developed to maximize validity” (pg. 282). For our study to be trusted the validity of it must be considered, which is why we decided to use the qualitative research validity of Johnson (1997). There are several strategies that can be used in qualitative research validity such as extended fieldwork, triangulation, reflexivity which is shown in table 10.

Table 10: Strategies used to promote qualitative research validity (Johnson, 1997)

Strategies Used to Promote Qualitive Research Validity

Strategy	Description
Researcher as "Detective"	A metaphor characterizing the qualitive researcher as he or she searches for evidence about causes and effects. The researcher develops an understanding of the data through careful consideration of potential causes and effects and by systematically eliminating "rival" explanations or hypotheses until the final "case" is made "beyond a reasonable doubt." The "detective" can utilize any of the strategies listed here.
Extended fieldwork	When possible, qualitive researchers should collect data in the field over an extended period of time.
Low inference descriptors	The use of description phrased very close to the participants' accounts and researchers' field notes. Verbatims (i.e., direct quotations) are a commonly used type of low inference descriptors.
Triangulation	"Cross-checking" information and conclusions through the use of multiple procedures of sources. When the different procedures or sources are in agreement you have "corroboration."
Data triangulation	The use of multiple data sources to help understand a phenomenon.
Methods triangulation	The use of multiple research methods to study a phenomenon.
Investigator triangulation	The use of multiple investigators (i.e., multiple researchers) in collecting and interpreting the data.
Theory triangulation	The use of multiple theories and perspectives to help interpret and explain the data.
Participant feedback	The feedback and discussion of the researcher's interpretations and conclusions with the actual participants and other members of the participant community for verification and insight.
Peer review	Discussion of the researcher's interpretations and conclusions with other people. This includes discussion with a "disinterested peer" (e.g., with another researcher not directly involved). This peer should be skeptical and play the "devil's advocate," challenging the researcher to provide solid evidence for any interpretations or conclusions. Discussion with peers who are familiar with the research can also help provide useful challenges and insights.
Negative case sampling	Locating and examining cases that disconfirm the researcher's expectations and tentative explanation.
Reflexivity	This involves self awareness and "critical self-reflection" by the researcher on his or her potential biases and predispositions as these may affect the research process and conclusions.
Pattern matching	Predicting a series of results that form a "pattern" and then determining the degree to which the actual results fit the predicted pattern.

Our goal here is to combine several strategies mentioned such as reflexivity and data triangulation, where the researchers will focus on self-awareness, "critical self-reflection" and control biases while using multiple data sources to help understand a phenomenon. Johnson (1997) describes how researchers must be careful and beware of one potential threat that is called researcher bias. This was mentioned to him by a colleague of his where she stated, "the problem with qualitative research is that the researchers find what they want to find, and then they write up with their results" (Johnson 1997 pg. 283). Therefore, it is essential for this study that the mentioned strategies are performed and include a peer review as the last strategy where interpretations and conclusions of the researchers will be discussed with others. The supervisors that follow the researchers during the semester will play the "devil's advocate" role where they challenge the researchers to provide solid evidence for

their interpretations or conclusions. This will help in gaining useful insights where it is relevant. In addition to the strategies chosen the study will assess the five main validity types: Descriptive, interpretive, theoretical, internal, and external validity that Johnson (1997) mentions in his paper which goes as follows.

- Descriptive validity: refers to the accuracy of the information that is reported. We start by having one researcher taking notes which later will be compared with the transcriptions. Additionally, we decided to use investigator triangulation where multiple observers will be attending the interviews so that they could cross-check observations and make sure the interviewer and the respondents are on the same page.

- Interpretive validity: refers to which degree the respondents' thoughts, feelings, intentions, experience, and the researchers understand viewpoints. Here is where we attempt to get inside the heads of the respondents to gain an understanding of what they see and feel.

- Theoretical validity: Is to validate through theoretical explanation form where the research fits the data. One should also look at cases that do not fit the explanation, to ensure that all aspects are investigated to ensure credibility. This research work performs it by looking at prior research and verifying our findings against them.

- Internal validity: By looking at cause and effect and their relationship a researcher can study how certain processes function/develop. The validity comes from looking at a phenomenon and investigating all potential reasons why it occurs and ruling out any other rival explanation. Thus, looking at if the causal factor occurs, does then the effect follow, and make sure that there are no other variables that are the reasons for the relationship.

- External validity: The primary goal of external validity is to generalize the information gathered from research, to make the information easy to replicate the research study, by providing certain information such as

number and type of people, selection method, relationship between researcher and participant etc. The more information about how the data was gathered, makes this easier to replicate.

3.9 Ethical Considerations

As mentioned, dealing with critical infrastructure, and gathering information about this can lead to findings that could be considered confidential by the companies we are investigating. After a thorough discussion with our supervisors and clients, it was decided that this study does gather sensitive data. Every interviewer was informed about their right to revoking their consent that could happen at any time. Additionally, we decided to look at what type of data was gathered from the interviews and once the analysis and findings have been written, the respondents would get a copy where they could read it and give their consent before it is published. Additionally, the researchers have been provided encrypted and safe cloud storage by the University of Agder to store all the interview recordings and transcripts. Another factor we had to consider was the Covid-19 pandemic that still is afflicting the country, which led to having physical interviews being canceled. It has been made clear by the professors that the GDPR legislation usually requires the interviews to be conducted in a physical and offline environment where the device used to record the interviews must not have any network connectivity. However, the social distancing rules and the fact that most people have home offices for the time being forced us to find other solutions. Therefore, the interviews had to be conducted through the internet in the form of online interviews. Both Zoom and Microsoft team's platform were used to carry out the interviews, as we have experience pre hand using these tools. In addition, some respondents from past experiences were more comfortable/known to use one of these tools, therefore we decided to provide the option of using both. The software's comes with encryption technologies and is safe to use for our data collection.

4.0 Empirical Findings

The empirical findings have been categorized and presented based on the structure of the literature review and the structure used for the interviews, as shown in Figure

10. The coding of all interviews followed the same structure, and the results are presented as sub-categories.

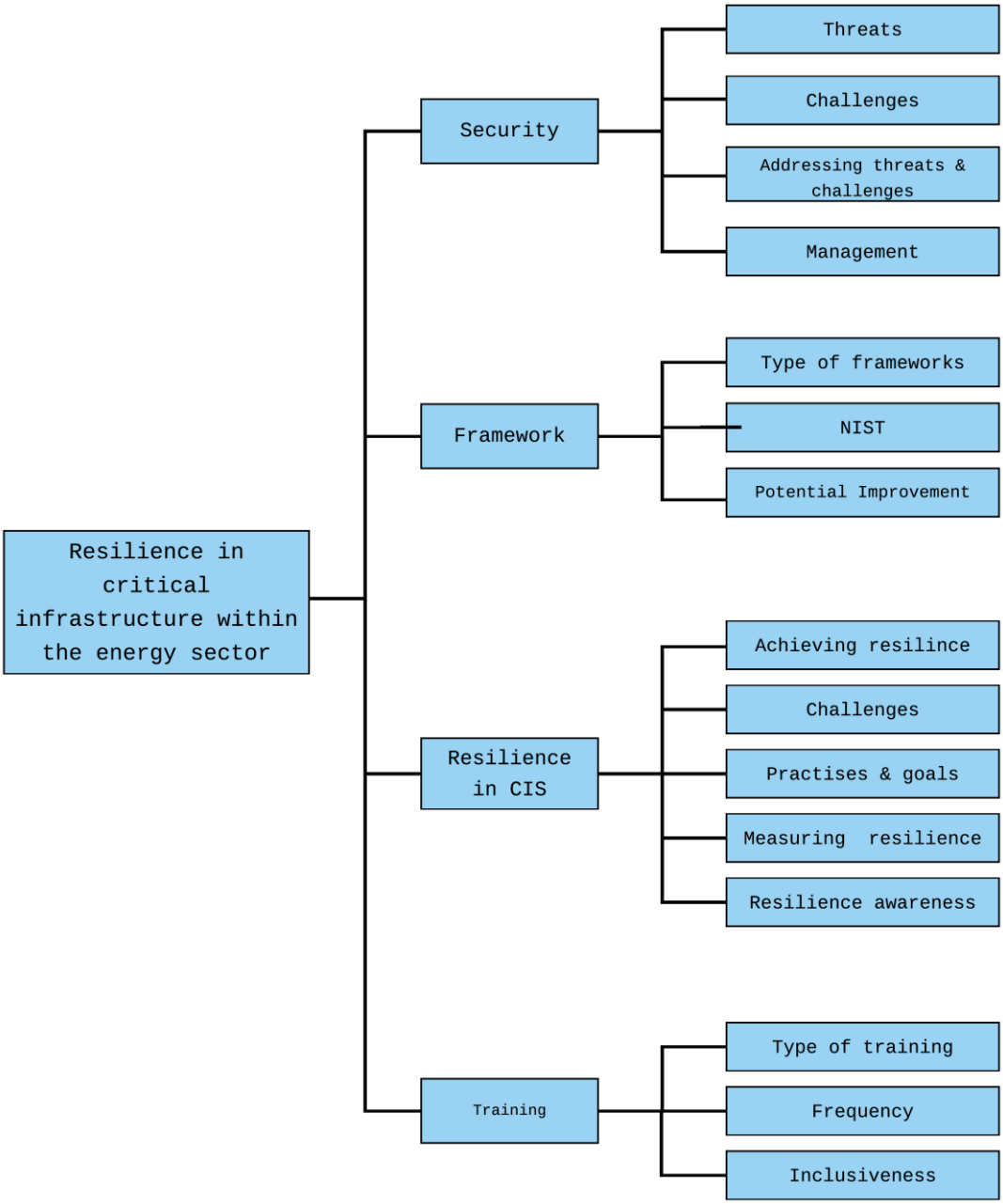


Figure 10: Resilience in critical infrastructure within the energy sector

4.1 Security Findings

Our goal of the security findings was to investigate what threats and challenges exist for the energy sector and what were the typical measurements used to counter these potential issues. All 11 respondents were at some level involved with security, either directly or as part of their role in the organization.

These sections are divided into four subcategories and provide some in-depth information about the key factors, as perceived by how the respondents viewed threats or challenges to their organization, and the energy sector. These subcategories aim to see what the common aspect between the respondents is, and what differs between them.

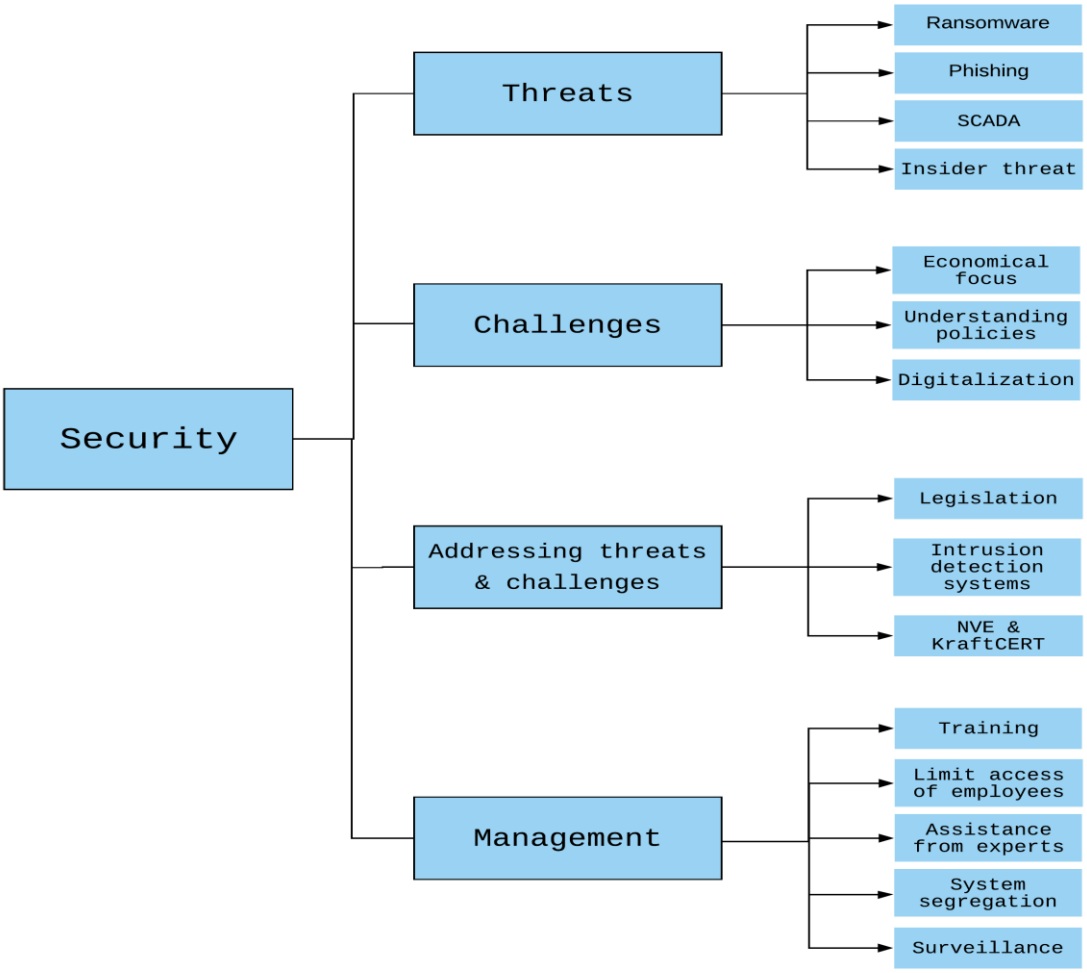


Figure 11: Security within the energy sector

4.1.1 Threats

All our respondents were familiar with the types of threats that exist within the energy sector and most of these respondents worked within that area to prevent these threats from causing unwanted damage to their systems. The majority of those who responded mentioned that the CIS and the energy sector are facing many different threats today and the outcome of these threats varies, however they all need to be addressed.

9 out of the 11 respondents mentioned that the energy sector in Norway uses a system called Supervisory Control and Data Acquisition (SCADA) to monitor and control their infrastructure. One of the threats they have is the connection of different systems that they call SCADA systems. The parts of those systems where the functionality is easy and very straightforward are called easy S systems, other parts of the systems are more difficult to operate based on how old they are. This creates an unwanted threat for the energy sector where they must build security for both systems. I7 & I8 also mentioned that the critical systems they have are isolated from the outside world and adding direct updates to a SCADA system are difficult and require more than just stopping and restarting the servers. In addition, if someone gains access to this system, they could start manipulating data in the system and affect the power plants in a harmful way, among others by increasing the voltage while everything looks fine in the control room. Furthermore, 5 out 11 specified that other threats have emerged and made the energy sector a target due to the following reasons:

1. The energy sector operates with a lot of power-sensitive and valuable information.
2. They have personal-sensitive information that contains customer data.
3. Having unauthorized people gaining access to systems will jeopardize the integrity of both their system and the deliverance of energy.

When asked about the other threats, I1 and I5 focused on both traffic monitoring and state-sponsored threats. It was mentioned that traffic monitoring of the data moving in between the endpoint and into the systems is important to secure. Unauthorized persons cannot have access to, or any control over this data, because if it is read there is room for printing. Room for printing could let them manipulate the data which could have significant consequences for the national infrastructure. The ability to deliver is a threat that was mentioned by several respondents. The energy sector relies on other organizations to deliver software and hardware components to them. I2 and I3 spoke about how the energy sector's ability to deliver could be accidentally or intentionally affected by the components they get and use. While the chances of that happening are small it is still a critical vulnerability that they need to address. Security roles and insider attack is described by four of our respondents as a typical threat the energy sector is concerned about.

Employees capable of performing a malicious attack can easily do this when they have authorized access and broad knowledge of the system's architecture and policies/procedures.

Out of the 11 respondents, 10 of them mentioned the most common threats the energy sector faces are ransomware and phishing. According to I1, various threat actors attempt at installing ransomware and other types of viruses or scripts to gain access to exploit the system, threat actors then ask for ransom or simply destroy or manipulate data. Moreover, it was explained that these threats such as phishing attacks are not aimed at certain people, but at the whole organization itself. I5 explained.

"They are looking for general attacks and just spam the employees with phishing emails and see if someone falls for the trap. However, what we are most concerned about is that we get exposed to ransomware. Knowing that if we become a victim of ransomware, the recovery from that is possible, but will be challenging regardless of the amount of training and security measurements we take."

The threat profile in the energy sector is getting more complex and tougher to manage. 5 out 11 explained that criminal organizations, cyber espionage, insider attacks, and state-sponsored actors are constantly trying to infiltrate their systems by using different methods and tools to stay ahead of the curve, which in return makes it difficult for organizations in Norway to keep up.

4.1.2 Challenges

When it comes to challenges, 5 out 11 have experienced that getting economic focus on getting the right tools and resources to protect their systems is inadequate, due to management's lack of interest and knowledge of cybersecurity. The energy sector has policies and procedures just like any other organization, and I10 referred to getting employees to understand and follow these policies are a challenge. Another challenge the energy sector faces today is how they can relate to legislation provided to them. I5 mentioned that the legislation could be interpreted in separate ways and in some cases, it is very general. Using a combination of legislation and other policies does help, however, it does not completely address the challenges. I6 further added that these policies sometimes are unknown to the employees or otherwise not followed as they should be.

One of the biggest challenges in the energy sector is digitalization. 7 of the respondents mentioned that digitalization is one of the main goals in the energy sector today. The demands for *digitalization* and making the systems more available are increasing.

I1 explained "*I want to say that at the same time as digitalization is fantastically exciting and that makes us move forward, it is digitalization that is the challenge. It goes incredibly fast and with that, safety must be increased. It may be that we are a bit behind and then there is also the fact that the threat actors are lightning fast to develop which demands organizations to be more robust and be more resilient to be able to either resist or handle incidents.*"

4.1.3 Addressing Threats and Challenges

When it comes to how the organizations, in this study, address their security 3 out of 11 explicitly mention they use "kraftberedskapsforskriften[4]" (KBF) and another 2 out of 11 mention it indirectly. The term "kraftberedskapsforskriften" is something that all our respondents have confirmed to use in their organization. They talked about how the KBF provides guidelines that can be followed to best handle security challenges.

7 out of 11 talks about the different technical measurements such as Intrusion detection system (IDS) or having some e-mail filter or having secured the traffic of information with encryption.

All respondents mentioned the use of third-party organizations such as KraftCERT or NVE to assist them in alerting and monitoring their traffic or data.

A recurrent theme in the interviews was a sense amongst interviewees that most of the organizations do believe they have a decent or proficient level of measurement, and there is a high trust factor towards these third parties to be a beneficial impact. Based on the information gathered from the respondents, there are some consistent similarities of tools used between them to ensure measurements. Such as aid from third parties and the use of technical solutions like monitoring to help address security challenges.

[4] the power contingency regulations

4.1.4 Management

When it came to the organizational aspect of their organization and what they do to maintain or increase security 6 out of 11 talked about implementing training for their employee, and communication within the organization to manage and maintain the security of the organization. I9 and I10 mentioned that hiring people or consultants to provide the necessary competence is one of the things they do to ensure they are on the right track. This indicates that having people with an understanding of security and what to look for of potential threats is a high priority to many of our respondents and their organization. I3, I4 and I5 talked more about making sure that the network, system, firewall, etc. was able to provide the security needed to avoid any potential threats, by limiting unnecessary access of employee, having some restricting on login to system, making sure that people who should not have access to sensitive information does not get it to mention some. In addition, I1 and I8 further mentioned use of third-party organizations, to assist in following up the organization and to assist in making sure that they get the supervision they need to maintain security.
Two discrete themes emerged in our interview group, whether you change the people to improve the system or change the system to improve people. This is expected to be about the background of our respondents, rather than a reflection on the organization whole.

When it comes to the technical aspect 7 out of 11 informed that there is a great focus on IDS detection and firewall to check for unwanted events, where some of the employees use the system or login incorrectly an alert is triggered and reported. Thus, even if many of these are false positive, they do show that the system can detect them.
Three respondents, I1, I8 and I11 mentioned that using or contacting third party organizations to assist in the technical aspect was beneficial, by helping with monitoring, logs or uncovering potential solutions.

When it comes to what the informant believed was the most beneficial countermeasures I2 and I4 talked about segregation of the system. Where the different systems do not have the same access to certain key switches, or sensitive

information and to make it tougher for an attack program to shut down everything. There was a higher number of respondents who credit technical solutions as the most beneficial countermeasures as well. 5 out 11 talked about surveillance, such as monitoring, logs, or tracking, and that having these implemented proved to be an effective way of checking if the system worked, and that events were caught and handled. For 4 out 11 the most important aspect was raising awareness among employees, teaching them that what they do, can impact the organization, and teaching them to be more alert and notify security personnel if something happens.

While there was an inconsistency with what were the most important key beneficial implementation, a majority (8 out of 11) mentioned to a varying degree, that ensuring an understanding of and teaching security to people or employees because people are considered one the biggest security threats to the organization.

4.2 Framework

The goal for inquiring about the framework and which was used was to see if there was a consistency of what framework was used within the energy sector, and if it were the same as in other countries or places.
During the interviews it was discovered that 5 of 11 of our respondents had limited understanding of their frameworks and what it did, because some could only provide surface information in their answering. Another finding was the lack of knowledge about NIST and its usages among our respondents. However, a very few numbers of respondents were able to give some information on the possible reasons for the lack of knowledge in Norway about NIST.

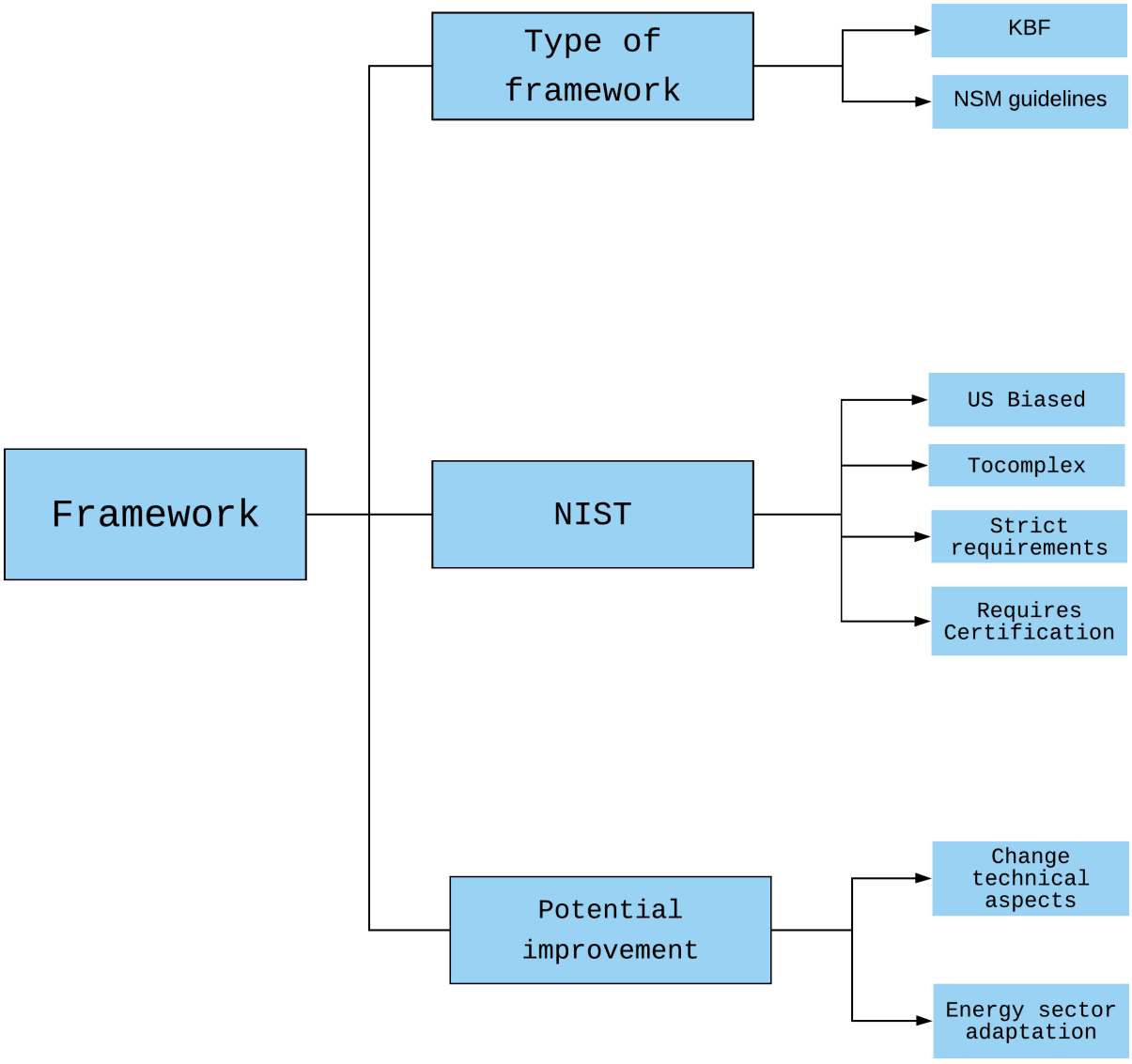


Figure 12: Framework within the energy sector

4.2.1 Type of framework

When interviewing the respondents there was a unanimous agreement on what type of framework was being used within their organization, as all talked about the KBF which is a set of guidelines that an organization follows to ensure that the energy sector is secured. The KBF applies to prevention, handling and limiting events that could harm this sector. While the KBF seems to be the standard for these organizations, it was not the only one used. 6 out of 11 talks about Nasjonal sikkerhetsmyndighet [5](NSM) being used with KBF as a tool for framework, and that they follow some of NSM guidelines, however I1 and I11 talk about how KBF is based

[5] The National Security Authority

on NSM and that many principals are the same. The NSM is a national framework that works on many different sectors, and KBF while based on NSM, is more targeted towards the energy sector. Therefor NSM will have some specific guidelines that are not covered in the KBF. KBF have many similarities with NSM, and that is why they are both used next to each other, and why some of the informant talks about both as if they are one.

There was some talk about how the organizations are subjected to KBF, and not necessarily NSM, where I1, I4 and I6 states that they must follow KBF and that they follow the recommendation of NSM, as a supplement to KBF rather than it being a requirement.

4.2.2 NIST

There was a lack of knowledge about what NIST framework was and what relation it had among all our interviews. Only 3 of the 11 respondents knew if NIST were practiced in their respected sector. I5 mentioned that they knew about NIST and other frameworks, but it was not practiced in their organization. The same informant referred to how NVE does not have any limitation on how many frameworks organizations within the energy sector can practice. They have listed a few that could help with choosing the one that fits the given organization, and NIST is rarely chosen. I7 and I11 explained that NIST is practiced in their organization with the help of NSM, which has managed to create a Norwegian variant of the NIST framework in several areas. The way it works is that the organization itself takes NSM core principles and uses the NIST framework as a reference to address threats, challenges, security management, risk analysis, etc.

4.2.2.1 Why is NIST not implemented?

Several of our respondents were then asked why NIST is not practiced, and they had assorted reasons as to why. 5 out 11 referred that KBF have incredibly strict frameworks for ICT security. I1 specified that the difference between the legislation made for the energy sector are extensive compared to other sectors, and that is one of the reasons why their respected sector does not see the need for implementation of another framework. In addition, 4 out 11 explained there are areas in the NIST framework where the energy sector needs to improve for them to be able to implement NIST. The asset and governance category of the function called identity

shown in Table 6 of NIST is where the energy sector lacks the desired knowledge and control. This makes it harder to introduce a framework such as NIST that is extensive and difficult for an organization of their size to implement. I5 explains that NIST is very Americanized and the NSM fundamental principles in Norway are written so that a person can, hypothetically, read and understand it without having any certification. There are also points within the NIST framework that are better suited for the segments in dissimilar categories, and therefore some organizations decide to combine different frameworks so that it is easier to reach their goal. I5 and I11 highlighted that NIST mention that being 100% compliant with their framework is an impossible task to do, but organizations can become a partner of NIST and seek assistance to reach their goal.
Therefore, several organizations in the energy sector use the framework KBF which are believed to be remarkably similar to both the ISO 27002 and NIST framework. KBF has the following principles.

1. Identify and map.
2. Protect and create.
3. Hold and discover.
4. Manage and restore.

In addition, several respondents mentioned that the European countries have their frameworks made for them and some of them are specially made for Norway, it is more natural to use them. However, there were many ideas and thoughts from NIST, and other frameworks implemented in the European one.

4.2.3 Potential improvement

When interviewing our respondents, we wanted to hear about the framework they were using and if it could be improved or if it was lacking in some areas.
To this question 6 out of 11 did have some perspective on what could be improved to make the KBF/NSM better for the organization. 4 out of 6 talked about how further adaptation toward the energy sector could help in improving the frameworks. The adaptation ranges from making the framework more understandable for people not heavily invested in framework and making it less comprehensive. In addition, making a lighter version for a smaller organization so they could easier handle the

framework. The last 2 of the 6 wanted some improvement on how some of the technical aspects are handled in the framework, such as changing some of the rules on data storing and network access.
The rest of the respondents did not know enough about their framework or did not know what could be improved about the framework.
The main potential improvement of KBF or NSM seems to be the same reason NIST is not used. That some frameworks can be too complex, or too big to be properly implemented in an organization, and making a smaller, easier to handle version, is something that certain organizations want. This is naturally easier said than done and with the complexity of the ever digitalization of our world, making a light version of framework, may not be possible.

As for the NIST framework and what improvements they can make for it to be used in Norway, I2 explains that NIST needs to create a custom version which is more focused on reality-oriented level. The current one is too detailed, and organizations might feel overwhelmed by it. I3 added that the expertise in the field is lacking, and organizations in Norway and NVE should focus on increasing the expertise by offering courses and certifications for their employees in the bigger organizations at the very least. Several respondents mentioned that for Norwegian organizations in the energy sector to use NIST or other frameworks, there must be a specific need that their given frameworks do not cover or address. So far that has not been a problem.

4.3 Resilience of the CIS

During the interview, we looked to see if the term resilience meant the same for all respondents or if there were some who understood that term differently. While there were some differences in how they explain it, the general understanding of the term resilience was similar among our respondents. We additionally discussed how respondents viewed resilience within their sector, and 11 out of 11 said that the level of resilience is good or above good, however the reasons did vary from informant to informant. 4 out of 11 give credit to technical reasoning for satisfactory level of resilience, and another 4 out 11 give credit to improved security teaching to employee and understanding of threats and what to do or who to contact, as their reasons for why resilience in the energy sector is good. I7 and I8 consider resilience as something

that is for the entire organization, and only when everything is taken into consideration, can you know if what you have is resilient or not.

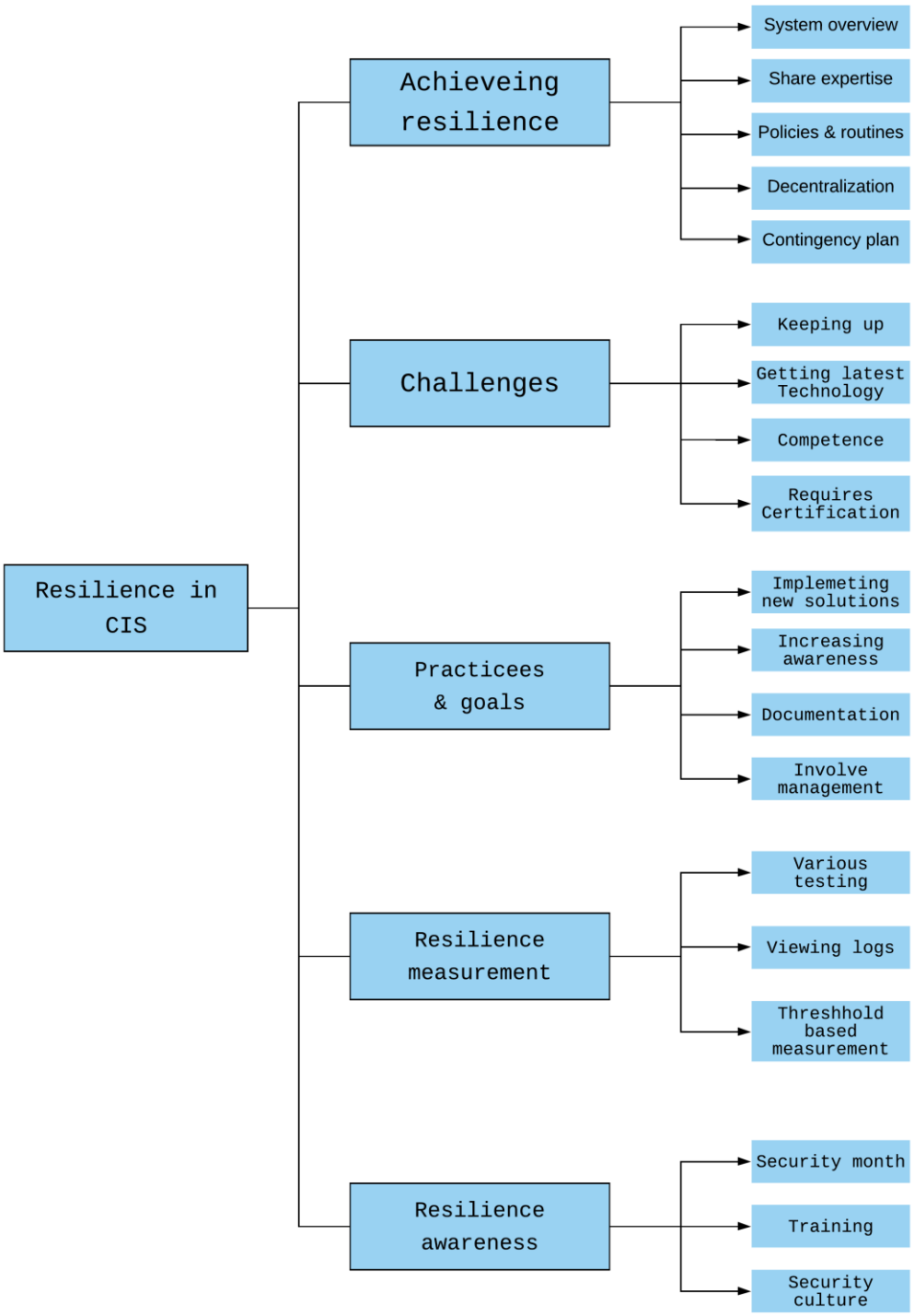


Figure 13: Resilience within the energy sector

4.3.1 Achieving resilience.

When asked how the energy sector achieves and maintains its resilience throughout the years. Several respondents specified that there are diverse ways of achieving resilience and it is a combination of procedures/actions taken that makes achieving resilience possible. These procedures/actions are both on an organizational and technical level.

Several of our respondents mentioned that to achieve resilience on the organizational level, there are some factors that the organizations within the energy sector need to address. This part of resilience is about having effective communication, understanding the picture, and knowing what is needed.
The first thing our respondents focused on is having the right competence, and that expertise is available to solve problems when needed. To make that work I3 mentioned that they need to have a minimum of 3 personnel who can do an operational role, and they must be able to have one man on holiday and one man ill and at least one man left. They are also in the process of moving it in the direction of having 5 personnel available to see how the work requirement has increased. Moreover, I9 and I11 explained that all the expertise and knowledge they have is shared between the companies in the industry and that NVE publishes a lot of information to inform about the threat picture and it is quite useful for them. In addition, the management is more involved as well when it comes to being resilient. NVE and NSM are helping the organization from top to bottom by showing them what types of threats exist out there and how to identify and mitigate them. I1, I3, and I5 highlighted that NVE has created several requirements that need to be followed by them.
Lastly I1, I6, and I9 mentioned that resilience on the organizational level is about following policies and effort plans that are created to help with how to do things. These policies include exercises that they have gone through to get the mindset of what to do in different situations, classification of emergency preparedness, and contacting the right people for IT security assistance. Therefore, to summarize it is about documentation and those who are involved in the organization are included and have had the proper training and overview of their systems which is mentioned later in the report.

As for the technical level of resilience, the respondents emphasized that having the correct tools and solution is a big part of becoming resilient. To get that, the organizations address IT security, and they rely on assessments made by experts within the field. Then a presentation will be made for why this system/solution is needed and how it could help with security/resilience. Then a conclusion will be made whether this system will be implemented or not. According to 4 out of 11 the conclusion usually results in getting the solution they need. I5 additionally mentioned that having temporary solutions with a physical contingency plan where they store them in two separate places is another way of achieving resilience. This may count both as an organizational and technical level of resilience, however, that means the solution provided would cover the technical side if they were attacked.

Another highlight that was mentioned by several respondents is the energy systems in Norway are built differently than other countries/nations. Whereas other countries have large nuclear and gas power plants, and if one or two of them are attacked/malfunctioning it would have a significant effect on society. Norway has their power plants built with very many producing units, if some of them are attacked or not working properly, it is not critical for the delivery of power. I3 explains.

"The power plant is also built to be self-propelled, at least the big ones. There has always been a culture in the industry for building solutions with both seat belts and seat belt braces, rescue services parachute all measures that the power plant should be able to operate on its own."

The energy sector in Norway is occupied with the structure of their security as well. I6 explains that security is built layer by layer. The backup systems built are optimal and have been tested. The traffic they use is safe and encrypted. The architecture of how the systems control, connection to the outside world, and monitoring traffic is of most importance to them. According to I10 resilience within the energy sector is technically built in the form of perimeter protection with firewalls, and a detection mechanism such as an Intrusion Detection System (IDS). There must be a balance between security, accessibility, usability, and economy. Achieving proper resilience is about creating that balance. I7 and I11 added that the technical part of resilience is about having solutions that increase their security by doing the following:

1. Measure the number of clients.
2. Send notifications to make employees aware of unpatched things.
3. Who has administrator rights (security roles)?
4. How many incidents/events do they get related to users (human error)

Several respondents highlighted that Resilience in the energy sector is achieved through having an overview of the system. Recognition of where one is weak, and strong. To put in countermeasures to address and secure the weakest links. The overview of lines and the production channels in the energy sector is quite fast, therefore organizations will have the ability to respond and get their systems back online quickly.

4.3.2 Challenges

Understanding what challenges can occur within the energy sector was of great interest to us, as it gave some clue to what can affect the energy sector in a negative way. In this area most of our respondents had several topics they believed to be the biggest challenges that could affect the resilience of the energy sector.

4 respondents believe that the energy sector's ability to keep up with newer and more advanced threats is an issue that is always there, and difficult to get ahead of.
I7 and I10 talked about how having modern technology could mitigate some of the challenges, by getting the newest digital solution where it is possible, would be the most important part in ensuring security. However, in contrast, 1 of the respondents was concerned about getting a new system worth million and where no one in the organization knew how to really use it, making it a waste of time and money.
But the biggest challenge that most of our respondents agreed upon was the competence of employees. 7 out of 11 says that it is a challenge to ensure that people have some level of understanding and competence when it comes to security. Such as making people aware of what they do and the consequences of it or making sure they do not make mistakes or fail to follow security routines. This was additionally pointed out about the importance of having the management and other leaders involved in understanding why doing certain things, or acquiring a certain security

system is important, for the continuation of their product, in this case supplying energy.

4.3.2.1 Bottlenecks

We further discussed with our respondents if there was a bottleneck area that could be potential challenging to resilience, that they could think of. And to this there was no real unity to the answers among our respondents and they were mostly individual, or already mentioned before.

I1 and I11 both discussed the challenges of getting the management to acquire different technical or equivalent items that could prove beneficial to the organizations. While they both say that some improvements have been made in this area, there are still some bottleneck issues there. I2, I5, I6 and I10 did have some concern about different technical issues, such as how security is built around this system, having control over what these systems do, or having detection in all stages or physical limitation, that influences how the technical aspect can operate.

4.3.3 Practices & goals

The respondents were asked about whether they have some form of practice and goal they used to increase the security or resilience in their sector.
5 out of 11 respondents say they have some practices about how to ensure that they follow the KBF, as well as some of these respondents additionally had some more individual strategy that they believed was an improvement to be in line with the KBF.
4 out of 11 mention that using third party members as a tool to either share expertise among organizations, being notified from third parties when there have been incidents, and vice versa, to be better prepared, these third-party members were organization such as KraftCERT, NC-spectrum and NSM.
Using another third party is a practice to help improve the resilience of some of these organizations. Only 1 of the respondents talk about being more independent and not so reliant on others, to minimize the number of entries points a threat actor can use from other organizations.
4 respondents talked about the use of technical solutions that they wanted to add, implement, or improve to achieve better resilience. These solutions were improving firewall technology or making sure more of the system is protected by aa security

system Some talk again about the use of a detection system, where they have some goals to implement it in more parts of the system, or just expand it to cover new areas. Another finding was that 4 out of 11 talks about increasing awareness as a goal, where they use drills, practices, and recent events to teach and improve awareness among employees. Having employees investigate events and being alerted about attacks and how they are happening is a strategy that they believe increases the employee's ability to avoid human error.

There is some focus on documentation among our respondents as well. Using documentation to provide apparent reasons to the management for why we need to do this or acquire that, or why doing it this way is bad. I1 and I5 support using documentation to create a more substantial way of reporting different events or using it to inform others about what they should know about. This is a similar goal to other respondents as well, how to convince the management to perform certain actions that can improve the resilience of their organization. 6 out of 11 mentions that information about security must be sent up to the management, and make sure that they either makes the right decision regarding security, inform them about what they must do, or raise awareness among them, as to reduce the likelihood of them falling for potential threats, such as phishing.

4.3.4 Measuring Resilience

We wanted to ask our respondents about how they know if they are resilient or not, and how do they measure this resilience. While some were unsure on how they measured whether they were resilient or not, there was some method they agreed upon that could indicate some level of resilience.

One method was the use of testing, 4 out of 11 used various levels of testing to see how many employees make mistakes, such as phishing-tests or testing the system with a penetration-test to see how well the system handled being attacked. In this way we can get some indication of how resilient a system is. Another method that was used was logs, I5, I7 and I10 mention viewing logs to see how well a system detects events, including “false event” where an employee makes some minor mistake, and the system detects and reports it as a threat event. Using logs to see how good the system can detect when an error is happening can further help provide some measures of resilience in an organization. In addition, I3 specified a certain way of measuring resilience of their systems by saying the following: “*We have a*

threshold based on one to six. Where level 6 is the most critical system and 1 being the least critical. Having a level 6 system means it has no form for redundancy and if that system is out, the whole organization is out of business. Therefore, we tag elements based on that and work on it." When asked if it was possible to see this threshold and how it determines if the system is level 1 or 6, the answer was no, this information is confidential. However, I10 mentioned a similar threshold level they use to measure systems and was able to provide an example shown below that it is possible to share with the public eye.

Table 11: Threshold level (provided by a research subject)

Maturity Level	Statement
1	***Initial*** (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.
2	***Repeatable*** - the process is at least documented sufficiently such that repeating the same steps may be attempted.
3	**Defined** - the process is defined/confirmed as a standard business process
4	**Capable** - the process is quantitatively managed in accordance with agreed-upon metrics.
5	**Efficient** - process management includes deliberate process optimization/improvement.

4.3.5 Resilience Awareness

Resilience awareness is described by 8 of our respondents as one of the most significant factors that contributes to proper security and resilience within the energy sector. When asked about how organizations achieve awareness of security and resilience, all our respondents mentioned that it is performed through appropriate training. I1 mentions awareness is increased through security month and implementation of IT security expertise which they have seen work exceptionally. They have also created a network of information based on projects, training, and previous incidents both internal and external that is available for everyone in the organization. The purpose of this network is to help both new and old employees gain an understanding of resilience and make them aware. Moreover, I1 specified that they have something called subject day, where once a year they get external

speakers from NSM and KraftCERT to hold a presentation about security and resilience awareness.

I3 and I5 describe the national security month they have is crucial to increasing awareness of their employees. In that month, a lot of information, training, and courses were taken about security and resilience. Several of the respondents mentioned that people in the energy sector are aware of security and resilience, however that was not always the case. To change that they went from having security days/months from being focused on health, safety and environment (HSE) to including IT security and putting it in context for the individual, whereas everyone is involved i.e., from cleaning to CEO. In addition to the security day/month there are semi-annual meetings that are held in the operating areas where they include several topics and discussions to increase awareness of resilience and the consequences of it if something should go wrong. While most of the respondents focused on training and how they are performed, I7 described that they do not have any specific way of increasing awareness in their organization. They focus on having general training, right mindset and attitude which indirectly helps with awareness. I7 explains "We *make employees aware of resilience through general training that is available for both new and existing employees. Some of them might require more sharp and extensive training than others, but there is nothing else besides that we do*."

In addition to training, all the respondents described part of increasing awareness is about building a security culture and making sure that the behavior of employees is the one required to have in today's IT world. The requirements they mentioned is the following:

- That the people become more competent.
- Get the training they need.
- Get involved in various aspects of the organization.
- Experience that security solutions are continuously updated and implemented.
- Adjust unappropriated solutions and then implement them.
- Communicate properly both internally and externally.

To further strengthen that security culture, I3 mentions that involving the employees in events such as making analysis of small units, then using them to learn and build awareness is essential. Along with that they are extremely focused on not playing the

blame game. If someone happens to make a mistake they would rather help and train that individual. I3 explains "*There is incredible value in learning from mistakes. It is much better to share information and teach the community (workplace) than trying to hide the mistakes.*"
Lastly, several respondents describe resilience awareness as an ongoing process that continuously creates new milestones and in general never has a clear stopping point. There is always room for improvement, and it is essential to have that type of mindset and never think what they have is good enough.

4.4 Awareness training

We wanted to know more about what type of training or practices are currently being used within the energy sector, how well they work for our respondents and if there was something they believed could be done differently to make it better.
We additionally discussed when and why people ignore security routines and how this can be handled within the organization.

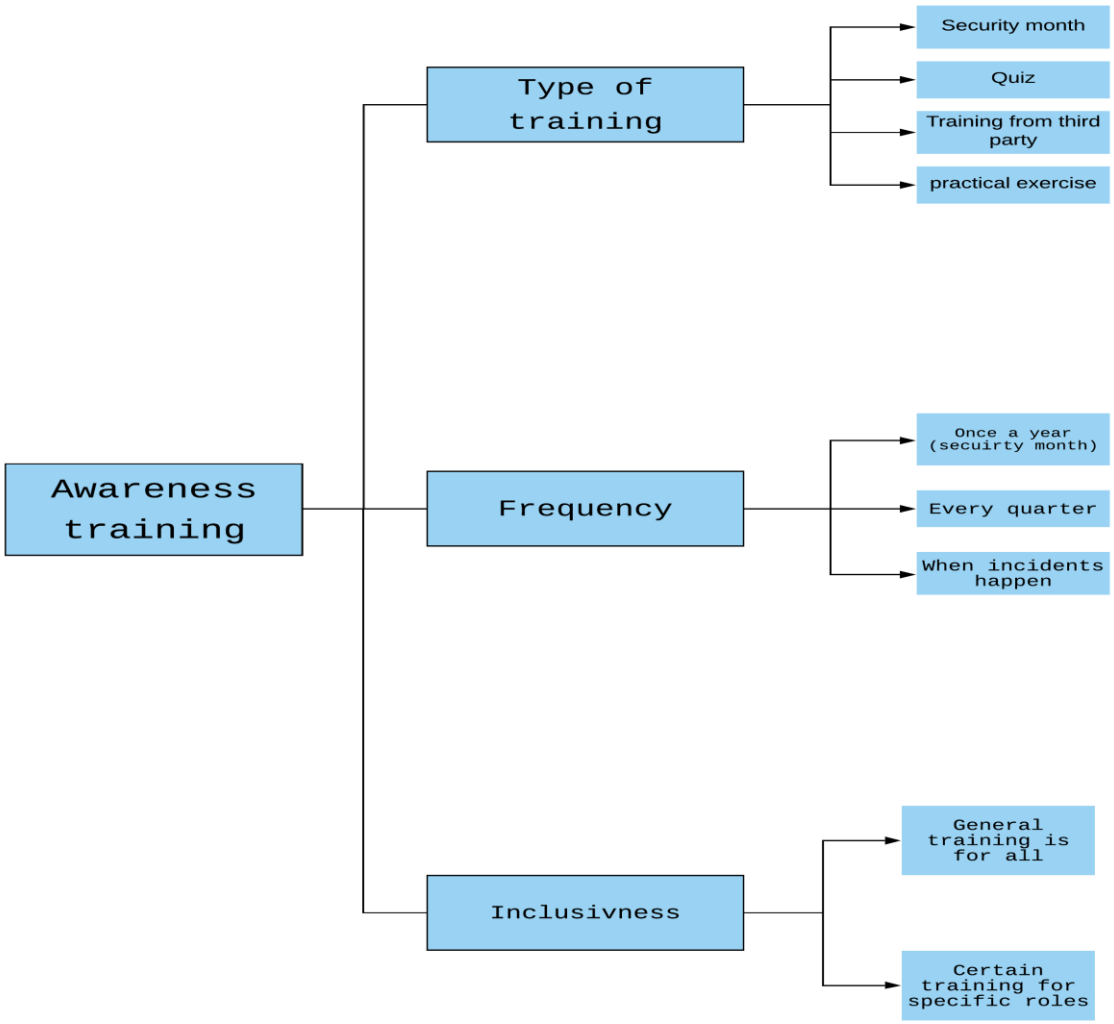


Figure 14: Training within the energy sector

4.4.1 Type of training

When it comes to what type of training is used within the energy sector, there is a general form of training that all respondents seem to have. Such as discussion of different security subjects, getting taught about rules and routines, and some use practices or paper exercise as a method for training. I1, I4, I5 and I10 contribute to the security month, as an important event for training employees.

The national security month is a yearly event, where one month (October) is dedicated to raising awareness and competence within business and provides better everyday security for all.

There was discussion about the use of a small drip to continuously inform and train employees. 5 out of 11 all agreed about using these small drips to keep their employee up to date with security threats, and to keep them aware throughout the year, rather than focusing everything on just one month. This training consisted of sending out information about relevant treats, courses they could take such as micro e-learning or doing phishing testing to get the employee talking and sharing.
I2, I6 and I8 further talk about having some drills where they look at mistakes made and what they can learn from them or having weekly Information sent out to inform on different issues that are in topic to keep employees informed and up to date on current trends.

While the security month is the main area for when training occurs, several of them take some time to undergo some training by themselves as well. Even though no specific training stood out among our respondents, there were some that were more important at this time than others. Such as awareness of e-mail and phishing attacks, and sharing information about recent cyber-attacks events, to create a culture where Cybersecurity is discussed more.

4.4.1.1 Training that may work.

We wanted to know more on an individual level about which practices that our informant preferred, and if there were some practices that they believed were the better method for learning about cybersecurity.

5 of our respondents think that having some third-party organization such as NC-Spectrum, KraftCERT, NordSIS and NSM share their experience, and talk about events that have happened. Information video and being part of their exercise is what they consider are practices that work to learn both themselves and others around them. It is having someone who can explain complex events in a simpler manner to people not heavily involved in cybersecurity.
I4 and I10 preferred a more hands on exercise, where they can involve themselves more in details, about what and how, who should we contact if X happens or what happens if Y is attacked.

Several respondents mention that training that worked for them also depended on what their current role in the organization was, where if they had a more technical role, they wanted more technical drills, and others in a more organizational role, wanted more organizational drills.

4.4.1.2 Training that may not work.

When it came to talking about training that did not work, it was more difficult for our respondents to answer, as some could not remember what did not work.
Making a finding here is also difficult because what works for one does not work for another. I1 and I4 were at some level of disagreement where one found a deep dive into the subject did not work, while the other was against a general shallow dive, as that was too boring and simplified.
Understanding what type of training work does not is highly dependent on the role of the individual, some find short brief exercise pointless, while others struggle with more comprehensive exercise.

4.4.2 Frequency

As mentioned earlier, training is a big part of making the employees aware of security and resilience, we wanted to find out how often this training is carried out. 8 respondents mentioned that they have something called “security month”, where one month a year (October in this case) they have full focus on security and resilience within their organization. In that month, the organizations focus on teaching and refreshing the employee's mind about security and resilience by going through the types of training mentioned earlier in the report. In addition to that one-month 5 out of 11 explained there is another training which is either once every quarter or at least twice a year that will include things the organization deem important to present and inform their employees about when it comes to security. I6 described the following when asked about the frequency of training.

“*We run it quarterly, but then we have extra focus throughout October as NordSIS and NSM are here to talk about security and resilience. Then we run fairly structured training with the most important topics throughout October.*”

Several other respondents further mentioned that besides the quarterly or the security month in October, their organization focuses on having some other small training/courses which help with keeping security in mind. Moreover, every time an incident happens that might be relevant to the energy sector, that incident is shared with the employees to show them what has happened and how it could be avoided.

Every informant was then asked the follow-up question: Do you feel the frequency of training you have is satisfactory?
While all our respondents described the training they had as satisfactory, the frequency part could be better. 7 out of 11 respondents mentioned that the training they have in October could be cut in half where they have half of it at the start/middle of the year and the other half at the end. They explained that there must be a balance on how much training and information can be given to employees without them getting bored and losing their focus/attention. According to I5, having extensive training once a year is too little. The training should happen more often if they are going to build it as part of their security culture and having an intensive month of security may not be enough. I7 explains that:

"When *it comes to frequency of training, we probably have a potential for improvement. In general, the employees are put into security instructions and good practice on information security and resilience, but the target based on the type of personnel and how often these training are carried out could be better*."

To summarize the training happens at very least twice a year and with extra focus during what they call the "security month" where the whole organization is focusing on security and resilience. When asked about the frequency of this training, most of the respondents mentioned that it should be increased and the security month in October should be throughout the year.

4.4.3 Inclusiveness

As for who in the organization gets included in the training depends on what type of training is being carried out. The security month in October is for everyone in the

organization and it is mandatory to participate in everything. I5 explains they have reports that show who has not completed courses or participated in the training. Those employees will then get a notification from the highest level of the organization to participate and finish the training. As for other times, the employees included will depend on their profession and position. I3 specified that some training they have had in the organization did not include the accounting department because the training they had was about installing software and patching them, which has nothing to do with accounting. However, if they see any need for that department to be part of the training, they will be included immediately. I1 explains that while most training is mandatory and everyone from the CEO down to the technicians must participate, additionally some of the training they do is voluntary where the employees could sign up and focus on broadening their knowledge of security and resilience.

The inclusiveness of employees when it comes to training is divided into two parts. One is about general security review and the general security level, where it must be raised across the entire organization. Then there is more specific training such as:

- Role-specific training.
- Critical role-specific training.
- Team-based training.
- Department based training.
- Location-based training.
- Work-related safety training.

I6 states that the energy sector and their organizations are genuinely concerned with running training that focuses on education and understanding of security and resilience for everyone in the organization regardless of position. The training may vary but everyone is included. This way every aspect of the organization and sector has the highest possible protection.

4.4.4 Security procedures

We asked our respondents two very personal questions, but we believed these questions to be important for organizations and companies to be aware of.

We wanted to know if they did and/or any within their organization ever neglected or did not follow certain security routines.
While many of our respondents answered differently, there was some agreement on why they sometimes did not follow security routines. These could be simplicity vs complexity, where if you should do it in a complex manner, but there was a simpler method for achieving the same, many said they did the simpler method sometime. Or when things are unclear or uncertain, they sometimes skip certain parts to get things to finish their objective. According to several of our respondents, when they need to do a task quickly, or there is a limited amount of time, the likelihood of them ignoring security procedures increases. They agreed that they believed it happens with others in the same organization for the same reasons, where people take shortcuts, or skip some steps to make the everyday simpler for them.
Understanding that people sometimes will make mistakes, take shortcuts, or time pressure may make people not take security into consideration, is something that all organizations need to be aware of.
It should be noted that our respondents only relaxed with non-vital areas, or areas with little to no consequence.

5.0 Discussion

The focus of this study was on analyzing security and the resilience of CIS in the energy sector. For the resilience part, we focus on what the characteristics of resilience are, how it is achieved, what challenges and bottlenecks they face, measuring resilience, and how they increased awareness among themselves when it comes to resilience. Furthermore, we investigated what type of routines, policies and frameworks are practiced when it comes to resilience in the energy sector. In this section we will relate the result of the study with the research questions and the literature study. To restate this study seeks to answerer these questions.

RQ1 "What are the characteristics of resilient critical infrastructures within the energy sector, and how can this be achieved?"

RQ2 "What are the best practices used to achieve resilience within the energy sector, and how are they carried out to increase the awareness of their employees?"

5.1 Characteristics resilient in critical infrastructure

The fist questions in this study sought to identify the characteristics of resilience within the critical infrastructure, and how resilience can be achieved within the energy sector. We presented several aspects of what are used to determine the definition of resilience, by analyzing and reviewing existing literature and through discussion with the respondents. By measuring the existing understanding of resilience with the experiences of people working with resilience, we make an understanding of what the characteristics of resilience are within the energy sector.

Understanding the definition of the term resilience can be difficult to define as the word "resilience" can be used in many different settings, each sometimes with its own characteristics. When it comes to resilience in critical infrastructure, Erik Hollnagel (2014, p.376) states, "*A system is resilient if it can adjust its functioning before, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions.*" The NAS report (2017, p1) states the following:
"*Resilience is not just about lessening the likelihood that these outages will occur. It is also about limiting the consequences and disruptions caused by outages while power is out, restoring service rapidly afterwards, and learning from these experiences in order to better deal with events in the future.*"
To get an overview of attributes that defines what resilience is, we look at figure 1, the umbrella concept by Øien m.fl., (2018), which was used by "forsvarets forskningsinstitutt[6]" (FFI) in 2019 as well. The figure provides 5 different attributes that define what resilience is.

1. Understanding risk.
2. Anticipate/prepare.
3. Absorb/withstand.
4. Respond/recover.
5. Adapt/learn.

[6] Norwegian Defence Research Establishment

Most of the existing material used these five attributes in some form or another. While many write these attributes differently the core explanation is still the same. However, it is worth mentioning that some materials do not include attribute nr one as definition of resilience.

When asked about what resilience is and what characterizes resilience, the respondents had diverse answers. Some respondents highlighted that one of the important characteristics of resilience is having a clear understanding of their systems, what it does and what it can encounter. By having this clear understanding, they would be able to understand the risks that could affect the system. Moreover, how these risks could lead to creating or finding vulnerabilities that could be used to threaten the system with a variety of attacks with disastrous consequences. Knowing what type of threats and risks exist, and the amount of damage they could cause makes it critical to gain an understanding of their system and how they could stay or attempt to stay ahead of the curve. The respondents were asked to list what type of threats/challenges the energy sector is facing today, and how essential it is for them to know about these threats and how to address them.
Based on our results from the interviews, we have created a table that shows the currently most common threats the energy sector faces today.

Table 12: Threats the energy sector faces today, according to the research subjects.

Nr.	Attack/Threat	Number of respondents
1	Ransomware	10 out of 11
2	Phishing	10 out of 11
3	System Vulnerabilities in SCADA	9 out of 11
4	Insider Threat	5 out of 11
5	State Sponsored	5 out of 11
6	Hacktivism	5 out of 11
7	Cyber Espionage	5 out of 11
8	Traffic monitoring	2 out of 11

Comparison of the findings in this study (Table 12) with those of other studies (Table 3) confirms that understanding of the common threats has changed. Knowledge of what threats can occur helps build up a resilience that can handle the more frequent attacks. Understanding risk and what may impact the organization is the same as the first attribute of what is resilience and leads to the second characteristic of resilience *preparedness*. Taking actions or activities by the energy sector to anticipate the threats and challenges they are facing or might face in the future is a big part of being resilient. In addition, the respondents mentioned that planning what to do and how to implement their goals is another characteristic of being resilient. Through planning they can manage to prepare, mitigate attacks, and have a proper response when something undesirable happens.

There is as well a geographical implication on how resilience is understood in Norway. Some of our respondents point out that other European countries usually have one or more large power plants that cover a large amount of area. While in Norway due to the mountainous landscape, there is a decentralization of power plants, with many small ones instead. Therefore, if one power plant is attacked and cannot function others can take its place. This is similar to attribute nr 3, where the ability absorb/withstand plays into effect, by not having a single defined target for attackers to focus on.

Other characteristics that all respondents mentioned to be of highest importance when it came to being resilient and that is the legislation, framework, and the role NVE plays in their respective sector. KBF and NVE seem to be a key characteristic to being resilient when it comes to the organizations/ respondents that we interviewed. The respondents highlighted that most if not everything the energy sector needs when it comes to security and resilience is accomplished by NVE and the assistance provided from NSM and KraftCERT.

Looking at the existing literature and what the respondents said about the characteristics of resilience, we can see that Norway applies the same resilience concept as the umbrella concept (figure 1) with the addition of what the 5 attributes that define/characterize resilience in the FFI report. Moreover, as mentioned by Lars Gjesvik (2019), NVE has a vital role as a supervisor for the energy sector when it comes to their security and resilience. NVE provides services for anything from what

type of threats exist, prepare for these threats, and how to protect themselves from it. According to the data gathered from the interviews there are some things that are different in Norway. The two things that stood out were the type of threats and HRO. None of the respondents mentioned anything about HRO and the HRO 5 hallmarks during the interviews. When we brought up HRO the respondents stated what they knew about it, however it was not used as a way of characterizing or achieving resilience in Norway.

As for the threats and challenges, if we compare Table 3 of threats/attacks provided by ECSO (2018) and Table 12 created based on the data gathered from the interviews, we can see that some of the threats have higher priority in Norway than other countries. According to our respondents, Norway has higher priorities on increasing awareness among employees. This is in accordance with what our respondents believed to be the biggest threats, such as ransomware and phishing, both are types of attacks that use employees to harm the organization. These priorities may look different from other countries which are more focused on dealing with threats such as malware and DDoS as shown in the ECSO (2018) table 3.

5.2 Achieving resilience in critical infrastructure.

There are several methods used to achieve resilience. Figure 2 illustrates how the NAS in the USA achieve a resilient system with four different steps. Prepare -> Ameliorate -> Quickly Recover -> Observe, Learn, and improve. (NAS, 2017: p,1) The last step loops back through the three first steps, and according to NAS following this method will help achieve a resilient system. This is similar to umbrella concept (Figure 1) where the same principles are to be prepared, be able to absorb the attack, and then recover and learn what went wrong, what worked and how to improve.

One of the challenges when using a framework is how easily or how well an organization can follow such a method. How does one prepare or how do one mitigate attacks? There are many frameworks that provide supposed solutions and methods to follow for achieving resilience. NIST or ISO standards are often mentioned in international areas, where large organizations can use these standards as intended. While other nations such as Norway, with smaller organization and less capacity create their own versions that they believe is better suited for them, such as KBF.

From the discussing about how our respondents achieve resilience in their organization one of the most common answers was that they followed KBF, and that it was a helpful guide in how to manage cybersecurity. Another quite persistent factor was communication with other parties, NVE, NSM, kraftCERT, KraftSIS etc., to help inform them about threats and what attacks happening, share knowledge and share competence. Where some had people come over to their organization to teach them or help them solve certain problems. Having a network with other organizations to provide some level of assistance seemed to be a characteristic for our respondents. In addition, the energy sector in Norway aims to achieving resilience through organizational and technical level, by having several methods for both of them. When it comes to the organizational part, the energy sector focuses on having proper policies, training, and routines which helps create a mindset of always being prepared and knowing what to do in different situations. As for the technical level, the energy sector is occupied with having the correct tools to both protect themselves and achieve resilience. There are several measurements taken to achieve resilience on the technical level. The systems used are usually inspected layer by layer to make sure that everything is optimal. Everything in their system is backed up, encrypted, and protected by their IDS. A balance created between security accessibility, usability, and resilience. Lastly, having an overview of the system and knowing where their weakest points are and patching them is an important way of achieving resilience in the energy sector as well.

When comparing existing literature with what our interviews, we see the expected similarities, where using the KBF is a valuable tool for our respondents, to help provide some guidelines on how they assemble literature. The same can be said for the use of third-party organizations to provide early warning, and information about threats, that can help with preparing for attacks. Additionally, there was a similarity between the way the energy sector and the RMI achieve resilience, where several methods mentioned by RMI are implemented in the energy sector.

5.3 What are considered the "best" practices to achieve resilience.

There are several practices that can help achieve resilience, implementing a framework or legislation known as "best" practice can be immensely helpful for organizations. In the international area, there are several frameworks that can provide this "best" method of achieving resilience. The literature study revealed several referrals to NIST and the ISO standards, and they are considered best-practice guidelines.

"Prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services." (Sedgewick, 2014 pg. 3)

When working with Cybersecurity, it is highly recommended to follow these standards, however, there have been some issues with scalability of the frameworks, especially for smaller organizations. In Norway there are other frameworks/legislation used, such as KBF which are still based on the NIST and the ISO but created to fit in areas where NIST or ISO are too large and too comprehensive to be effectively used. Nevertheless, having and using these frameworks are particularly important.

"*The framework enables organizations - regardless of size, degree of cybersecurity risk, or cybersecurity sophistication - to apply the principles and best practices of risk management to improving the security and resilience*." (Barrett, 2018, p v).

While having and using frameworks is a vital practice there are other practices that are more specific to how to achieve resilience. When analyzing existing material several specific topics emerged. One of these was e-mail filtering that helped prevent phishing. Social engineering attacks are quite common, and all it takes is one unconscious employee to achieve some effect. phishing attacks take advantage of what is often considered the weakest part of the system, the people. Therefore, it was expected that practices helping prevent or mitigate social engineering are among the essential practices.

Another "best" practice, was monitoring the system, where tools such as DLP, and SIEM were controlling the information, and monitoring for abnormality and reporting if any are detected. Having control of the information and making sure it

stays safe when it enters, or leaves is a practice that helps mitigate potential security issues.

According to our respondents there are several practices implemented in their respected sector that are considered “best”. Policies, routines and creating a culture within the organization that aims at having the best security possible and being resilient is one of the practices mentioned multiple times during the interviews. The way to achieve resilience according to our respondents is by following KBF as much as possible. In addition, they use other practices, such as collaborating with third parties that would assist their organization in maintaining proper security and resilience by sharing expertise, giving notification, and showing them how to respond or recover from certain situations. Documentation and logging are used quite often and according to our informant they are both highly effective and efficient. Documentation and logging are used in the following ways to achieve resilience:

- Report on events/incidents.
- Inform others on how and what to do.
- Provide sufficient evidence/reasons for why a certain practice needs to be implemented.
- Assists with reducing the likelihood of being victim to attacks.
- Convince management of making the right decision.
- Raise awareness among the organization about security and resilience.

Raising awareness is a practice itself in the energy sector, in addition to be part of documentation. The respondents explain that increasing awareness within the organization is a practice and a goal that they want to achieve implementing and continuously improving.

Other practices that were mentioned were knowing what type of technical solutions should be implemented to achieve better resilience. Some respondents described, implementing, and improving firewall technology (if possible), and adding IDS in more areas helps with expanding their resilience and security, which could be considered as “best” practice for them. In addition to adding these solutions, it was mentioned that testing and measuring the systems are one of the practices they carry out to achieve better resilience. The energy sector uses penetration tests to measure the resilience and the endurance of the system. Moreover, they keep logs which are

continuously monitored for how well their system detects and reports events as threats, including false ones. There are more practices to achieve resilience used in the energy sector today than what is covered in this thesis, however those were either not mentioned or be described due to confidentiality.

There are several similarities between the existing literature and what our respondents have shared with us. Using framework or legislation were an essential key factor in both cases, and our respondents credited KBF for being one of the "best" ways to ensure security and resilience within their organization.
While frameworks were a big aspect of security, they were not the only once. Several of our respondents talked about system monitoring, such as having IDS or focusing on implementing firewalls.
One challenge that may be difficult to reflect on is what are the specific "best" method for employees between existing literature and what our respondents have said. This is because we were able to dig deeper into how and why with our respondents and get personal experience from them. However, with existing litterateur, most was a more general approach to employees. Lastly, based on what the respondents have said about practices used in their organization, we can see that the energy sector is implementing the aspects of figure 6 as best practices.

5.4 How awareness is increased among employees.

During the literature review we discovered that information on awareness has mostly focused on a more general view.
Therefore, our understanding of the specifics on how awareness is increased among existing literature is limited.

Throughout the literature review it was discovered that having an organization or analytical team that worked on teaching employees about security, helping them understand and identifying the existing threats, and how to keep their data secure from attacks such as phishing or ransomware, was one of the methods in rising awareness of the employee. Practicing an incident response plan to train employees to know what to do when an unexpected event happens, was a high priority as well. Most information about increasing awareness was primarily targeting social

engineering threats, this may be because of how employees are targeted by these kinds of threats.
Training, informing, and having a response plan are some of the main attributes of how awareness is taught to employees. However specific details of the training and response plan were not investigated.

In the interviews we discussed with our respondents how the practices implemented in the energy sector contribute to raising awareness. It was mentioned that they help the employees understand why things are carried out in a certain way, i.e., documentation helps the organization understand more things about themselves and make the employees aware of where they might improve. In addition, when it comes to providing or increasing resilience, most decisions are made by the management, and one practice is to provide evidence or reasoning for why certain measurements must be taken. Through reasoning provided by documentation, reports or presentation (depending on who is for) employees from the bottom organization all the way to management can be informed of resilience and the importance of it.
Regarding third parties, several respondents mentioned that having third parties with their expertise and knowledge where they are sharing data, warning them of new threats and risks, point to new incidents, and respond to threats or attacks is essential for the energy sector. Moreover, the combination of third parties and KBF assists the energy sector with creating a desired security culture within the organization where they focus on being as resilient as possible. Training was another practice mentioned in the findings when it came to increasing awareness. The energy sector has training at certain times of the year, and some are more frequent than others. These training courses show the employees what is important when it comes to resilience, how resilience is achieved. Training further shows them certain scenarios on how things can go terribly wrong if the employees are not aware of resilience or are not following certain policies, routines, guidelines, or tools provided for them. In addition, these training courses are performed throughout the year so that employees are reminded of the importance of their job and how to maintain and protect the resilience achieved within the organization. The practices are carried out in many ways to reach everyone in the organization. The energy sector knows that people learn in different ways, therefore these practices have a variety of methods to teach about resilience, it could be anything from videos, quizzes, team-based games,

VR, and more. This is performed so that the training can reach and affect the entire organization.
These practices are performed so that organizations in the energy sector can have the ability to investigate events or incidents, be alerted, how it happened, and how to respond if they were the victim of these incidents.
Furthermore, the practices help them with understanding what is out there and avoid or prevent mistakes or attacks that might occur.

Increasing the awareness of employees can be a challenge, because of how different people respond to teaching and learning. Looking at the existing literature and discussing with our respondents, we understand that there is no single best practice that can cover everything. Organization must be flexible in training personnel based on their role and experience. Our findings did discover that certain practices are more effective than others, such as getting small nuggets of information to help understand what is happening around them, how this can affect them, and what they can do to avoid it. Engaging the employee with scenarios where they are free to fail without consequences and giving them the chance to trial and error can make the employees feel more comfortable learning about resilience and increasing their awareness.

6.0 Contribution and suggestion for further research

The purpose of this study was to investigate the resilience of CIS within the energy sector and how they increased the awareness of resilience within their respected sector. This study was established after we had a term project that focused on frameworks and security within the energy sector and decided to look upon resilience for our master thesis. We started by organizing a literature review to gain an understanding of what type of literature exists about the risks, threats, challenges, security, and resilience of the energy sector and then prepare for the qualitative approach. The empirical data we collected was thematically analyzed and categorized based on the structure of the literature review and one we used in the interviews,

which consisted of 11 qualitative semi-structured interviews. This was then used to answer our research question with the addition of the existing literature.

6.1 Summary of Related Research

The mapping of the study for this thesis has resulted in 34 papers. The review starts by briefly explaining what CIS is and the importance of it. Then it aims at the risks, threats, and challenges the energy sector is dealing with. To deal with these challenges the review provides various practices/methods to address them and increase the security, resilience, and the awareness of the respected sector.

This led to identifying what resilience is and are the attributes that can be used to define it. And how do the employees learn or become more resilient Secondly, we investigate what constitutes best practices, and if there are any explanations of why these are considered best practices. Finally, we investigated different frameworks that potentially could improve or impact resilience in some way.

6.2 Summary of Empirical Findings

The empirical findings identified 8 types of threats/attacks that our respondents were most concerned about. The energy sector is guided by NVE on how to deal with existing and upcoming threats through various methods/practices. One of them is the legislation called KBF which is specifically made for them on how to build and maintain a desired level of resilience. In addition to KBF, the findings show that the energy sector achieves resilience through implementing policies, training, proper tools, sharing knowledge with others, and including everyone. These are carried out frequently to keep the mindset of the employees and the sector focused on always achieving the best resilience possible.

6.3 Contribution to Theory

Resilience - The term resilience is a system that can adjust its functioning before, during, or following events and thereby continue operating under both expected and unexpected conditions as said by Eirik Hollnagel. Following this as well as other definitions we discovered several key characteristics that can define resilience.

We identified four common attributes from most of the existing literature, these were *Anticipate/prepare, Absorb/withstand, Respond/recover,* and *Adapt/learn.*
These attributes represent the core of what a resilient system is.
However, we discovered a fifth attribute from Øien m.fl., (2018) which added Understanding risk as the first step, this was an attribute that was confirmed by several of our respondents to be a major step in making the system resilient. Adding this attribute as a core to what a resilient system is helps emphasize the importance of being updated on risk and threats that are continuously changing.

Identifying threats - The energy sector is susceptible to several threats such as equipment failure, software, human error, and insider attack, which does make it difficult to operate, secure and ensure that the system is robust (Kyriakides & Polycarpou, 2014). Moreover, other threats have emerged and focus on harming the energy sector through cyberattacks, which can harm systems to the point of shutting them down or even give full remote access to the attacker. As mentioned, ECSO findings in 2018 presented a table (table 3) of most common threats that the energy sector encounters and how some of them have higher probability than others. After the analysis of the findings, we identified that the threats in the Norwegian energy sector differ from the ECSO-findings in 2018.

Table 13: Threat comparison

Nr.	Attack/Threat ECSO 2018	Attack/Threat Study 2021
1	Malware	Ransomware
2	DDOS	Phishing
3	Cyber Espionage	System Vulnerabilities in SCADA
4	Web-based Attacks	Insider Threat
5	Insider Threat	State Sponsored
6	Hacktivism	Hacktivism
7	Malicious Code	Cyber Espionage
8	Phishing	Traffic monitoring

The differentiation lies with the probability of the threats happening and which ones concern them the most. These newly identified threats lay the grounds for carrying out a quantitative study to further understand how threats change over time and their relevance.

NIST framework - When it came to framework, one of the most common talked frameworks that existed for organizations to use was NIST framework. This framework is considered best-practice and supposedly can work for any organization regardless of size.
"*The framework enables organizations - regardless of size, degree of cybersecurity risk, or cybersecurity sophistication - to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.*" (Barrett 2018)
While in theory this might be true, in practice it is quite different as we discovered. Frameworks such as NIST are not practiced in Norway due to several reasons. KBF, which is tailored for the energy sector, is an incredibly strict framework/legislation for ICT security and resilience and they do not see the need for implementing something else. Additionally, we identified that some organizations in the energy sector lack desired knowledge and control in areas such as asset management and governance shown in Table 6 of the NIST framework, therefore it makes it more difficult to introduce/implement it. The NIST framework is very Americanized and compared to the KBF and other frameworks implemented, NIST seems to be very extensive, and difficult to operate without having a certification. Due to these reasons NIST framework, among other heavy frameworks, are too complicated for many if not all organizations in Norwegian energy sector to follow even though these frameworks claim to be the best-practice and can be implemented for any organization regardless of size.

6.4 Implications for Practitioners

The gathered results from the interview and literature review show that the awareness of what characterizes resilience, and how the energy sector achieves it is at a satisfactory level. We have found that many of the employees have a good relationship and knowledge of resilience and what their organizations are doing to

maintain that type of resilience. These organizations find it important to implement ways for practitioners to understand the importance of security and resilience within their given sector and that it should always be kept in mind. However, it was further mentioned that the energy sector is aiming to increase that awareness even more. By increasing the awareness, the organizations within the energy sector would be able to help every practitioner understand the importance of resilience from the top all the way to the bottom, creating an environment where not only some people are aware of resilience but rather all. With that being said, the results showed that the awareness of resilience is not quite clarified on every level of the organization as well. Even though the energy sector might be aiming to improve that, at this very moment it is not where it should be. If every practitioner is familiar with term resilience and how it could be achieved, it might reduce the impact of existing threats today.

6.5 Limitations and Implication for Further Research

This study was a qualitative study that used lengthy interviews to conduct research. To this end we wanted to achieve 15 interviews, with different organizations within the energy sector of Norway. However, we encountered some limitations with acquiring people to interview, for varied reasons, such as many did not have time, for this type of interview, some believed they were unqualified to answer, and declined. While COVID-19 was not a direct issue for us, as our interviews were planned to do virtually, it may have unforeseen complications for people we wanted to interview, which made them unavailable for interview.

Because of this we reached 11 interviews, which we believed to be acceptable, but having more interviews with more organizations may have led to more discovery or reinforced this study even further.

As for further research, we found the subject of how security and resilience is implemented, and how frameworks play a part, to be something that can be investigated a broader area, with other sector to see how many need to create their or own version of framework, to act as guideline when raising awareness or increasing security. Furthermore, an extensive study that includes more actors, other stakeholders, and more respondents that have the knowledge and expertise of resilience would be interesting to conduct.

6.6 Conclusion

The goal of this study was divided into two factors. First was to investigate the RQ1 question, of the energy sector's understanding of resilience; what resilience is, what defines a resilient system, and how one can achieve resilience. To answer this question, we investigated different existing literature to see if there were some common features that could be considered as a definition. From there we could compare our data to see whether there were some differences from the literature. The challenge was to analyze what was said by our respondents and determine whether it matched our research without some level of bias, or by overestimating what was being said by our respondents. To best meet these challenges, we broke down each informant's data, and used the literature research as the basis for measuring, from there it simplified the process of analyzing the data. And based on this we were able to provide some findings to RQ1, where based on our respondents which represent seven different organizations, there was a greater understanding of what resilience is, many of them described the key attribute of resilience found in the literature research. Some respondents consider resilience as something that is for the entire organization, and only when everything is taken into consideration, can they know if what they have is resilient or not. In addition, just as the threat actors will continuously attempt to find new ways to breach systems, the energy sector should as well find new ways to achieve better security and resilience. While some had more understanding of what the term meant, and how it related to their sector, there were significant deviation was discovered from the literature research and the respondents.
However, differences exist such as the existence of HRO and that it was not mentioned by our informant, most of these differences are either not fully investigated by our side, or we believed the quantity of respondents were too few, to provide adequate data.

After looking into resilience and what it is, we were prepared to move into the second part of this study, and answer RQ2. For this part we need to understand what is considered best practice, how well they work, and how they can be used to increase the awareness of their employees. As same as RQ1 we investigated what was defined as best-practices and tried to find ways to determine if they worked.

The challenge here is that there are a few big companies that provide the best practices such as NIST or ISO, and there are many smaller companies that also provide some best practices, but many references back to NIST or ISO. Therefore, comparing existing literature with other sources to see if certain practices stood out became difficult. We proceeded therefore to use these best practices to compare them with our respondents in the energy sector. Based on our literature research and from information from our informant we knew that much of the best-practice framework was based on ISO, and NIST. However, we further discover that these best-practices as they are represented where to large or complex for the energy sector in Norway, this meant that the best-practices that ISO and NIST used, was not viable in this area, instead they use other framework or legislation that they consider best-practices such as KBF. They had to adapt ISO and NIST standards into something that was more specialized for their needs. This leads to the speculation that only large organizations can use the existing best-practices, while smaller organizations must instead create their own standards, that only use some part of best-practices to achieve resilience. The same can be said about how they are carried out to increase awareness among employees. For most of our respondents they use the security month to raise awareness, but some additionally has more focus and having small test or provide information throughout the year, and when discussion this aspect with informant that mostly followed the one-month standard, several of them did wish they also had some more awareness training that was not confined to the cybersecurity month. An unexpected finding in this area was the level of intertwining in the networks between our respondents and the third parties. which were connected through sharing of information and people to help raise the overall resilience of the energy sector.

As a final summary of our conclusion, we have provided characteristics of what resilient critical infrastructures within the energy sector are and found that they are similar to what was discovered among our respondents. Understanding this characteristic can provide further measurements and guidelines to help organizations to achieve knowledge of whether they are resilient or what they need to investigate to become more resilient.

As for best-practices there is a gap between what is defined as best-practices in the literature research, and what is defined as best-practices in the energy sector in

Norway. This could imply that NIST and ISO standards are limited to size, where smaller organizations can base some practices on their standards, they may not be good enough for their area.

References

Andersen, M. S. & Pettersen, D. T. M. (2020) Achieving Sustainability Through Geodata: An Empirical Study of Challenges and Barriers (Master's thesis). University of Agder, Kristiansand. https://hdl.handle.net/11250/2677172

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep*. https://doi.org/10.6028/NIST.CSWP.04162018

Bailey et al., (2020) "The Energy-Sector Threat: How to Address Cybersecurity vulnerabilities." https://www.powermag.com/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities/

Berg, V., Birkeland, J., Nguyen-Duc, A., Pappas, I. O., & Jaccheri, L. (2020). Achieving agility and quality in product development-an empirical study of hardware startups. *Journal of Systems and Software*, *167*, 110599.

Bhatt et al., (2014) The operational role of security information and event management systems.
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6924640

Boumphrey, R., & Bruno, M. (2015). *Foresight review of resilience engineering-designing for the expected and unexpected*. Technical report, Lloyd's Register Foundation.
https://www.researchgate.net/publication/283297519_Foresight_Review_of_Resilience_Engineering_designing_for_the_expected_and_unexpected

Cantu, J., Tolk, J., Fritts, S., & Gharehyakheh, A. (2020). High Reliability Organization (HRO) systematic literature review: Discovery of culture as a foundational hallmark. *Journal of Contingencies and Crisis Management*, *28*(4), 399-410.
Cantu et al. High Reliability Organization (HRO) systematic literature review: Discovery of culture as a foundational hallmark. (2020) PDF file.

Centre for the Protection of National Infrastructure (CPNI) last updated April 21. 2021
https://www.cpni.gov.uk/critical-national-infrastructure-0

Jackqueline Joseph. (2020). Carilec.org 2020 "Resilience in energy sector"
https://www.carilec.org/resilience-in-the-energy-sector/

Chen, J. Scott, G. 2020 "Energy Sector"
https://www.investopedia.com/terms/e/energy_sector.asp

Croope, S. V., & McNeil, S. (2011). Improving resilience of critical infrastructure systems postdisaster: recovery and mitigation. *Transportation research record*, *2234*(1), 3-13.
https://journals.sagepub.com/doi/pdf/10.3141/2234-01?fbclid=IwAR0ty7D6s8CgQ8_wOTOxDal4ToKvWhAHnY6SeYg6xySFLa-seSk_nmE0YT4

Cruzes, D. S., & Dybå, T. (2011). Recommended Steps for Thematic Synthesis in Software Engineering. 2011 International Symposium on Empirical Software Engineering and Measurement, 275–284.
https://ieeexplore.ieee.org/document/6092576/

Cyber-Attack on Indian Nuclear Power Plant Exposes Threat of "Snooping" Malware
BRIAN THOMAS | NOVEMBER 8, 2019 | TAG: THIRD PARTY DATA BREACH
https://www.bitsight.com/blog/cyber-attack-on-indian-nuclear-power-plant-exposes-threat-of-snooping-malware

Department of Homeland Security (2013). *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: Government Publishing Office
https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Direktoratet for samfunnssikkerhet og beredskap, (2016). Samfunnets kritiske funksjoner.
https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Dr. Ivonne A. Herrera, et al., (2018) Paper on Resilience Management Guidelines for Critical Infrastructures. From theory to practice by engaging end-users: concepts, interventions, tools and metods, link. https://www.humanist-vce.eu/fileadmin/contributeurs/humanist/white-paper.pdf

EU Directive 2008/114/EC, Identification and designation of European critical infrastructures (2008)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

Fairbanks, R. J., Wears, R. L., Woods, D. D., Hollnagel, E., Plsek, P., & Cook, R. I. (2014). Resilience and resilience engineering in health care. *Joint Commission journal on quality and patient safety*, *40*(8), 376-383.
Fairbanks et al. Resilience and resilience engineering in health care (2014) PDF file

F.D petit, et. al. (2013) Resilience Measurement index: An indicator of critical infrastructure Resilience
https://publications.anl.gov/anlpubs/2013/07/76797.pdf

Fritts, S., Tolk, J. N., Cantu, J., & Gharehyakheh, A. (2017). Convergence of research on high reliability theory and critical infrastructure protection. *Proceedings of the International Annual Conference of the American Society for Engineering Management*, 1– 9.

https://search.proquest.com/docview/2010278734

Fontana, A., & Frey, J. (2000). The Interview: From Structured Questions to Negotiated Text. (pp. 645–672). https://www.semanticscholar.org/paper/The-Interview%3A-From-Structured-Questions-to-Text-Fontana-Frey/6aafc4b0566f7b6299bbb2cfb220bbdca785368e

Gebauer, A., & Kiel-Dixon, U. (2009). High Reliability Organizing Managing the Unexpected by Building up Organizational Capabilities. *ICL Berlin (In collaboration with Ursula Kiel-Dixon, ThyssenKrupp Academy)*. https://www.semanticscholar.org/paper/High-Reliability-Organizing-Managing-the-Unexpected-Gebauer-Kiel-Dixon/19285c092a39c6a35c1fb88f170ede2b726462b7

Gjesvik, L. (2019) "Comparing cybersecurity critical infrastructure protection in Norway, the UK and Finland" https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2598280/NUPI_Report_5_2019_Gjesvik.pdf?sequence=1&isAllowed=y

Gifun, J. F., & Karydas, D. M. (2010). Organizational attributes of highly reliable complex systems. *Quality and Reliability Engineering International*, *26*(1), 53-62. https://doi.org/10.1002/qre.1034

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage. https://books.google.no/books?hl=en&lr=&id=_InCDwAAQBAJ&oi=fnd&pg=PP1&dq=qualitative+research+methods

Hoepfl, M. C. (1997). Choosing qualitative research: A primer for technology education researchers. *Volume 9 Issue 1 (fall 1997)*. https://vtechworks.lib.vt.edu/bitstream/handle/10919/8633/hoepfl.pdf?sequence=1

Hollnagel, Erik. (2016). Resilience Engineering: A New Understanding of Safety. Journal of the Ergonomics Society of Korea. 35. 185-191. DOI:10.5143/JESK.2016.35.3.185

Iyamu, T. (2018). Collecting qualitative data for information systems studies: The reality in practice. Education and Information Technologies, 23(5), 2249–2264. https://doi.org/10.1007/s10639-018-9718-2

Jensen, C. 2019 "What is Critical infrastructure and how should we protect it." https://www.tenable.com/blog/what-is-critical-infrastructure-and-how-should-we-protect-it

Johnson, R (1997). Examining the Validity structure of Qualitative Research. edu, 118. https://www.researchgate.net/publication/246126534_Examining_the_Validity_Structure_of_Qualitative_Research

Jovanović, A., Øien, K., & Choudhary, A. (2018). An indicator-based approach to assessing resilience of smart critical infrastructures. In *Urban Disaster Resilience and Security* (pp. 285-311). Springer, Cham.
Øien et al. An indicator-based approach to assessing resilience of smart critical infrastructures. (2018) PDF file.

Juliet Mian et al., (2018) Critical Infrastructure Resilience Understanding the landscape
https://www.resilienceshift.org/wp-content/uploads/2019/01/Critical-infrastructure-resilience_RevA_Final_011018.pdf

Kraftberedskapsforskriften (2018). Forskrift om sikkerhet og beredskap i kraftforsyningen Sist endret for-2018-11-01-1641 fra 01.01.2019. hentet fra https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

Kallio H, Pietila A, Johnson, M & Kangasniemi M (2016) Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. 1-12
https://onlinelibrary.wiley.com/doi/abs/10.1111/jan.13031

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering.
https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Kolb, B. (2008, September). Involving, sharing, analysing—Potential of the participatory photo interview. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 9, No. 3).
https://www.qualitative-research.net/index.php/fqs/article/view/1155

Kwasinski, A. (2016). Quantitative model and metrics of electric grids' resilience evaluated at a power distribution level. Energies 9(93).
https://doi.org/10.3390/en9020093

Kyriakides, E., & Polycarpou, M. (Eds.). (2014). *Intelligent monitoring, control, and security of critical infrastructure systems* (Vol. 565). Springer.
https://link.springer.com/book/10.1007%2F978-3-662-44160-2

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018, June). Implementing cyber-security measures in airports to improve cyber-resilience. In *2018 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Marshall, C., Brereton, P., & Kitchenham, B. (2015). Tools to support systematic reviews in software engineering: A cross-domain survey using semi-structured interviews. Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering, 1–6.
https://doi.org/10.1145/2745802.2745827

Melchiorre, T. (2018). Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security. https://www.enseccoe.org/data/public/uploads/2018/04/d1_2018.04.23-recommendations-on-the-importance-of-critical-energy.pdf

Miron, W. Muita, K. (2014) Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. technology innovation management review 33-38 https://timreview.ca/article/837

M.T., Ramsay, C.G., & Kelly, T. (2009). Enhancing organizational resilience through emergency planning: learnings from cross-sectoral lessons. Journal of Contingencies and Crisis Management, 17(1), 24-37. https://doi.org/10.1111/j.1468-5973.2009.00556.x

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Myers, D.M. (2008) Qualitative Research in Information systems. MISQuarterly. [Online] Available: http://www.qual.auckland.ac.nz/[2009,10. Februar]

NAS (2017). National. Academies of Sciences, Engineering, and Medicine. Enhancing the resilience of the Nation's Electricity System. Washington, DC: The National Academies Press. https://doi.org/10.17226/24836

NSCI. 2019"National Strategy for Critical Infrastructure" ISBN: 978-1-100-11248-0 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

Nickolov, E. (2006). Critical information infrastructure protection: analysis, evaluation and expectations. *Information and Security*, *17*, 105. Nickolov Critical information infrastructure protection: analysis, evaluation and expectations. (2006) PDF file

Olje og energidepartementet. (1990) (revised 2019). Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. for-2019-10-24-1414 fra 01.11.2019 (energilovforskriften) https://lovdata.no/dokument/SF/forskrift/1990-12-07-959#KAPITTEL_9

Pettersen, K. A., & Schulman, P. R. (2019). Drift, adaptation, resilience and reliability: toward an empirical clarification. *Safety science*, *117*, 460-468. https://doi.org/10.1016/j.ssci.2016.03.004

Pettersen, K. A., & Schulman (2016). Drift, adaptation, resilience, and reliability: toward an empirical clarification. Safety Science. DOI:10.1016/j.ssci.2016.03.004

https://www.questionpro.com/blog/quantitative-research/

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical infrastructure protection*, *25*, 125-138. https://www.sciencedirect.com/science/article/pii/S1874548218301744

Rehak, D., Senovsky, P., & Slivkova, S. (2018). Resilience of critical infrastructure elements and its main factors. *Systems*, *6*(2), 21. https://www.mdpi.com/2079-8954/6/2/21

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, *21*(6), 11-25. Rinaldi et al. Identifying, understanding, and analyzing critical infrastructure interdependencies. (20019 PDF file.

Robles, R. J., Choi, M. K., Cho, E. S., Kim, S. S., Park, G., & Lee, J. (2008). Common threats and vulnerabilities of critical infrastructures. *International journal of control and automation*, *1*(1), 17-22. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.528.1436&rep=rep1&type=pdf

Robson, C. 2002. Real World Research: A Resource for Social Scientists and Practitioner-Researchers (second ed.), Wiley-Blackwell, Oxford, UK; Madden, Mass (2002)

Runeson, P., & Höst, M. (2008). Guidelines for conducting and reporting case study research in software engineering. Empirical Software Engineering, 14(2), 131. https://doi.org/10.1007/s10664-008-9102-8

Sabino, V. (2020) "Energy sector cybersecurity is vulnerable but achievable" https://www.power-eng.com/2020/02/12/energy-sector-cybersecurity-is-vulnerable-but-achievable/#gref

https://doi.org/10.6028/NIST.CSWP.02122014,

Sedgewick, A. (2014), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST - Cybersecurity Framework, [online]. http://nist.gov/cyberframework/ (Accessed June 3, 2021) https://doi.org/10.6028/NIST.CSWP.02122014

Stavland, B., & Bruvoll, J. (2019). Resiliens–hva er det og hvordan kan det integreres i risikostyring?. FFi-rapport 2019 Stavland, B., & Bruvoll, J. Resiliens–hva er det og hvordan kan det integreres i risikostyring? (2019) PDF file.

Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A., & Varpio, L. (2015). Choosing a Qualitative Research Approach. *Journal of graduate medical education*, *7*(4), 669–670. https://doi.org/10.4300/JGME-D-15-00414.1

The European Commission. 2007 “European Programme for Critical Infrastructure Protection”
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. American Journal of Evaluation, 27(2), 237–246.
https://doi.org/10.1177/1098214005283748

Tugrul, B., & Cimen, S. (2016). Importance of Corporate Governance for Energy in Sustainable Development and Evaluation with Quantitative SWOT Analysis. *Acta Physica Polonica, A.*, *130*(1).
Tugrul, B., & Cimen, S. Importance of Corporate Governance for Energy in Sustainable Development and Evaluation with Quantitative SWOT Analysis. (2016). PDF file.

The European Cybersecurity Organisation (ECSO), 2018, Energy Network and Smart grids Cybersecurity for the energy sector.
https://ecs-org.eu/documents/publications/5fdb2673903c6.pdf

u.s. department of energy office of electricity delivery and energy reliability (2015) “energy sector cybersecurity framework implementation guidance”
https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

U.S. Pipeline Shutdown Exposes Cyber Threat to Energy Sector
By Collin Eaton, James Rundle and David Uberti Updated May 9, 2021 6:47 pm ET. https://www.wsj.com/articles/u-s-pipeline-shutdown-exposes-cyber-threat-to-energy-sector-11620574464

Walsham, Geoff. (2006). Doing interpretive research. European Journal of Information Systems, 15(3), 320–330.
https://doi.org/10.1057/palgrave.ejis.3000589

Weingart, S. H. (2000, August). Physical security devices for computer subsystems: A survey of attacks and defenses. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 302-317). Springer, Berlin, Heidelberg.
https://link.springer.com/chapter/10.1007/3-540-44499-8_24

Xiao-Juan, L., & Li-Zhen, H. 2010. Vulnerability and Interdependency of Critical Infrastructure: A Review. *Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA)*: 1–5.
https://ieeexplore.ieee.org/document/5679237

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. 2011. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art. *Energy Policy*, 39(10): 6100–6119.
https://www.sciencedirect.com/science/article/pii/S0301421511005337?via%3Dihub

Appendix 1 Interview Questions

Section 1: General information about the interviewee

1. Position role in the organization, work experience in the organization
2. What do you work with daily?
3. Have you participated in any relevant security, framework, or resilience projects?
4. What was the goal of the project?
5. Did you have any challenges?

Section 2: Security

6. What type of threats & challenges are critical infrastructures facing today (energy sector)?
7. What do you consider to be the biggest challenges related to security in CIS?
8. How are these security challenges & threats addressed in CIS?
9. Can you explain the necessary measurements taken to main/increase security of CIS both on organizational and technical level?
10. From all the measurements implemented, what do you experience has assisted CIS in maintaining/increasing their security the most?

Section 3: Framework/legislation

11. Are there any frameworks/legislations you are implementing when it comes to security/resilience in CIS?
12. What does the given framework address when and how?
13. Have you heard of the NIST framework and is it being used in your type of organization?
14. How come no other frameworks are implemented? Especially the most known one such as NIST?
15. What do you think needs to change for you to implement other known frameworks such as NIST?
16. Do you feel that the framework/ policies could be implemented differently? If so, how?

Section 4: Resilience

17. How would you describe resilience in your given sector?
18. How do you achieve resilience in your given sector both on organizational level and technical?
19. Which parameters do you use to measure resilience/ progress?
20. What type of strategies and goals do you have/use to increase the security and resilience of CIS/energy sector?
21. How do you increase the awareness of employees of resilience?
22. What training is performed when it comes to security and resilience?
23. How often does your organization conduct training?
24. What do you consider the biggest challenges related to resilience?
25. Do you have other potential challenges that you experience as a bottleneck when it comes to resilience?

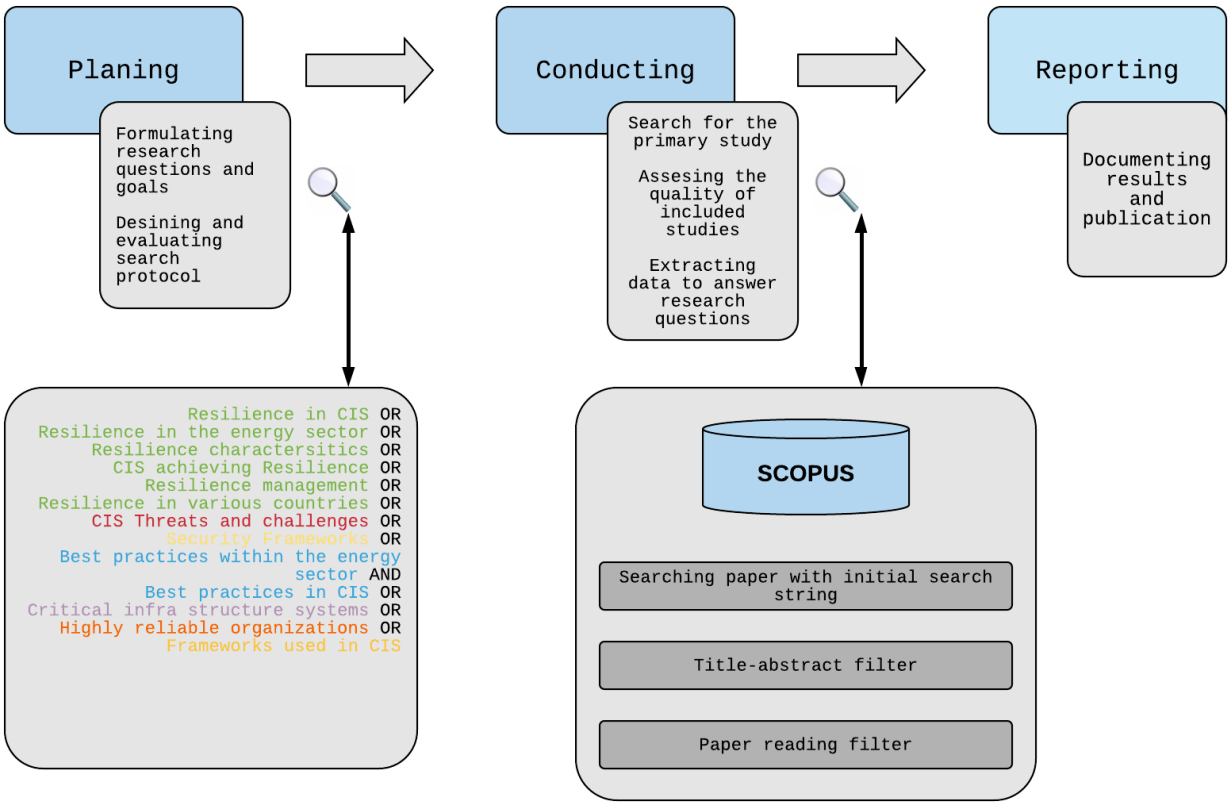
Section 5: Practices

26. Are these training performed for CERT teams or for the organization as whole?
27. What security training or practice has worked for you?
28. What security training or practice has not worked for you?
29. Do you sometimes not follow certain security practices, if yes why?
30. Do you think others in your organization do not follow certain security practices? If yes, why?

Section 6: Closing-up

31. Do you have anything else you like to add?

Appendix 2 Literature Review Search Process



Appendix 3 Interview Guide

Thank you for participating in this interview with us. The purpose of this interview is to investigate resilience in the energy sector, practices used to achieve it, and how this is carried out to increase awareness of the employees. And to potentially discover what works, what does not work and potential best practices.

This interview is anonymous, we will NOT write any personal information about our interviewee, any personal information record will not be transcribed or added in the document and all recordings will be deleted at the end of the master delivery, estimated date: 10.06.2021. The interviewee stands free to refuse to answer a question without given reason for it. The interviewee understand that this interview and information gathered from it, will be used in the master thesis “Resilience & security in critical infrastructure within the energy sector” and gives consent for the students of UiA under the Master: cyber security: Eirik Andre Stålesen & Shiwan Hassan, to use the interview and record in their master thesis.

The interview will ask questions about how the employee has experienced security practices, if they have some understanding of resilience, and how this impacts their

organization and how well certain practices work for the employee. The estimated time for this interview is 45 minutes.

Section 1: General information about the interviewee

2. Position role in the organization, work experience in the organization
3. What do you work with daily?
4. Have you participated in any relevant security, framework, or resilience projects?
5. What was the goal of the project?
6. Did you have any challenges?

Section 2: Security

7. What type of threats & challenges are critical infrastructures facing today (energy sector)?
8. What do you consider to be the biggest challenges related to security in CIS?
9. How are these security challenges & threats addressed in CIS?
10. Can you explain the necessary measurements taken to main/increase security of CIS both on organizational and technical level?
11. From all the measurements implemented, what do you experience has assisted CIS in maintaining/increasing their security the most?

Section 3: Framework/legislation

12. Are there any frameworks/legislations you are implementing when it comes to security/resilience in CIS?
13. What does the given framework address when and how?
14. Have you heard of the NIST framework and is it being used in your type of organization?
15. How come no other frameworks are implemented? Especially the most known one such as NIST?
16. What do you think needs to change for you to implement other known frameworks such as NIST?
17. Do you feel that the framework/ policies could be implemented differently? If so, how?

Section 4: Resilience

18. How would you describe resilience in your given sector?
19. How do you achieve resilience in your given sector both on organizational level and technical?
20. Which parameters do you use to measure resilience/ progress?
21. What type of strategies and goals do you have/use to increase the security and resilience of CIS/energy sector?
22. How do you increase the awareness of employees of resilience?
23. What training is performed when it comes to security and resilience?
24. How often does your organization conduct training?
25. What do you consider the biggest challenges related to resilience?
26. Do you have other potential challenges that you experience as a bottleneck when it comes to resilience?

Section 5: Practices

27. Are these training performed for CERT teams or for the organization as whole?
28. What security training or practice has worked for you?
29. What security training or practice has not worked for you?
30. Do you sometimes not follow certain security practices, if yes why?
31. Do you think others in your organization do not follow certain security practices? If yes, why?

Section 6: Closing-up

32. Do you have anything else you like to add?

Appendix 4 Consent Form

Vil du delta i forskningsprosjektet

" Sikkerhet og resiliens i kritisk infrastruktur innenfor energi sektor."

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å **avdekke sikkerhet og resilience knyttet til kritisk infrastruktur.** I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Vi ønsker å se hva sikkerhet og resiliens betyr for organiasjoner som har kritisk infrastruktur systemer og eventuelt hvordan oppnår de ønsket nivå av resiliens? Vi fokuserer på å forstå hva resiliens er i energi sektor, hvordan de oppnår det og hvilken best practises blir brukt innen for angitt sektor i Norge. Hensikten er om å avdekke om resiliens betyr det samme for forkjellige infrastrukturer i samme land eller andre, hva som gjøres for å beskytte sikkerheten til en kritisk infrastruktur og hvordan oppnår de det.

Hvem er ansvarlig for forskningsprosjektet?
Universitet i Agder er ansvarlig for prosjektet, i samarbeid med NC Spectrum.

Hvorfor får du spørsmål om å delta?
Studiet ble trukket gjennom samarbeid med NC Spectrum og instituttets og veileders nettverk, samt aktører som vi anser som relevant innen for kritisk infrastruktur og energi sektor.
Kontakt opplysningene kan være innhentet gjennom NC-Spectrum eller Universitet i Agder.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det å svare på spørsmål stilt i intervjuer. Vi samler inn navn, epost eller telefonnummer i tilfelle det inngår kontaktinformasjon. Vi skal også ha lydopptak som transkriberes. Bakgrunnsopplysninger som vil kunne identifisere en person vil bli slettet og anonymiseres før publisering.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Prosjektgruppe som består av to masterstudenter, samt veileder ved Universitet i Agder vil ha tilgang til opplysningene vi samler inn, før de anonymiseres.

- Vi vil unngå personlig informasjon av deltakerne, slik at vi ikke lagrer navn og kontaktopplysninger av deltakerne, alt av informasjon som blir tatt opp lydopptaket vil lagres på instituttets godkjente datalagringstjeneste: OneDrive. Hvis navn eller kontakt opplysninger blir tatt opp i lydfil, vil de ikke ble transkribert, og slettet ved slutten av prosjektet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er

10.06.2020. Ved prosjektslutt destrueres opptak og lagrede personlige data, og gjengis kun i anonymisert form.

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

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

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

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Devendra Bahadur Thapa ved Universitetet i Agder, veileder for masteroppgaven (+47 952 56 430, devinder.thapa@uia.no)

- Vårt personvernombud: Ina Danielsen (+47 381 42 140 ina.danielsen@uia.no).

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig
(Veileder) Eirik Andre Stålesen eirias16@uia.no
Shiwan Hassan shiwah16@uia.no

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet: Motstandskraft og sikkerhet i kritisk infrastruktur innen energisektoren, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca 10.06.2021

(Signert av prosjektdeltaker, dato)