Mari Langås
Sanna Løfqvist

Cybersecurity Preparedness Exercises in Smart Grid: Collaboration With Suppliers During Incident Response

Master's thesis in Communication Technology
Supervisor: Basel Katt
Co-supervisor: Martin Gilje Jaatun, Thomas Haugan
June 2021

Master's thesis

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

NTNU
Norwegian University of
Science and Technology

Mari Langås
Sanna Løfqvist

Cybersecurity Preparedness Exercises in Smart Grid: Collaboration With Suppliers During Incident Response

Master’s thesis in Communication Technology
Supervisor: Basel Katt
Co-supervisor: Martin Gilje Jaatun, Thomas Haugan
June 2021

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

NTNU
Norwegian University of
Science and Technology

Title: Cybersecurity Preparedness Exercises in Smart Grid: Collaboration with Suppliers During Incident Response

Students: Mari Langås and Sanna Løfqvist

Problem description:

Today's society is highly dependent on reliable power supply. Similarly to the rest of the society, the electrical energy sector is going through a digitalization process to increase efficiency. This includes the introduction of Information and Communications Technology (ICT) and other emerging technologies, resulting in a new generation power grids called smart grids. The smart grid makes it easier and faster to operate and handle incidents in the power grid, but it also results in the introduction of new attack scenarios and a widened attack surface. In recent years, there has been an increasing number of attacks against the power grid. Consequently, the electrical energy sector needs to have well-functioning contingency plans and incident response processes.

With smart grids, the sector has experienced an increase in the number of external parties that are involved in the power supply. As both the supply chain and the systems become more complex, the power supply becomes dependent on suppliers and the complexity of the incident management process increases. This results in a more prominent risk for supply chain attacks. Therefore, the Distribution System Operators (DSOs) and their suppliers need to adapt to the changing threat landscape and prepare to handle cyber attacks across the whole supply chain.

This thesis aims at contributing to enhance Norwegian DSOs' ability to conduct effective cybersecurity preparedness exercises that improve collaboration with suppliers during incident management. This will be achieved by studying attack scenarios and designing preparedness exercises that require involvement from suppliers. Furthermore, an investigation into factors that can make it easier for suppliers to participate in preparedness exercises will be performed.

Date approved: 2021-02-11

Supervisor: Basel Katt, IIK

Cosupervisor: Martin Gilje Jaatun, SINTEF Digital
Thomas Haugan, IEL

Abstract

The introduction of Information and Communications Technology (ICT) into conventional power grids has resulted in a digitalized power grid, commonly referred to as smart grid. Smart grid enables a more efficient and robust operation and incident handling. However, it can also lead to increased risk and new threats due to more complex systems and longer supply chains. Recent attacks and threat reports indicate that the electrical power grid is an attractive target, promoting the need for well-prepared incident management processes that involve external suppliers. Consequently, it is necessary to improve Distribution System Operators' (DSO) ability to conduct effective cybersecurity preparedness exercises with their suppliers. This thesis addresses this through the development of scenarios for collaborative preparedness exercises and an investigation into which factors may contribute to making it easier to include suppliers in preparedness exercises.

This thesis' primary data collection methods are a literature study and qualitative interviews with DSOs and suppliers. Based on the data collection, a set of scenarios with corresponding discussion questions was created. The final drafts of the scenarios have been adjusted based on feedback gathered from both DSOs and authorities. For one of the scenarios, *Ransomware*, the additional documents necessary to use the scenario in a discussion exercise were created, and an exercise was conducted with a DSO. Feedback on the exercise was gathered through a joint first impression evaluation directly after the exercise and an individual questionnaire that was distributed the following day. In addition, by performing an analysis of the collected data, a list of factors that may make it easier to include suppliers in preparedness exercises was created.

The results from the thesis consists of empirical results from the data collection and a set of created scenarios with associated documents for discussion exercises. From the feedback on the scenarios and the results from the conducted discussion exercise, it is shown that the scenarios can be used in exercises and that they are likely to provide value to the industry. Furthermore, we identified seven factors that can simplify the involvement of suppliers in exercises. These include involving the suppliers earlier in the incident management processes and taking steps to make the organization of and participation in exercises less resource-demanding. Additionally, it is important to set clear requirements for the suppliers regarding their involvement, either in legislation from the authorities or in the DSOs' contracts with suppliers.

Sammendrag

Introduksjonen av informasjons- og kommunikasjonsteknologi (IKT) i det tradisjonelle strømnettet har resultert i et digitalisert strømnett, ofte referert til som smart grid. Smart grid gjør driften og hendelseshåndteringen mer effektiv og robust, men kan samtidig også føre til økt risiko og nye trusler på grunn av mer komplekse systemer og lengre leverandørkjeder. Nylige angrep og trusselvurderinger indikerer at strømnettet er et attraktivt mål, noe som fremmer behovet for godt forberedte prosesser for hendelseshåndtering som involverer eksterne leverandører. Det er derfor nødvendig å forbedre nettselskapenes evne til å gjennomføre effektive cybersikkerhetsøvelser med sine leverandører. Denne studien adresserer dette gjennom utviklingen av scenarioer til bruk i beredskapsøvelser og en undersøkelse av hvilke faktorer som kan bidra til å gjøre det enklere å inkludere leverandører i beredskapsøvelser.

Hovedmetodene som ble brukt til datainnsamling i denne studien var en litteraturstudie og kvalitative intervjuer med nettselskaper og leverandører. Basert på de innsamlede dataene ble et sett med scenarioer og tilhørende diskusjonsspørsmål laget. De endelige utkastene er justert basert på tilbakemeldinger fra både nettselskaper og myndigheter. For ett av scenarioene, *Ransomware*, ble de tilhørende dokumentene som er nødvendig for å bruke scenarioet i en øvelse laget og en øvelse gjennomført med ett nettselskap. Tilbakemeldinger fra øvelsen ble samlet inn gjennom en felles førsteinntrykksevaluering rett etter øvelsen og en spørreundersøkelse som ble sendt ut neste dag. I tillegg, ved å gjennomføre en analyse av den innsamlede dataen, ble en liste over faktorer som kan bidra til å gjøre det enklere å inkludere leverandører i beredskapsøvelser utarbeidet.

Studiens resultater består av empiriske resultater fra datainnsamlingen og en samling av scenarioer med tilhørende dokumenter for diskusjonsøvelser. Tilbakemeldingene på scenarioene og resultatene fra den gjennomførte øvelsen viser at scenarioene kan bli brukt i øvelser og at det er sannsynlig at de tilfører verdi til bransjen. Videre identifiserte vi syv faktorer som kan forenkle det å involvere leverandører i øvelser. Disse inkluderer å involvere leverandørene tidligere i hendelseshåndteringsprosessen og innføre tiltak for å gjøre organiseringen og deltakelsen i øvelser mindre ressurskrevende. I tillegg er det viktig å stille klarere krav til leverandører om deres involvering, enten i lovgivning fra myndigheter eller i nettselskapenes kontrakter med leverandørene.

Preface

This master's thesis marks the conclusion of the five-year Master of Science (MSc) in Communication Technology program at the Norwegian University of Science and Technology (NTNU).

We would like to thank our supervisors Martin Gilje Jaatun and Thomas Haugan, and responsible professor Basel Katt for the guidance and support throughout this project.

We would also like to thank the organizations that contributed to the interviews for taking part in this study, and sharing their ideas, views, and opinions. A special thanks to the DSO and suppliers that participated in the conducted preparedness exercise for setting aside the time and resources necessary for this.

Lastly, we want to thank our family and friends for the support during this project and the past five years.

Mari Langås and Sanna Løfqvist
Trondheim, June 2021

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

AMI Advanced Metering Infrastructure.

AMS Advanced Metering System.

CEO Chief Executive Officer.

CFCS Centre for Cybersecurity.

CFO Chief Financial Officer.

DDoS Distributed Denial of Service.

DSB Norwegian Directorate for Civil Protection.

DSO Distribution System Operator.

ENISA European Network and Infomation Security Agency.

ICS Industrial Control Systems.

ICT Information and Communications Technology.

IEC International Electrotechnical Commission.

IP Internet Protocol.

IRT Incident Response Team.

ISIM Information Security Incident Management.

ISO International Organization for Standardization.

ISP Internet Service Provider.

IT Information Technology.

KBO Kraftforsyningens beredskapsorganisasjon.

NIST National Institute of Standards and Technology.

NSM Norwegian National Security Authority.

NTNU Norwegian University of Science and Technology.

NVE Norwegian Water Resources and Energy Directorate.

OT Operational Technology.

PCS Process Control Systems.

SCADA Supervisory Control and Data Acquisition.

SLA Service Level Agreement.

TSO Transmission System Operator.

Chapter 1 Introduction

The electrical power grid is considered one of the most vital critical infrastructures in modern society and almost all essential societal functions rely heavily on electric power for their operation. As the world is becoming increasingly interconnected and digitalized due to rapid technological development, this is also the case for the electrical energy sector. The digitalization involves the incorporation of Information and Communications Technology (ICT) into the traditional power grid, leading to a smarter grid and new functionalities. Smart grid makes the operation and incident handling of the power grid more efficient and robust due to monitoring, automation, and remote control of components. To achieve this, the Distribution System Operator (DSO) has to make use of new equipment and systems delivered by suppliers, leading to more complex systems and longer supply chains. As a result, smart grid also gives rise to new threats to the power supply, a widened attack surface and new potential consequences of attacks.

The electrical energy sector is one of the most frequently targeted sectors by cyber attackers [Ste19]. In an international context, there have been examples of large-scale attacks in the last few years, the most famous one being the cyber attack on the Ukrainian power grid in 2015, resulting in hundreds of thousands of people left without electricity [Rob16]. According to the annual national threat assessment *Risiko 2021* [Nas21] from the Norwegian National Security Authority (NSM), the Norwegian electrical energy infrastructure is at risk of being a target of cyber operations such as espionage, data breaches, and advanced attacks from both state actors and criminals. The introduction of smart grid results in increased automation and integration in the power grid and blurs the line between Operational Technology (OT) and Information Technology (IT). Accordingly, attacks on the power grid can cause more severe consequences since systems that initially were not intended to exist outside closed networks are now connected to the rest of the network and exposed to various threats. When our most important societal values are transferred to the digital domain, attacks causing long-lasting power outages can wreak havoc in all parts of society.

As the risk of successful cyber attacks against the electrical energy sector increases, the need for well-prepared incident management processes for cybersecurity incidents becomes evident. The dynamic and complex threat landscape makes it challenging to adopt security measures fast enough, making preparedness exercises an important tool to detect, assess and respond to cybersecurity incidents. The DSOs' dependence upon an increasing number of suppliers creates a need for close collaboration between all involved parties in the supply chain when an incident occurs, especially the suppliers of the affected systems. In a report on the customer and supplier relationships in the electrical energy sector from the Norwegian Water Resources and Energy Directorate (NVE) [KL18], they recommend that Norwegian DSOs conduct preparedness exercises and review incidents management plans with their suppliers. However, Eriksen and Gunabala [EG20] investigated the collaboration of DSOs and their suppliers in the management of potential cybersecurity incidents in their Process Control Systems (PCS). According to their findings, suppliers are rarely involved in cybersecurity preparedness exercises, even though there is a need for it. Few studies have investigated how the collaboration between DSOs and suppliers during incident management can be improved by creating appropriate attack scenarios that can be used in preparedness exercises, and this is the motivation for this project.

1.1 Research Questions

This thesis aims to enhance DSOs' ability to conduct effective cybersecurity preparedness exercises that improve collaboration with suppliers during incident management. This will be achieved by studying and designing attack scenarios and a preparedness exercise that requires involvement from suppliers. Furthermore, an investigation into factors that can make it easier for suppliers to participate in preparedness exercises will be performed. Through literature reviews, qualitative interviews with DSOs and suppliers, as well as validation of the results through a preparedness exercise, the following research questions will be answered in this thesis:

- RQ 1: What are scenarios for preparedness exercises that can improve the collaboration between DSOs and suppliers? And how can these be used in exercises?
- RQ 2: Which factors could make it easier for suppliers to participate in preparedness exercises with DSOs?

1.2 Contributions

The contributions from this thesis will be of two types. The first contribution will be a set of created scenarios and associated documents for discussion exercises that can be used to improve the collaboration between DSOs and suppliers. The other contribution is empirical results from the data collection. This data is based on the information collected in the interviews with DSOs and suppliers and feedback from stakeholders in the electrical energy sector. The created scenarios and exercise documents are presented in Chapter 4 Created Scenarios and Exercise, whereas the empirical results are presented in Chapter 5 Data Collection Results.

1.3 Scope and Limitations

The scope of this thesis is limited to the Norwegian electrical energy sector and the involvement of suppliers in preparedness exercises as a part of the incident management process. Thus, the results in this thesis are mainly based on information obtained about Norwegian DSOs and their suppliers of ICT services and systems.

Due to the time constraint of 21 weeks and a lack of answers to our request, the number of organizations interviewed is limited to four DSOs and two suppliers. This number might be less than desired to create a result that can be generalized for the entire industry. As the primary method of collecting data in this thesis was through interviews, another limitation can be that we have limited experience in conducting interviews. The validity, reliability, and generalizability of this study are further discussed in Section 3.3.

1.4 Outline

This section provides an outline for the chapters of this thesis.

Chapter 2 presents relevant background material for this project. It gives an introduction to the Norwegian electrical energy sector, the current threat landscape, the information security incident management process and lastly preparedness exercises and existing solutions.

Chapter 3 introduces the research methods used to conduct this thesis. It includes the method for the literature study, the qualitative interviews, and the scenario and exercise development.

Chapter 4 presents the produced scenarios and the additional exercise material.

Chapter 5 presents the data collection results from the conducted interviews, the feedback on the scenarios and the evaluation of the preparedness exercise.

Chapter 6 discusses each of the research questions in light of the data collection results.

Chapter 7 provides a conclusion and proposes potential future work.

Appendix A includes a collection of the created scenarios and a separate document for each scenario, containing the scenario descriptions and discussion questions for each part.

Appendix B provides examples of the documents that were created as exercise material for the discussion exercise. In addition, it contains a guide for how to use the created scenarios in a discussion exercise.

Appendix C contains the interview guides used for the interviews with the DSOs and the suppliers.

Wordlist

The following wordlist contains the translations of terms from Norwegian to English that have been used in this thesis.

Briefing	Øvingsdirektiv
Contingency plan	Beredskapsplan
Data Collector	Evalueringsansvarlig
Exercise Facilitator	Øvingsleder
Facilitator guide	Veileder for øvingsleder
First impression evaluation	Førsteinntrykksevaluering
ICT security coordinator	IKT sikkerhetskoordinator
Incident response plan	Innsatsplan
Operational network	Driftssentralnett
Participants guide	Øvelsesdokument til deltakere
Playbook	Dreiebok
Preparedness coordinator	Beredskapskoordinator
Sensitive Power System Information	Kraftsensitiv informasjon

Chapter 2
Background

This chapter presents relevant background material to gain an understanding of the state of the Norwegian electrical energy sector, the incident management process and preparedness exercises as a tool. First, Section 2.1 provides an introduction to the electrical energy sector in Norway, before the current threat landscape is presented in Section 2.2. Then, insight into the information security incident management process is given in Section 2.3. Section 2.4 contains an introduction to preparedness exercises, training, and the use of attack scenarios. Finally, Section 2.5 and 2.6 focuses on existing solutions and previously conducted work in the field.

2.1 The Electrical Energy Sector in Norway

> In today's society electricity is a necessity. Almost all important societal tasks and functions are critically dependent on a well-functioning power system with a reliable power supply [Olj12]. (Translated from Norwegian.)

The Norwegian electrical energy sector is regarded as a critical infrastructure sector, meaning that the society is highly dependent on its functioning. Should it fail, severe consequences will fall upon other critical societal functions such as transportation, healthcare and communication. The inter-dependencies between different critical infrastructures lead to an interconnected and complex network, and disruptions in the power supply can quickly lead to chains of negative impacts and harm to citizens.

There are mainly two entities in the electrical energy sector that process and deliver the produced power: Transmission System Operators (TSOs) and Distribution System Operators (DSOs). The TSOs provide the transmission infrastructure that connects producers with consumers in a nationwide system and is used to transport the power from the producers to different geographical locations. The DSOs, on the other hand, are responsible for the distribution out to the end-users. The

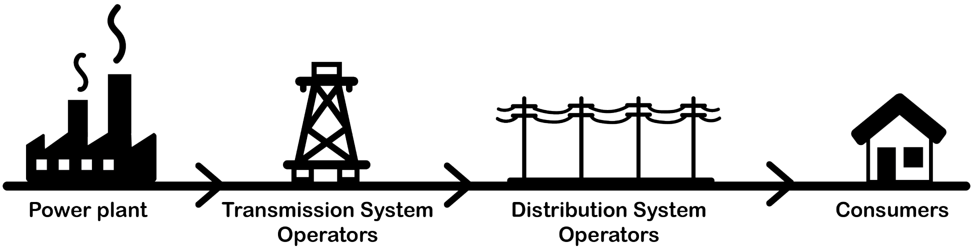


Figure 2.1: Traditional power grid with one-directional power flow and centralized power generation. Adapted from [E.D14].

traditional power grid is based on a one-directional distribution of electricity and a more centralised power generation, as illustrated in Figure 2.1. Statnett is the TSO in Norway, while NVE reported that there were approximately 104 DSOs that operate their own distribution grid in 2019 [Nor20].

Operational Technology (OT) is the use of hardware and software to monitor and control physical processes, devices and infrastructure [For21]. In the electrical energy sector, OT refers to components used to ensure a safe and reliable generation and delivery of energy. Industrial Control Systems (ICS) are included in the category of OT systems, and the largest subgroup of ICS is Supervisory Control and Data Acquisition (SCADA) systems [ENI21]. These systems are responsible for the monitoring and control of the infrastructure in the power grids. In traditional power grids, the OT systems have been physically separated from the Information Technology (IT) infrastructures and the Internet. We are currently seeing a digital transformation towards cyber-physical systems (CPS) typically denoted Industry 4.0 or the fourth industrial revolution [iS17]. As a consequence of this transformation, we see a drive towards data-driven and remote operations, causing a convergence between IT and OT [MJV17]. This requires cooperation between process control workers and IT workers, which can lead to challenges due to cultural differences and a lack of understanding of each other's domains and differences in priorities [LTJ11]. The continuous development within IT systems enables OT systems to gain new functionalities, making them more efficient in terms of both cost and resources. In addition, it enables the possibility for more secure, reliable and streamlined operations [Bab18]. However, a consequence of this interconnection is that the OT systems become vulnerable to the attacks that previously were only associated with IT infrastructure.

The introduction of smart grid has further pushed this interconnection between OT and IT and is rapidly blurring the distinction between the two categories. Smart grids were proposed as a way to increase power utilization, efficiency and reliability.

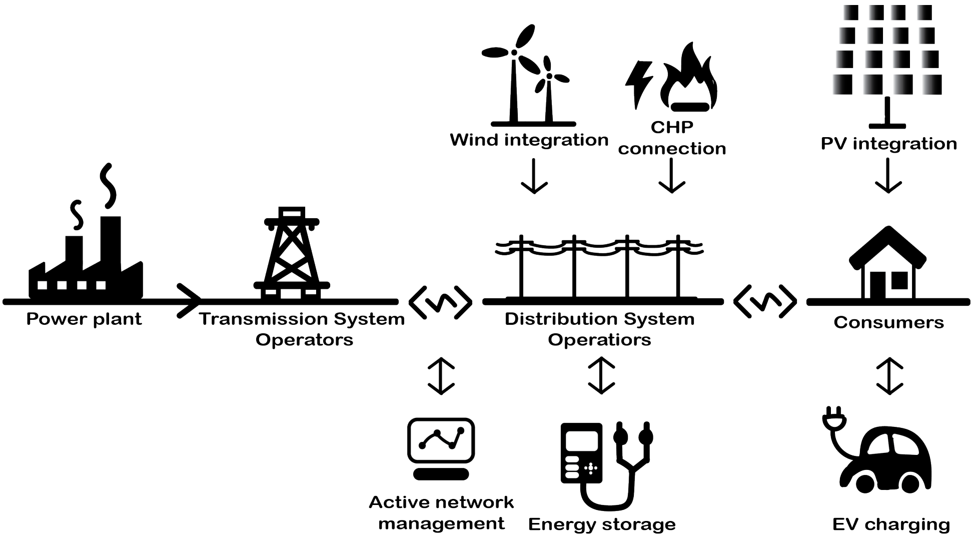


Figure 2.2: Smart grid infrastructure as a distributed network with bidirectional power flow. Adapted from [E.D14].

In addition, it facilitates easier integration of renewable energy resources, which is essential with the changing power landscape and the focus on green energy sources. It is characterized by the bidirectional flow of electricity and data between the various stakeholders in the electricity market, which can be analyzed to optimize the grid, enhance monitoring, enable faster fault detection and develop new services [iS19]. Figure 2.2 illustrates this bidirectional connection, allowing end consumers to act like producers by distributing excess electricity to other consumers. This is achieved by utilizing expansive sensor networks combined with high bandwidth communication technologies and computational intelligence.

The installation of smart meters, or Advanced Metering System (AMS), at all consumer endpoints is a part of the smart grid development, and is essential in enabling the enhanced monitoring and efficiency of the smart grids. These meters register the electricity consumption every hour or more often and automatically send information about the consumption to the DSO [Nor19]. This results in a quicker and more correct consumption reading and a more accurate basis for billing consumers. The meters will have two-way communication between the smart meter and the DSO, through which the consumer can receive real-time information about consumption and prices via a smartphone or in-home display. The communication is enabled by the Advanced Metering Infrastructure (AMI), which connects the dots between the customer and the DSO. It will also enable automatic control of devices and remote access to power switch functionality located in the smart meters [Evj17]. The power switch allows the DSO to disconnect the end consumer from the grid. The system in AMI that is responsible for the control of the smart meters is the head-end system, also known as the meter control system [Bru13]. The DSOs are obligated to install security systems to ensure that personal information is not disclosed and that only authorized persons have access to the systems in the AMI [Nor16].

Bidirectional communication is vital for the utilization of the sensor and control networks and the AMS. The combination of these different systems enables the smart grid to aid in fault prevention, detection and correction, enabling DSOs to detect and manage outages early. This is achieved by utilizing the sensor network to monitor values like voltage and current amplitudes and thermal variations [Kab16], and gather the various measurements from sensors and smart meters. Moreover, to fully take advantage of the smart grid infrastructure, it is necessary to have access to a high bandwidth communication system.

2.1.1 Security Properties of Smart Grid

Both the convergence of IT and OT and the implementation of a smarter power grid requires an adaption of the security properties in the energy sector. The most important properties of information security are defined in the ISO/IEC standard as confidentiality, integrity and availability, often referred to as the CIA triad [Int18].

Confidentiality The introduction of the smart meters into the consumers' homes and the automatic reporting about consumed power is the most noticeable change for the consumer. Even though this will help the consumers control their consumption and possibly reduce it, it will also have implications for the citizens' privacy. This data needs to be well protected, during both transfer and storage, to avoid unauthorized persons or organizations gaining access [LTJ11].

Integrity Another aspect of the AMS is that the consumers are given physical access to equipment connected to the grid. This physical access to electronic components opens for much more advanced tampering and possible damage than network access only. Therefore these devices must be tamper-proof, and there must be ways to confirm the accuracy and trustworthiness of the data.

Availability As electricity is one of the most fundamental infrastructures in modern society, the power grid generally operates with high requirements for reliability, robustness and availability. This security property is regarded as the most important in smart grids due to the fact that compromising availability disrupts access to information in a smart grid. Down-time usually has substantial financial and societal consequences, and therefore the highest priority is keeping the system running in operation with high availability.

2.1.2 Stakeholders

This section introduces some of the regulatory or legislative authorities and advisory organizations that exist within the electrical energy sector in Norway.

The Norwegian Water Resources and Energy Directorate (NVE)[1] is responsible for the management of Norway's water and energy resources. In addition, they have the overall responsibility for maintaining the national power supplies and coordinating the work with preventive safety and emergency preparedness regarding the power supply.

KraftCERT[2] is an advisory organization for the electrical energy sector and was founded by three large organizations in the sector on an initiative from NVE. They are working for more secure and robust ICS by making the sector aware of relevant vulnerabilities and threats. Their purpose is to support the electrical energy sector in preparing for, mitigating and handling digital attacks.

Kraftforsyningens beredskapsorganisasjon (KBO)[3] is the Norwegian organization for energy emergency preparedness and its purpose is to coordinate the preventive security and preparedness in the power supply. It consists of NVE and all the organizations responsible for the collective Norwegian power supply, including Statnett and the DSOs. The participants in the organization are referred to as units. The Norwegian Energy Act from 1990 sets requirements for the electrical energy sector in Norway with regard to production, distribution, use and emergency preparedness. In addition, the *Regulation on security and preparedness in the energy supply* [Olj19], named *Kraftberedskapsforskriften* in Norwegian, was introduced as a supplement with regards to safety and emergency preparedness. Together they form jurisdictions and regulations that contribute to Norway having a good security of supply of electricity and preparedness for situations that deviate from normal operations. According to *Kraftberedskapsforskriften*, all DSOs shall have a contingency plan and both an ICT security coordinator and a preparedness coordinator in the organization. The responsibilities of these two roles are to have an overview of the ICT security and emergency preparedness work in the organization and to be contact points for the emergency preparedness authority on each field. In addition, the DSOs must secure digital information systems so that confidentiality, integrity and availability are upheld and conduct preparedness exercises for extraordinary incidents. All units are responsible for ensuring that it meets the requirements in the regulation. *Kraftberedskapsforskriften* states the following about the implementation of preparedness exercises:

[1] https://www.nve.no/english/

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

[3] https://www.nve.no/damsikkerhet-og-kraftforsyningsberedskap/kraftforsyningsberedskap/organisering-av-kraftforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/

> § 2–7.Exercises
> *KBO units shall conduct exercises with such content and scope that the unit maintains and improves its competence to manage all relevant extraordinary situations. The organizations should have an exercise plan that covers several years and conduct at least one annual exercise* [Olj19]. (Translated from Norwegian.)

Kraftberedskapsforskriften also specifies requirements for the use of suppliers. Each DSO is responsible for ensuring that the suppliers meet the requirements regarding information security and confidentiality for sensitive information. Additionally, each DSO should have the right to control and audit the suppliers' compliance to these requirements. To do this, the DSOs should implement systems and routines for checking the compliance, to verify that the requirements are upheld [Olj19]. There are also special requirements for suppliers that have remote access to power switches or that deliver operational systems. These suppliers must be located in countries that are members of EFTA, EU or NATO.

In addition, *Kraftberedskapsforskriften* defines what kind of information that should be regarded as *sensitive power system information*. This applies to information that contains specific or in-depth details about the power supply that can be used to harm vital infrastructure and systems or affect important functions for the power supply. Examples of information included in this definition are details about all systems that handle important operational control functions, the location of cables and backup substations and the content of performed risk and vulnerabilities assessments that can be used to cause deliberate damage.

2.1.3 Outsourcing to Suppliers

A supplier is a person or organization that provides something needed such as a product or service.[4] In the context of the electrical energy sector, the customer is often another organization and the service is often either hardware or software systems. After the Norwegian Energy Act was introduced, it resulted in a restructuring of the electrical power market and of Norwegian DSOs. One of the consequences was that outsourcing became more common and the current digitalization of the power grid has further increased the need for it. The benefits from outsourcing are usually a higher quality of both products and services by taking advantage of the suppliers' expertise and better cost regulation. Thus, allowing the DSOs to focus on their core business areas [AAF$^+$08]. However, as pointed out in Meld. St. 25 [Olj16] from 2016, there is a risk that the DSOs may become too dependent upon suppliers. In 2017, NVE released a report that investigated the state of information security

[4] https://www.lexico.com/en/definition/supplier

in the power supply [SKP+17]. Here, they concluded that as many as 8 out of 10 companies in the electrical energy sector are dependent on their suppliers to handle ICT incidents and recover the systems after failure. The power supply's ICT security and preparedness are therefore largely dependent on the suppliers' ICT security.

As a result of the DSOs dependence upon their suppliers, NVE made a report in 2018 that investigates the ICT security in connection to outsourcing in the electrical energy sector and challenges in the relationship between DSOs and the suppliers [KL18]. The report disclosed that it is hard for the DSOs to keep track of the security throughout the supply chain, and both the DSOs and the suppliers only have control of up to a maximum of two links in the supply chain. Most DSOs have some form of contract with their suppliers regarding the security requirements of the service provided. However, it is challenging to verify these requirements, and most DSOs do not take advantage of the opportunity to audit their suppliers. One of the recommendations in the report is that the DSOs should conduct exercises and reviews of the preparedness plans with their suppliers. NVE also concludes that it is necessary to take a closer look at the preparedness and interaction between the different entities in a stressful environment.

The outsourcing of services and components in the Norwegian electrical energy sector leads to increased complexity in the networks. This can complicate the incident management process, cause problems with coordination between stakeholders, and open up the risk of supply chain attacks. As a consequence of the relatively small size of the Norwegian electrical energy market when viewed in a global context, the number of suppliers in the market is limited by the number of possible customers. A report issued in 2021 from the Office of the Auditor General of Norway (*Riksrevisjonen*) [Rik21], states that many of the DSOs use the same suppliers of ICT systems. This leads to a concentration of suppliers where attackers can manage to disrupt the power supply across the country by only targeting a small number of suppliers. According to a report on the regulation of cybersecurity in the electrical energy sector [HHT+17], this creates a concentration of risk where the dependence on a product or service increases the sector's overall risk.

2.2 Threat Landscape

The technological changes to the power grid lead to a new threat landscape where additional threats and vulnerabilities make the systems more susceptible to cybersecurity incidents. During the past few years, the amount of targeted attacks has risen, and there have been several attacks that have included targets in the energy sector [Wue14]. According to the NSM, the Norwegian electrical energy sector is considered to be a potential target of malicious activity performed by both state actors and criminals [Nas21]. From 2016 to 2017 approximately 70 % of the organizations in the Norwegian energy sector experienced unwanted cybersecurity incidents [SKP+17]. The increasing complexity of the digital supply chains results in new vulnerabilities and dependencies that the threat actors can exploit. According to threat reports from Symantec from 2018 and 2019, the number of software supply chain attacks increased by 200 % in 2017 [Sym18] and 78 % in 2018 [Sym19]. As a consequence of the longer supply chain, there is an increasing need for a well-functioning collaboration across the supply chain in case an incident should occur. The attacks mentioned below demonstrates that ICS and the electrical power industry and its suppliers are attractive targets for cyber attacks.

Stuxnet Stuxnet was first discovered in June 2010 and is a malware that targets industrial control systems [LTC12]. It is a special type of malware called worm, that can spread by replicating itself without any human interaction after the initial infection has happened.[5] Even though it was first discovered in 2010, samples of the worm dating back to June 2009 have been found. The first wave of Stuxnet attacks is believed to have started in Iran, consisting of 10 initial infections targeting five organizations [LTC12]. It caused irreparable damage to centrifuge equipment at Iranian nuclear facilities [Ste19].

Ukraine 2015 In December 2015, a cyber attack hit the Ukrainian power grid and resulted in approximately 200 000 people left without electricity. This is the first publicly acknowledged cyber incident to result in power outages [Rob16]. It was coordinated against three power distribution companies. The attackers were highly sophisticated and performed long-term reconnaissance to study the environment and execute a synchronized multisite attack. Spear phishing was used to gain access to the business networks of the involved distribution and supply companies. The malware BlackEnergy 3 was used together with KillDisk, but the malware itself did not cause the outage [Rob16]. The malware was used to gain access to the electricity distribution networks, and then legitimate remote access software was abused to cut off power [Rob16].

Ukraine 2016 Almost a year after the 2015 attacks, Ukraine was the victim of another cyber attack that targeted a single transmission substation outside of Kiev. The malware Industroyer, also called Crash Override, was used and initially created a backdoor into the systems for the attackers [Dra17]. Industroyer exploits that the communication protocols used in power supply infrastructure were designed decades ago without security in mind, back when industrial systems were isolated from the outside world. It applies the protocols in the way they were supposed to be used, hence there is no quick patch that can mitigate the attack. This attack was seemingly less damaging than the 2015 attack and attracted much less attention. Because

[5] https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

of the relatively low impact and the large potential of the malware, many security experts believe that this attack was a large-scale test and that the malware has the possibility to be much more damaging [Ant17]. Industroyer is perceived as the largest threat to ICS since Stuxnet, because of its potential to control switches on electricity substation and circuit breakers directly [Ant17].

NotPetya In June 2017, another malware outbreak was discovered in Ukraine. The servers of a Ukrainian accounting software provider was hacked and used to distribute corrupted software updates to their customers [Ste19]. NotPetya uses the EternalBlue Server Message Block (SMB) exploit and gathers user credentials from the infected host to connect to other systems on the network [Log17]. Damage to the electrical energy sector included at least six local electric utilities in Ukraine, but it also spread to many other sectors with damages of more than USD 10 billion [Ste19]. One of the companies that faced the most devastating damages was the danish shipping company Maersk, with around USD 300 million in losses [And18]. The NotPetya attack demonstrated the reach and the destructive power of a supply chain attack.

Other Supply Chain Attacks The report by Livingston et al. [Ste19] covers some cyber attacks that demonstrate that supply chains can pose a threat to the electrical energy sector. The first one is the breach of utility Industrial Control Systems (ICS) through multiple supply chain partners in 2016–2017. The attackers used the watering hole technique by altering commonly visited industry websites to spread malicious content and gather visitors credentials. This was later used to launch attacks and gain access to IT service providers and utilities' corporate networks. The attack did not lead to any outages, but the attackers were able to conduct valuable reconnaissance that can potentially be used in later attacks. The hacker group Dragonfly, who is suspected to be an advanced persistent threat actor backed by a nation-state, is believed to have been behind this attack [Ste19].

The report also discusses the attack on a small cloud service provider in 2018 that impacted the US natural gas, oil and electric power sectors. It is suspected to be ransomware, but it has not been disclosed. This impacted some large power providers where the connection to the platform that provides the pricing, demand models and estimated bills was affected. The attack did not cause any outages, but showed the dependence between sectors and their vulnerability to extensive disruption from a supply chain attack [Ste19].

2.3 Information Security Incident Management

This section provides a definition of both information security incidents and Information Security Incident Management (ISIM) as defined in the ISO/IEC 27035

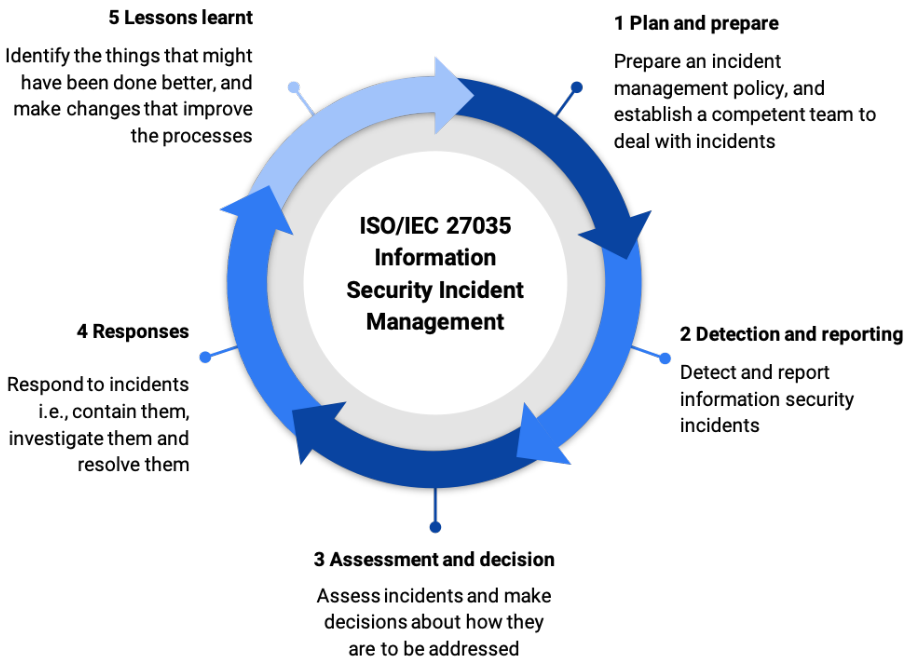

5 Lessons learnt
Identify the things that might have been done better, and make changes that improve the processes
1 Plan and prepare
Prepare an incident management policy, and establish a competent team to deal with incidents
ISO/IEC 27035 Information Security Incident Management
4 Responses
Respond to incidents i.e., contain them, investigate them and resolve them
2 Detection and reporting
Detect and report information security incidents
3 Assessment and decision
Assess incidents and make decisions about how they are to be addressed

Figure 2.3: Illustration of the different stages of the ISO/IEC 27035 Information Security Incident Management process.

standard [Int16].

An information security incident is defined as one or multiple related and identified occurrences that indicate a possible breach of information security or failure of controls, where a breach of information security means a breach in confidentiality, integrity or availability of information. The incident must have a significant probability of harming the organization's assets or compromising its operations to be classified as an information security incident [Int16]. ISIM comprises all the necessary activities when managing such information security incidents and requires a consistent and effective approach. The approach consists of detecting and reporting, as well as assessing and responding to incidents. In addition, it includes an evaluation of the incident management in order to learn from the incident, conduct risk assessments and identify improvements. ISO/IEC 27035 [Int16] concretizes and describes this process by dividing it into five distinct phases, as illustrated in Figure 2.3.

The first phase is an iterative phase that is vital to ensure successful information security incident management. This phase includes preparatory activities such as defining a detailed incident management plan, updating the information security policies, and establishing and training an Incident Response Team (IRT). In addition, the task of designing and developing an awareness and training program for information security incidents and testing the incident management plan fall under this phase. The four other phases are triggered by an actual event and involve using the established information security management schemes defined in the preparation phase. The second phase involves the detection of information security events and the collection of associated information. In addition, either manual or automatic reporting of occurrences of information security events or discovered vulnerabilities, and monitoring and logging of network activity are included in this phase. The third phase involves assessing the gathered information, deciding whether the event classifies as an incident and determining the actions to be made. The fourth phase is the response to the incident, which comprises forensic analysis and recovery from the information security incident. The final phase occurs when the incident has been resolved, and includes learning from and evaluating how the incident was handled and identifying and making improvements to the plans and procedures. The identified improvements are then implemented in the new version of the incident management scheme and are included in the next iteration of the *Plan and prepare* phase.

2.3.1 Other Information Security Guides

In this section, a selection of other relevant information security guidelines are mentioned and presented. This is to highlight the amount of well-documented and accepted guidelines that exists, and that the main essence of all the guidelines comply with each other.

Computer Security Incident Handling Guide, NIST The National Institute of Standards and Technology (NIST) recommends a process for computer security incident management in their report *Computer Security Incident Handling Guide* from 2012 [CMGS12]. They divide the process of handling an incident into four phases: (1) preparation, (2) detection and analysis, (3) containment, eradication and recovery, and (4) post-incident activities. This report provides guidelines for incident handling and analyzing incident-related data to determine the appropriate response.

Incident Handler's Handbook, SANS In the SANS Institute's Incident Handler's Handbook from 2011 [Kra11] they limit the scope of the incident handling process to six phases and includes an incident handler's checklist. The six phases are preparation, identification, containment, eradication, recovery, and lessons learned. The latter is named the most critical phase as it is intended to be used to improve the performance in the event of a similar incident.

Good Practice Guide for Incident Management, ENISA The European Network and Infomation Security Agency (ENISA) published a guide for incident management called *Good Practice Guide for Incident Management* in 2010 [Eur10]. In this guide, they have limited the scope to IT and information security incidents, i.e. incidents that involve computers, networks, and the information contained inside this equipment. The guide from ENISA focuses primarily on incident handling and describes four significant components to this process: detection, triage, analysis and incident response.

NSMs grunnprinsipper for IKT-sikkerhet, NSM In this guide, called *NSMs grunnprinsipper for IKT-sikkerhet* [Nas20], the Norwegian National Security Authority (NSM) have collected the basic concepts and principles that are most relevant for Norwegian organizations to protect their systems. These principles are divided into four categories: identify and map, protect and maintain, detection, and manage and recovery. NSM also states that conducted exercises should include relevant subcontractors and suppliers. Additionally, NSM has constructed a guide with recommendations for maintaining the information security when outsourcing, called *Sikkerhetsfaglige anbefalinger for tjenesteutsetting* [Nas17].

Informationssikkerhed i leverandørforhold, CFCS The national IT security authority in Denmark, Centre for Cybersecurity (CFCS), published a guide on information security in supplier relationships [fC19]. In this guide, CFCS focus on information security in the different stages of a customer-supplier relationship. They recommend that organizations with critical functions should carefully consider what to outsource and not due to their vital systems and sensitive information. In order to do this, they need to conduct proper risk assessments. CFCS recommends that an agreement should be customized, and both parties must be familiar with the required specifications for security. Since suppliers might enter similar agreements with several customers, it is vital to formalize communication details in case of an incident. After the agreement is settled, the customer should be able to monitor and verify that the supplier is in compliance with the agreement.

2.4 Preparedness Exercises

> A preparedness exercise within IT is an exercise in handling non-conformance situations, typically a cybersecurity incident [Mar20]. (Translated from Norwegian.)

Cybersecurity preparedness exercises fall into the category *Plan and prepare* in the incident management process, as presented in Section 2.3. The purpose is to strengthen the capabilities of an organization to respond in case of emergencies.

This should be done by training personnel to respond to situations that deviate from normal operations and make the correct decisions in a stressful situation. It is necessary to have well-documented procedures and clear definitions of the different roles and responsibilities prior to incidents. However, during an incident, it is vital that these procedures and plans can be translated into more dynamic processes, where coordination and improvisations play a much larger role [BM16]. Preparedness exercises provide a way to test the incident management plans on simulated scenarios and improving them by using practical experiences. By giving the employees the opportunity to gain experience in anticipating and responding to incidents, their prerequisites for recognizing and responding to unexpected events will be better. By conducting frequent exercises the organization will be better prepared for unexpected incidents, as it is not possible to plan for all events [HT13].

According to Floodeen et al. [FHT13], all parties who play a role during an incident should be involved in exercises since exercising is a crucial part of the development of mutual understanding and a shared mental model among the members of the IRT. The suppliers who deliver the affected systems will likely have to be involved in incidents concerning those systems. Thus, DSOs will benefit from conducting collaborative exercises with their suppliers [KL18].

It is essential for all organizations to conduct preparedness exercises to strengthen their response capabilities. However, studies show that cybersecurity preparedness exercises are not commonly performed in the electrical power sector [LTJ14, LTJ16]. At some point, all organizations will experience incidents related to cybersecurity, and despite the existing cybersecurity mechanisms, it is still infeasible to prevent all incidents. The attacks described in Section 2.2, together with statistics from NVE [SKP^{+}17], demonstrate that the electrical energy sector is an attractive target for adversaries. When incidents occur, it is vital to have a plan in place for incident handling, as this increases efficiency and facilitates coordination. However, Hove et al. [HTLB14] argues that while plans and procedures are necessary as a basic structure, experienced incident handlers are much more valuable in emergency situations. This experience is best gained by conducting preparedness exercises.

2.4.1 Difference Between Preparedness Training and Exercises

Preparedness training and exercises are often used synonymously and thus also sometimes in the wrong context. According to the Norwegian Directorate for Civil Protection (DSB), training is when an individual's knowledge and skills are tried and developed, whereas exercises target the organization and test its overall knowledge and skills [Dir16a].

Preparedness training is essential to raise the awareness of the staff about what emergencies they may face in the future and developing the skills needed to handle such incidents. Training is a prerequisite for conducting well-functioning exercises and ensures that the participants are prepared and familiar with the plans and procedures defined within the organization. Before conducting an exercise, all the participants must be aware of their roles and responsibilities and be reasonably comfortable with them [GOV15]. The organization should provide their employees with the opportunity to train on processes and procedures in a safe environment before they are subject to the stress of an exercise.

Preparedness exercises are used to test the knowledge of the procedures and plans and how they function. The preparedness level of an organization cannot be considered sufficient or reliable until it has been tested and the plans and procedures are proven to be workable in a stressful situation when dealing with a crisis. During the exercise, the focus should be on validating the education of the staff, evaluating the procedures and obtaining feedback or recommendations from the participants. All of these aspects are of equal importance during an exercise. An incident is a dynamic situation, and therefore, an exercise should be as well. The participants in the exercise can find that their plans and procedures do not function properly for the given situation, and improvisation is sometimes necessary. The outcome of an exercise should be an enhanced understanding of the procedures, increased confidence in own capability to respond to real events and either a verification of the plans or concrete pointers to what should be altered and improved [oM20].

2.4.2 Different Types of Preparedness Exercises

Preparedness exercises are usually divided into four types: discussion exercises, game exercises, functional exercises, and full-scale exercises. The purpose of all types of exercises is to improve the participants' ability to manage crisis and prepare personnel for responding to emergency situations. The definitions of each exercise below are based on the definitions in the guidebooks from DSB [Dir16a] and NVE [Lar15].

Discussion exercises, often also referred to as tabletop exercises, can be both effective and productive at the same, as it is cost-saving since no specific equipment is needed. These exercises also require minimal time and resources for planning, while still providing value to the participants. This type of exercise aims to promote discussion between the participants in the exercise, where the topics can be roles, responsibilities, procedures, coordination, and decision-making. All the participants are gathered at the same location, and the duration can vary between one hour to a whole day of activities. These kinds of exercises are usually performed by having a facilitator who presents a scenario and initiates a discussion. However, no physical measures are taken during the exercise, and there should be no contact with non-participants during the exercise. Discussion exercises are efficient when the goal is to review and learn documented plans and procedures for incident response.

Game exercises typically divides the participants into teams based on their role or function, and the teams are physically separated in different rooms or locations. Game exercises require more resources than a discussion exercise, especially since the implementation requires a group of organizers and coordinators. The exercise is built on a simulated scenario, where the exercise leaders insert new events or information to drive the exercise along. The communication takes place either physically or via means of communication like phone or e-mail, where the organizers of the exercise have a playbook and might use media events like news articles to steer the exercises in a particular direction [Dir16c]. Generally, no physical measures should be taken during a game exercise. However, normal tasks for the incident response team such as alerting, reporting and use of alternative means of communication can be exceptions.

Functional exercises require a simulation of some functions that have been identified as essential to manage real events. To perform these simulations it is necessary to use physical equipment and execute procedures, such as alerting and reporting. This gives the stakeholders a more realistic impression of how things will be handled during an actual emergency.

Full-scale exercises typically include larger portions of the organization in one exercise, where the whole chain of command from the strategic level to the operational level participates. In addition, it is common to involve external parties to practice cooperation when handling large and complex incidents. Full-scale exercises are the most complex and resource-demanding type of exercise and should be as realistic as possible. This means that all activities are conducted as if the real incident had occurred. The exercise is performed in real-time, creating a stressful, time-constrained environment that closely mirrors real events. These types of exercises require a substantial amount of planning and coordination between the different participating parties.

2.4.3 Planning and Conducting Preparedness Exercises

This section presents three different guides on how to plan and organize preparedness exercises. The main focus is NVE's guide on planning and carrying out exercises in the electrical energy sector introduced from 2015 [Lar15]. In addition, we will introduce two similar guides from DSB and NIST.

Guide From NVE

This guide from NVE focuses specifically on the electrical energy sector and divides the exercise into four phases of equal importance: planning, implementation, evaluation, and follow-up.

Planning When an exercise is to be planned, it is important to identify who should be involved in the planning of the exercise, i.e. the exercise staff. Here the most important roles to define are an exercise facilitator and a data collector. In addition, it is essential to determine what the goals and learning outcome should be, and create scenarios and collect input from stakeholders. A risk and vulnerability assessment or previous experiences can be used to determine which scenarios should be selected for an exercise. The exercise goals should be determined based on what one wants to achieve with the exercise and have to be measurable and possible to evaluate. Furthermore, one must find out which type of exercise is most suitable for the desired learning outcome. A guiding document used to describe the rules and other practical information should be distributed to the participants in advance of the exercise.

Implementation Before the exercise begins, the exercise leader must start by going through the plan for the exercise, presenting the learning objectives and repeating the relevant theory, so all participants have the same foundation. The specifics of the implementation will depend on the type of exercises chosen. One or more facilitators (depending on the size of the exercise) should be present to guide the participants. During the exercise, the facilitator should be as inactive as possible to avoid affecting or steering the participants. All distributed documents should be marked with “Exercise” so that they are not mixed with other papers during and after the exercise.

Evaluation After the exercise, it is important to set aside the time to conduct an evaluation based on the participants’ first impressions. This time should be used to discuss the experiences and opinions of the participants regarding the conducted exercise. The appointed data collector for the exercise is responsible for gathering feedback from the participants and preparing a report after the exercise. The report should repeat the goal of the exercise and discuss whether it has been achieved. In addition, it should summarize the course of the exercise, including challenges that have been identified along the way, and list experiences and follow-up points based on the exercise’s goals and elements. The evaluation provides a retrospect of how processes worked to develop existing practices further, and it is beneficial if all relevant parties participate, both internal and external [FHT13].

Follow-up The evaluation report will form the basis for further work after the exercise. The follow-up after the exercise consists of implementing the measures identified during the exercises and summarized in the report. These measures can be both practical or organizational, such as updating contingency plans or making use of the measures in business planning. A person responsible for follow-up should be appointed to ensure that the follow-up is carried out in a satisfactory way. It can be beneficial to conduct another exercise after the measures have been implemented in the organization, to uncover whether the follow-up from the previous exercise has given the desired effect.

Other Guides for Exercise Planning

DSB has a guide on planning, conducting and evaluating exercises [Dir16a]. This is a general guide for how organizations and institutions of societal importance should plan and conduct exercises, and it also discusses all the choices that have to be made prior to an exercise. In addition, they also have a guide for discussion exercises [Dir16b], which explains more in detail how the exercise staff should go about planning and conducting a discussion exercise. This includes the same steps as other guides, but has an extra focus on the roles that should be defined for the discussion exercise, how to facilitate and ensure a good discussion among the participants, and the specific documents that should be created and distributed.

NIST provides guidance on exercises planning in their *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* [GNB+06]. This guide explains how both tabletop exercises and functional exercises can be planned and conducted. For both types of exercises, they divide the process of conducting an exercise into the following phases: (1) Evaluate the need for an exercise, (2) Design the exercise, (3) Develop the exercise material, (4) Conduct the exercise, (5) Evaluate the exercise.

2.4.4 Scenarios

According to the Cambridge Dictionary, a scenario is a description of possible actions or events in the future.[6] Thus, a scenario is an outline that describes the sequence or development of a potential event or events that are assumed will occur. In the context of information security, scenarios are commonly used to increase organizations' knowledge of potential threats and risks. Furthermore, organizations use scenarios in information security preparedness exercises to describe potential emergency incidents that the organization could be exposed to. The scenario is a sequential, narrative account of a hypothetical incident and is intended to introduce situations that will inspire responses and demonstrate the exercise objectives [GNB+06]. The choice of scenario should be based on a risk and vulnerability assessment and should be adapted to fit the decided goals of the exercise and the aspects that the participants want to practice.

DSB gives a description of the work with creating a realistic scenario in its guide for how to plan an exercise [Dir16c]. According to this guide, the events in the scenario should trigger actions from the participants. Usually, a scenario has the following structure: from normal conditions to crisis, managing the crisis, from crisis

[6] https://dictionary.cambridge.org/dictionary/english/scenario

to normal conditions again. A study conducted by Line and Moe [LM15] shows that a scenario divided into multiple phases aids the participants in seeing connections over time and discovering incidents that otherwise would go undetected. It is very rare that an attack only has one phase, and they are often discovered by finding connections. With a basis in the theme of the scenario one must identify which systems will be affected, what the function of this system is, which employees or actors should be involved, and what consequences this incident will have. The scenario should consist of three main components: the backdrop, the conditions and facts, and the causes and consequences. The backdrop should be information about the situation that has the potential to lead to one or more incidents. The facts should be the outer bound for the exercise and set the stage by giving information about the date, time, location and currently available resources. As the final component, the causes and consequences should initialize the exercise and give the participants information about an event and a consequence that demands decisiveness and management.

NVE has constructed a collection of example scenarios that can be used in both discussion and game exercises for organizations within the electrical energy sector [Lar15]. All the scenarios have associated descriptions of which employees or actors that should be included, duration, exercise goals, a guide for implementation and how evaluation and follow-up should be conducted. Out of eleven scenarios in the collection, only one scenario focuses on cybersecurity incidents, whereas the others concern incidents such as storms, natural disasters, and fires. The cybersecurity scenario is divided into four examples of incidents varying in severity, where two of the examples are internal ICT incidents and attacks on control systems.

The US Electric Power Research Institute (ERPI) has produced a report [Ele15] containing failure scenarios with both malicious and non-malicious cybersecurity events in smart grids and divided them into six different categories: Advanced Metering Infrastructure (AMI), Distributed Energy Resources (DER), WAMPAC (Wide Area Monitoring, Protection, and Control), Electric Transportation (ET), Demand Response (DR) and Distribution Grid Management (DGM). Furthermore, they have included two additional categories: Generation (GEN) and Generic.

2.5 Existing Solutions

In this section, a selected number of existing solutions within the field of cybersecurity preparedness exercises are presented. These solutions demonstrate that there are many different ways to conduct preparedness exercises and training and represent only three possibilities out of many.

Ovelse.no

Ovelse.no [fsobD20] is an exercise portal containing cybersecurity exercises that the Norwegian government created as a part of the national exercise *Øvelse Digital 2020*. The portal provides cybersecurity discussion exercises based on 12 different scenarios that any organization can use. The goal is to give all organizations in Norway a tool to conduct cybersecurity exercises and increase awareness of digital threats. Each discussion exercise consists of 8 steps that the participants should go through:

1. Background information and an introduction to the scenario
2. Discussion questions for the introductory scenario
3. Advice for further work
4. Second part of the scenario
5. Discussion questions for the second part of the scenario
6. Advice for further work
7. Third part of the scenario
8. Concluding information and evaluation survey

In addition, some extra information is provided to the facilitator of the exercise. This includes more information about the scenario and questions to drive the discussion forward. The exercises are intended to be useful for the entire organization and are developed in a collaboration between DSB, the Norwegian University of Science and Technology (NTNU), the Norwegian Center for Information Security (NorSIS), the Norwegian Digitalisation Agency *(Digitaliseringsdirektoratet)* and NSM.

Play2Prepare

Play2Prepare [GLB15] is a board game that simulates a large scale attack on the electric power grid. It was developed as a part of a master's thesis at NTNU in 2015 for supporting IT security preparedness exercises for industrial control organizations. The game intends to trigger discussions and knowledge exchange between the participants. It provides several scenarios and questions that are used while the players move around on the board and neutralize local attacks. *Play2Prepare* is designed for 3–4 players, where each player is given a particular role with accompanying skills that have to be used to win the game. It follows a logic similar to an existing board game called *Pandemic*[7], but has been adapted to the context of cybersecurity in the power grid.

[7] https://zmangames.com/en/products/pandemic/

Cybersecurity Competence Center Luxembourg (C3)

The Cybersecurity Competence Center *(C3)* [Cyb20] in Luxembourg was launched in 2017 and aims to help businesses face cyber risks. They provide services related to threats and vulnerabilities, resilience testing and simulation platforms. The training and simulation platform allows teams to train on preventing and reacting to incidents. The flagship of *C3* is *Room#42*. It is a simulation game that allows the participants to face a cyber attack in an immersive and playful environment. The flow of the exercise is adjusted depending on how the players interact and behave; good decisions are rewarded, and poor decisions penalized. An exercise session in *Room#42* can be organized to adapt to different purposes and people.

2.6 Previous Research and Exercises

In this section, a selected number of reports and research articles focusing on cybersecurity preparedness exercises or the involvement of suppliers in incident management in the electrical energy sector are presented. These represent some of the previous work that has been conducted in this field. However, none of these has focused on how to enable the involvement of suppliers in cybersecurity preparedness exercises, which is the basis of this thesis.

Challenges in IT security preparedness exercises: A case study

In this study, Bartnes and Moe investigated the collaborative challenges between different areas of expertise within an organization during IT security preparedness exercises [BM16]. This was done by a case study on the Norwegian electrical energy sector. The focus was to uncover challenges that organizations meet during exercises to strengthen the response capabilities during real incidents as well. To investigate this, they observed three DSOs when they conducted tabletop exercises. They recommend to define only one main goal for the exercise, make existing written plans and procedures available during the exercise and ensure a certain time pressure. In addition, it is essential to ensure that all required competence are present, including personnel from external suppliers, and involve all personnel that will play a role during a real-life incident.

The future of information security incident management training: A case study of electrical power companies

Bartnes et al. [BMH16] conducted an extensive study with the aim of identifying improvements for ISIM practices in the Norwegian electrical energy sector. They discovered that training for cybersecurity incidents was given low priority and that IT staff and control system staff have different mindsets when it comes to information security. Additionally, the existence of plans for incident management varied among the DSOs. They concluded that cross-functional response teams are needed to cover all perspectives and competencies in incident management and that learning from previous incidents and preparedness exercises is important for improving practices for responding to incidents. The recommendations from the study included that more scenarios for preparedness exercises should be developed and exercises should be conducted frequently.

Cybersecurity Incident Management In The Electrical Energy Sector: Involvement Of Suppliers

In this master's thesis, Eriksen and Gunabala [EG20] investigated cybersecurity incident management in the electrical energy sector, related to PCS, with a focus on the involvement of suppliers. The scope was limited to the Norwegian electrical energy sector and incident management regarding PCS. The study took a qualitative approach with interviews and document reviews as the primary data collection methods. A case study of two small and two large Norwegian DSOs, in addition to a supplier of PCS were performed. The findings show differences between small and large DSOs with indications that some small DSOs are not prepared to handle cybersecurity incidents in their PCS, and that there was little involvement of suppliers in plans, exercises and the evaluation of incidents. In addition, it showed that a combination of high supplier dependence and the small number of suppliers creates a vulnerability for the sector towards multiple, simultaneous attacks on several DSOs. The thesis resulted in a set of recommendations for improving the involvement of suppliers in incident management.

Øvelse Østlandet 2013: Evalueringsrapport

Øvelse Østlandet 2013 [Nil14] is a preparedness exercise run in the Norwegian electrical power sector in 2013. The exercise focused on extreme weather and the consequences for critical infrastructure with extra attention to handling situations with prolonged downtime. This evaluation report describes the organization of the exercise, including the scenario, the goals and the participants. In addition, it addresses points of improvement and recommendations for measures to be implemented.

Grid Security Exercise: GridEx III Report

The North American Electric Reliability Corporation conducted a security and emergency response exercise called GridEx III [Cor16] in 2015. It consisted of a two-day distributed play exercise and an executive tabletop exercise the following day. More than 4,400 individuals from 364 organizations across North America participated in GridEx III, including industry, law enforcement, and government agencies. The report from the exercise provides information about the conducted exercise, and observations and recommendations based on the information gathered from the after-action survey.

Exercise PowerPlay: Post Exercise Report

Exercise PowerPlay [Ran19] is a collection of three cybersecurity exercises run in the UK electricity sector in 2019. The National Cyber Security Centre facilitated the exercises in collaboration with the Department of Business Energy and Industrial Strategy, TSOs, DSOs, supply chain organizations and QinetiQ. The report presents the feedback and observations from the three exercises, and makes recommendations to improve the electrical energy sector and third party supplier's resilience to national cyber incidents. It also makes recommendations for improving future sector-wide cyber exercises.

Chapter 3 Method

In the following chapter, we elaborate on the chosen research methods and justify the choices made during the project. We used a qualitative research approach for data collection by performing a literature review and semi-structured interviews. The literature study is addressed in Section 3.1.1. The interviews, as presented in Section 3.1.2, were the primary data source, and the method for data analysis is explained in Section 3.1.3. In addition, we have used iterative methods to produce and verify some of the results from the thesis, as found in Section 3.2.1 and 3.2.2. Limitations to the methods and ethical considerations are discussed in Section 3.3.

3.1 Qualitative Research

The common choices of research design are often either quantitative research, qualitative research, or mixed-method research [RM16]. Whereas quantitative research often is more theory-driven and associated with measurements and quantification, qualitative research focuses more on social research and discovering patterns based on observations. Qualitative research is often a good approach for research based on people's opinions and feelings concerning a topic. Mixed-method research is a combination of the two other mentioned research types [RM16].

As mentioned, a qualitative research method was used to conduct the study in this thesis. This method was chosen because collecting information and gaining in-depth knowledge from relevant organizations was necessary to perform a thorough analysis of the topic and create valuable results for the industry. Qualitative research is a very flexible design strategy. Therefore, it sets requirements for the researchers regarding knowledge and analytical abilities, especially the ability to be open to conflicting evidence and reflected and unbiased in the analysis. If this is not the case, it could have a negative impact on the results. The observations in this study were collected through interviews, a literature study, and a conducted preparedness exercise to validate some of the created results.

3.1.1 Literature Study

A literature study is a survey of relevant sources on a specific subject and provides an overview of current knowledge, relevant theories and methods. To acquire relevant publications for our master's thesis, we have performed searches for relevant literature. It was necessary to study a broad spectrum of background material to gain sufficient knowledge and understanding of the industry, cybersecurity incident management and exercises as a tool to prepare for cybersecurity incidents. There is a large selection of literature available within our topic of study, so it was necessary to be critical during the information gathering phase and evaluate the discovered sources both with regards to relevance and credibility. However, we have not made any attempt at performing a systematic literature review of all the literature on the topic since this would be too time-consuming given the additional work in this study.

To gather the information, we created three categories of searches, depending on the purpose of the information. The three categories were:

1. A search for papers, reports and articles that can verify or refute the relevance of our research area within the electrical energy sector and whether the thesis would contribute with any value to the industry. In this category, we searched for studies that had performed research on the topic of the involvement of suppliers in incident management, which substantiated the need for more research on the area.

2. A search for papers, reports and articles that provides the necessary background information or knowledge needed to conduct the project.

3. A search for papers, reports and articles regarding existing tools or existing collections of scenarios that can be used to conduct exercises. This was done to find inspiration and to see what had been done in the field within different industries and sectors.

To gather the necessary insight about the electrical energy sector in Norway and incident management procedures for Chapter 2, we have studied guidelines from the relevant authorities, standards for incident management, as well as standards and procedures for performing preparedness exercises. The focus was well-established and internationally accepted ISO/IEC standards and legislation and publications from NVE. However, we have also looked into relevant documentation and guidelines from NIST, ENISA and DSB. To investigate the current threat landscape, we have looked into previous attacks on the power grid and vulnerabilities caused by the increasing digitalization of the sector. In addition, related research into ways to perform preparedness exercises has been studied. In this literature study, a mixture of articles, reports and previous theses, both Norwegian and international, have been analyzed.

3.1.2 Qualitative Interviews

There are several types of interviews, and qualitative interviews have been categorised in a variety of ways. However, a common way to differentiate them is as unstructured, semi-structured and structured interviews [RM16]. Semi-structured in-depth interviews are the most widely used interviewing format for qualitative research, and the main objective of qualitative interviews is to see the research topic from the interviewee's perspective and based on their real-life experiences [DBC06]. Thus, we chose to use qualitative semi-structured interviews as the primary method for conducting the interviews.

Semi-structured interviews require that the questionnaire has been developed in advance, and the interview guide should contain an ordered list of questions. However, the order of questions can be rearranged during the interview to achieve a better flow, and the interviewee can be encouraged to elaborate by using follow-up questions. Our approach to conducting the qualitative semi-structured interviews was divided into five steps: (1) defining the research question, (2) deciding and contacting the participants, (3) creating the interview guide, (4) carrying out the interviews and (5) follow-up questions and feedback.

The interviewees were given information about the main topics that the interview would focus on in advance. The interviews lasted approximately 45 minutes to 1 hour, and the answers were recorded with pen and paper only. The results from the interviews are given in Section 5.1.

The Interview Guide

We created two different interview guides: one for the DSOs and one for the suppliers. This was done to ensure that the same desired data was collected from each participant and to give structure to the interviews. The interview guides can be found in Appendix C.

Both interview guides contained the same phases: a warm-up phase, reflection phase and round-off phase. In the first phase, the focus was to warm up the subject with an introduction of us, our thesis and with questions regarding the organization and the interviewee's role in it. Then, in the second phase, the questions focused on reflection about incident management schemes in the company, the collaboration between the DSO and suppliers regarding incident management procedures and preparedness exercises, and previous cybersecurity incidents. In addition, we asked about ideas for scenarios that would require the involvement of both the DSO and suppliers. This phase was the main phase of the interview and focused on the topics we wanted to gain insight into. As a round-off, we ended the interview with some open-ended questions. These focused on if they had any general thoughts about what was important to ensure that the collaboration between DSOs and suppliers was as good as possible and if they otherwise wanted to share anything. In the end, we thanked the subject for participating and explained that we would like to have another meeting later to get feedback on the scenarios.

Participants

Four of the participants represented Norwegian DSOs. The DSOs varied both in the number of employees and the number of energy subscribers. Regarding the number of energy subscribers, the most common classification is that small DSOs each serve around 10.000 customers or less, and large ones serve close to 100.000 or more. However, to distinguish the DSOs that we have interviewed, we made a new classification: small DSOs have 50 000 or less customers, medium DSOs have between 50 000 and 150 000 customers and large DSOs have over 150 000 customers. Thus, the first participating DSO is classified as a small DSO, the second DSO is classified as a medium DSO, while the third and fourth DSOs are large DSOs. For each of the interviewed organizations, it was of interest to interview people with positions such as ICT security coordinator since all DSOs are required to have that position. The main focus of the interviews was to gain insight into how they work with incident management and, more specifically, preparedness exercises and how they collaborate with their suppliers during incident response. In addition, we wanted to understand which scenarios and which suppliers that are most relevant to include in cybersecurity exercises.

Interviews were also conducted with two suppliers. These interviews mainly focused on investigating their view on the importance of collaborating with their customers (DSOs) and participating in preparedness activities. In addition, we wanted to understand their role in incident management better so that we could adapt the events in the scenarios to how things would have been during an incident. In these interviews, we were interested in interviewing people that are involved in the ICT security of the organization and somewhat responsible for the communication with DSOs during incidents.

3.1.3 Data Analysis

> The analytic challenge for all qualitative researchers is finding coherent descriptions and explanations that still include all of the gaps, inconsistencies, and contradictions inherent in personal and social life [MHS20].

The main difficulty with qualitative data is the analysis phase, as there is no clear and universally accepted set of conventions for analysis corresponding to those of quantitative data analysis [RM16]. Qualitative data is often subjective and rich, and usually comes in the form of words or other non-numerical data. Therefore, analyzing qualitative data involves going through a large amount of data, searching for similarities or differences, and identifying themes and categories.

This section describes the method used for structuring and analyzing the qualitative data we collected in the conducted interviews. The process is inspired by the step-wise deductive, inductive method described by Tjora [Tjo17]. We mainly followed the inductive process and simplified this into three steps that were conducted in order to analyze the qualitative data. The result from the previous step was used as input to the next step, and the end goal was to develop theories and extract the common factors from the processed data.

Step 1: Since we did not record the interviews, only took notes, we did not need to transcribe the interviews afterwards. However, after each interview, it was necessary to go through the notes to correct the mistakes and fill out incomplete sentences while we still had the interview fresh in mind. In addition, we wrote summaries with the most important aspects from each interview. These summaries were meant to highlight the most important information, so it would be easy to discern the main results from each interview.

Step 2: After we had completed the first step of processing the data from the interviews, we started on the process of structuring the data. To do this, we used color-coding by defining codes for information about suppliers, incident management plans, exercises, general thoughts about collaboration, and scenarios, and using a different color for each code. The answers from the DSOs were then structured in a common spreadsheet, where the summary of the answers to the questions was written, along with a column for relevant quotes. The same was done for the suppliers. Then we went through the spreadsheet and highlighted things of importance by using the defined color codes. This way, we could easily compare the answers from both DSOs and the suppliers and gain an overview of the results.

Step 3: To analyze the data, we decided to use a variant of empirical coding. Based on the codes defined in Step 2 and further structuring of the data, we categorized and grouped the questions from the interview guides to compare the answers to similar topics. We wanted to look at how the two groups (DSOs and suppliers) answered the same questions to discover differences and similarities in their opinions. In the end, we ended up with four different categories, which are presented in Chapter 5. In addition, we had to decide upon how to structure the discussion in Chapter 6. Since we used an inductive research approach, theories and observations were formed when working with the collected material. We identified focus areas for both the first and second research question during the analysis phase.

3.2 Scenario and Exercise Development

A part of the work with this thesis involved designing scenarios and corresponding preparedness exercises. There is a wide range of available methods for developing scenarios and corresponding exercises that can be adapted to fit our purpose. It is important to use a predefined method to ensure that all the essential elements are included and show how we have reached the results. In this section, we describe the methods used to develop the scenarios and the preparedness exercise.

3.2.1 Scenario Development

The scenarios were created by looking at existing scenarios for inspiration and using acquired knowledge about the electrical energy industry and the ICT security in their systems. The development of the scenarios was done by using a simplified and adapted version of the iterative development process defined below.

> **Iterative development** is an approach that is based on repeating and refining a defined cycle, called an iteration [agi21]. This cycle represents the whole development process and includes planning, design, development, and testing steps [Eas21], as shown in Figure 3.1.

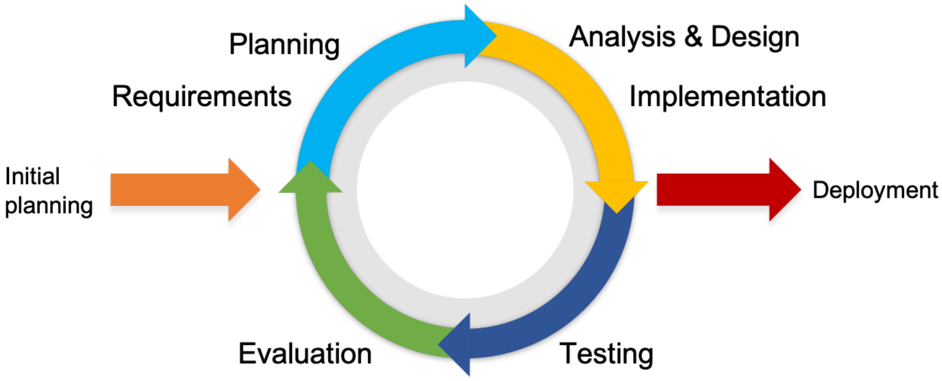


Figure 3.1: Illustration of the stages of an iterative development process.

The first step was to gather the necessary information through literature studies and interviews. Then a cycle consisting of the steps enumerated below were conducted in two iterations. Based on the feedback collected in the third step, the cycle repeated, and the scenarios were adjusted to the new requirements.

1. Specifying the requirements for the scenarios
2. Design and implementation of scenarios
3. Feedback and evaluation

During the second step in the cycle, when designing and implementing the scenarios, the guide from DSB [Dir16c] on designing realistic and relevant scenarios for exercises was used. This guide was presented and described in Section 2.4.4. For each produced scenario, we added relevant questions and discussion points to each phase. This was done in order to make the scenarios ready to be used in discussion exercises. For one of the scenarios, we created the other necessary associated documents for a discussion exercise.

In the third step in the cycle, feedback from DSO A and B and NVE and KraftCERT, as representatives of the industry, was collected. This was done by distributing the drafts of the scenarios and a set of questions or aspects that we wanted feedback on. The feedback was either given through meetings or in writing, depending on their preferences.

After the cycle had been repeated two times, one of the scenarios and the associated documents for a discussion exercise were tested by conducting an exercise. Based on the evaluation from the participants, the scenario and other documents were adjusted one last time.

3.2.2 Preparedness Exercise Development

The planning and implementation of the preparedness exercise were inspired by the guidelines for planning and carrying out exercises produced by NVE [Lar15], DSB [Dir16b] and NIST [GNB+06], which was presented in Section 2.4.3. In general, the development of the exercise was divided into the following four steps:

1. Planning
2. Implementation
3. Evaluation
4. Follow-up

The planning phase The planning phase is essentially a design phase where it is necessary to define the important aspects of the event. To acquire the necessary information to plan the exercise, this phase included conducting interviews with DSOs and suppliers. In addition, information found through literature studies was utilized. Inspired by the steps in the mentioned guides for exercise planning, we defined the following milestones:

- Identify exercise staff
- Determine type of exercise
- Determine the exercise goals
- Identify participants
- Select or design scenarios to be used
- Set the duration

Towards the end of the planning phase, the necessary exercise documents were produced and distributed. This included a briefing, a participant guide, and a facilitator guide used during the exercise. The briefing contained practical information to be distributed to the participants in advance, such as the time and place of the exercise, the agenda, the participants and the exercise goals. The facilitator guide contained some additional information about and descriptions of the scenario and additional discussion questions to lead the discussion. The participant guide was meant to guide the exercise and included the different parts of the scenario and related discussion questions.

Implementation The exercise staff is comprised of the roles of exercise facilitator, data collector and observer. The roles as exercise facilitator and data collector were filled by representatives from the DSO, while we acted as observers and support for the other roles. The exercise facilitator is in charge of the organization of the exercise, including identifying and inviting the relevant participants and deciding on the scenario to be used. During the exercise, the exercise facilitator's responsibility is to present the different parts of the scenario and facilitate the discussion aided by the participant guide and the facilitator guide. The data collector is responsible for evaluating the exercise and following up on the identified points of improvement. The role as observers allowed us to identify possible improvements and limitations with both the organization of the exercise and the scenario used.

Evaluation During the exercise, we observed and took notes which were used to evaluate the exercise. Directly after the exercise a first impression evaluation was performed, where the participants discussed the organization of the exercise and whether the exercise's goals had been achieved. This first impression evaluation ensured that the initial thoughts and observations regarding the exercise are recorded before they are lost. In addition, the participants were asked to answer a questionnaire in the following days. The questionnaire focused on both the goals and the organization of the exercise, including how the use of a digital video conferencing tool affected the learning outcome. This gave us a more structured evaluation of the exercise. The results allowed us to identify factors to improve in both the scenario and the organization of the exercise. The results from the evaluation are presented in Section 5.3.

Follow-up Since our intended purpose with the preparedness exercise was to validate and identify improvements with the scenarios and the organization of the exercise, our follow-up phase focused on adjustments and not on implementing the measures to improve the identified shortcomings at the DSO and suppliers. Therefore, this phase consisted of adjusting the exercise and the scenarios based on the information obtained from the evaluation.

3.3 Limitations and Ethical Considerations

Since the study are built on interviews and human interpretation, it is necessary to evaluate the study's reliability and validity to determine the level of trustworthiness of the study. This is especially important for qualitative research, but it is also important to consider this for the methods used for the produced scenarios and exercise. In addition, the generalizability of the study and ethical considerations will be addressed.

3.3.1 Validity

> Validity is concerned with whether the findings are 'really' about what they appear to be about [RM16].

To determine whether a study's results are accurate, correct or true, is challenging, and in qualitative research these things are especially difficult to be sure about. This thesis's validity and its interpretations are built on a comprehensive background study of relevant topics and existing research. Previous work and reports from the industry disclosed that suppliers are rarely involved in exercises and that it is recommended to collaborate with suppliers on preparedness exercises. In addition, industry organizations like NVE and KraftCERT were asked whether the topic would bring value to the electrical energy sector to validate the thesis.

The amount of experience of the researchers may affect the results, and this applies to both the produced scenarios and exercise and the results from the qualitative interviews. For the produced scenarios and exercise, the lack of experience with this work and the lack of insight into the industry might have an effect. For the results from the qualitative interviews, the minimal experience and lack of practice in the role as an interviewer can be harmful to the study and affect the subjects when they answer. Especially in the eagerness to get results, asking leading questions and not being patient enough when subjects are thinking of their answers are possible mistakes that can weaken the validity of the results.

We did not record the interviews but decided upon one of us to write a thorough report of the answers during the interviews, while the other asked the questions. This worked well for us, but there is a chance of errors or misinterpretations in the report. Therefore, this might affect our ability to produce an accurate description of what we heard afterwards. In addition, it took the focus of one of us away from the interview and hindered the participation in the interview and the ability to help asking the right questions. After starting the data analysis, we saw that some of the answers to the questions were a little incomplete. Therefore, we reached out to the subjects via e-mail and asked for some clarifications to ensure that we wrote down the correct results.

The interview subjects were given a chance to read through and give feedback on the final draft to assure the validity of the data. This process is known as member checking, and it can be a valuable means of guarding against researcher bias and demonstrates that you value the contribution of the participants [RM16].

3.3.2 Reliability

> Reliability refers to the consistency or stability of a measure, and indicates whether the result can be replicated and consistent over time, so that the same results can be obtained later [RM16].

According to Robson, reliability can be obtained through an audit trail [RM16]. Therefore, all activities performed during the thesis project were recorded during the study, including notes from literature searches, interviews, scenario and exercise development and data analysis.

In addition, all the interviews followed the same format. Meaning that the same information was distributed beforehand, the setting was similar, and the interview guide was followed when conducting the interviews. However, other things will also affect the reproducibility of the results in qualitative research.

The competence and knowledge of the subjects within the same category may vary. With the DSOs, we talked to employees with the same roles in the company, so their knowledge should be similar. However, the two suppliers did not have the same background and roles, so it is difficult to ensure that their knowledge was the same. This affects to what extent different answers can be compared and how consistent they are.

The collected data may also be affected by who the interviewer was since different interviewers can get different answers from the same subject. This is regardless of the fact that the questions are asked in the same way. As a result, it is very challenging to ensure that the results are reproducible.

Regarding the scenario and exercise development, the input was also gathered by distributing the same set of questions to the DSOs and the authorities. In that way, we could ensure that all the different parties had covered the same aspects when providing the feedback.

3.3.3 Generalizability

> Generalizability refers to the extent to which the findings of the enquiry are more generally applicable outside the specifics of the situation studied [RM16].

In a qualitative study, the samples from the target group must be representative and large enough to ensure generalizability. Thus, it would be desirable to include as many organizations as we could in the interviews within the boundaries of the study. However, both a lack of answers from DSOs and suppliers and the time constraint resulted in us not being able to talk to as many in the target group as hoped. Therefore, even though we wanted to produce a result that could be used by the entire industry, our study is not fully generalizable. However, by interviewing DSOs of different sizes, measured in the number of employees and customers, and suppliers that combined deliver their services and products to a large number of the Norwegian DSOs, the findings of this thesis still provide a certain overall perspective.

The conducted exercise included only one DSO and two of its suppliers, and only tested one of the scenarios. Thus, the results from this test might not be generalizable for the other created scenarios and other DSOs. However, to ensure that the created scenarios will have as much value for the industry as possible, we gathered feedback on the drafts from two of the interviewed DSOs. While we did not get feedback from all of the DSOs, we received feedback from DSO A and B, which represent the category to which most of the Norwegian DSOs belong. In addition, feedback was also collected from both NVE and KraftCERT, as representatives for the industry authorities. This does not guarantee that all Norwegian DSOs and their suppliers can use the scenarios, but it increases their overall likely value to the industry.

3.3.4 Ethical Considerations

When working with research that includes interviews and information gathered from individuals, it is important to be aware of the necessary ethical considerations. According to Tjora [Tjo17], when using interviews in a study, most of the ethics are connected to the presentation of the data. However, it is also important to have a certain focus on it when conducting the interviews. During our interviews, we did not record any sound or video, only notes were taken. In addition, an alias was assigned to each company and each interviewee present at the interview. Hence, the notes do not include any personal information. All results presented in the thesis are anonymized, and the interviewees are given the opportunity to read through the parts that deal with their interviews. This way, the interviewees are given the opportunity to request changes if they find it necessary to clarify any misunderstandings.

Before we acted as observers at the conducted preparedness exercise, we signed a confidentiality agreement with the DSO, since there was a possibility that we would learn some sensitive power system information (as presented in Section 2.1.2). This stated that we could not share any sensitive information that was discussed at the exercise. During the interviews with the DSOs and the suppliers, we did not learn any sensitive information, so there was no need to sign any additional confidentiality agreements.

Chapter 4
Created Scenarios and Exercise

This chapter presents the created scenarios and associated documents for discussion exercises. The content and intended use of the different documents will be explained, while the complete documents can be found in Appendix A and B. Table 4.1 provides an overview of the documents and their intended use.

The scenarios and exercise documents have been created based on input from interviews with DSOs and suppliers and feedback from industry authorities. The data collection results are presented in Chapter 5.

Document	Description
	Appendix A
Collection of scenarios	A collection of different scenarios that provide descriptions of hypothetical incidents
Discussion exercise	A scenario and related discussion questions that can be used during a discussion exercise
	Appendix B
Briefing	General information about the exercise to be distributed to all the participants in advance
Participant guide	The information that the participants will receive during the exercise, including the scenario and discussion questions
Facilitator guide	Information about the responsibilities of the facilitator, additional information about the scenario and a list of questions to drive the discussion along
Evaluation scheme	Evaluation questions to be discussed immediately after the exercise and questions to be answered individually later in a questionnaire

Table 4.1: Overview of the created documents and their intended use.

4.1 Scenarios

Each of the scenarios consists of two or three phases representing the sequential development of a hypothetical incident. The scenarios are designed to facilitate the involvement of suppliers in exercises. Together with the corresponding discussion questions, the scenarios form a discussion exercise with the goal of improving the collaboration between DSOs and suppliers during incident management. We have created the scenarios in a way that should make it easy for the users to adapt and customize them to their own use. To achieve this, we have tried to have an appropriate level of detail in the scenarios, making it easy for the users to add additional information. In the places where it is necessary to include details that may vary from DSO to DSO, we have tried to make it clear to the users that they can choose the alternatives that best suit their situation. This is done by adding instructions in italics, encapsulating the different alternatives in square brackets or by using the discussion questions to guide the users in how they should proceed. The scenarios may also be used in discussion exercises with different goals by adjusting the discussion questions. Furthermore, they may be used as a starting point for larger exercises like game exercises, functional exercises and full-scale exercises.

Ransomware This scenario deals with a ransomware attack against a DSO. The DSO's systems are compromised, including servers and systems provided by one or more external suppliers. The first part of the scenario describes that attackers have gained access to the DSO's network and moved further into the systems and server platforms. In the second part of the scenario, the attackers launch the ransomware attack, leading to unavailable systems that affect both the DSO and its suppliers. In addition, it is discovered that the attackers used phishing to gain initial access to the network. The last part of the scenario deals with media management and customer relations. This scenario was inspired by the ransomware attack on the Norwegian aluminium producer Norsk Hydro [ACS19], hence displaying realism and relevance.

Attack on SCADA System This scenario concerns an attack on a DSO's SCADA system that initially starts with a power outage in a smaller area on Christmas day. At first, the operators cannot see any alarms going off in the SCADA system, but when sending an operator to check they discover that an area is without power. In the second part of the scenario, a few hours later, more areas are experiencing power outages and it is considered that the problems may be caused by malware in the SCADA system. The supplier of the SCADA system is called up to run a full diagnostic of the system. In the final part, the DSO has to manage both the media and concerned customers.

Attack on AMI This scenario covers an attack on the DSO's Advanced Metering Infrastructure (AMI) that is provided by a supplier. In the first part, they are alerted about irregularities in the electricity readings and that customers are experiencing power outages. A few days later, a large power outage that affects 1/3 of the customers occurs and the attackers announce in the media that they have gotten inside the DSO's head-end system and installed malware on all their smart meters. This gives the attackers remote access to all the power switches and they demand a large sum of money not to turn off the power for the rest of the customers. It is discovered that the attackers gained access to the network by using the credentials of an employee at the DSO, indicating either social engineering or an insider.

Disclosure of Sensitive Power System Information This scenario deals with the disclosure of sensitive power system information, which can potentially harm the DSO and its infrastructure. KraftCERT contacts and inform the DSO that sensitive power system information has been published on a hacker forum. Some of the documents concern the DSO's SCADA system. Since a supplier delivers the SCADA system, it is unknown whether the hackers have obtained the information from the DSO's or the supplier's servers. In addition to the documents published on the hacker forum, it is suspected that more documents have been stolen, but it is challenging to identify which documents. To stop the attackers from continuing to have access to the network and the servers it might be required to reset various systems.

Attack on Cloud Services This scenario describes an attack on a DSO's systems that are located in the cloud. At first, the employees discover that some systems are displaying error messages and that the internet access is offline. In the second part of the scenario, they learn that internet access is disrupted due to a DDoS attack targeting the DSO's IP range. The employees are consequently not able to access the systems that are running in the cloud. In order to regain internet access, it is necessary to coordinate with the ISP and the cloud service provider.

Exposed Vulnerable Services This scenario concerns that the DSO discovers that a service that is revealed to be vulnerable is used in one of the DSO's systems. At first, it is discovered that the DSO's administrative systems utilize a vulnerable service that is exposed to the internet. The system has been vulnerable and exposed for a longer time period, and it is not certain whether it has been compromised. The vulnerable system contains sensitive information that may have been stolen if the vulnerability has been exploited. It is necessary to investigate whether the vulnerability has been exploited and ensure that attackers cannot exploit the vulnerability in the future.

Defacing of Website This scenario concerns both the threat of hacktivists and the compromise of a web server. In the first part of the scenario, a customer notifies the service desk that the front page of the DSO's website is changed to "Why you should boycott companies like the DSO that contributes to wind energy development in Norway". In the second part of the scenario, it is discovered that activists have hacked the website and the DSO cannot regain control of the website alone since an external supplier is involved with the operation of the website.

4.2 Exercise

The preparedness exercise was conducted to validate one of the scenarios in the situation they are intended to be used. The exercise was conducted with DSO A and the scenario that was used was *Ransomware*. The exercise was held in the form of a discussion exercise, and due to the Covid-19 pandemic, it was held digitally by the use of Microsoft Teams.[1] The participants in the exercise from DSO A were the CEO, CFO, ICT security coordinator, quality and innovations manager (also preparedness coordinator), division manager for utility customers and operations center manager. In addition, representatives from two of the DSO's suppliers participated; the head of information security from one supplier and the ICT security coordinator from the other. Hence, there were eight participants in the exercise in total.

In order to conduct the discussion exercise, we had to create the necessary documentation and plans for the implementation. The purpose of these documents is described below, and Figure 4.1 illustrates how they relate to each other and are used in the exercise. Templates for these documents based on the documents used for the discussion exercise with the *Ransomware* scenario can be found in Appendix B. In addition, a written description of how to utilize the scenarios and related discussion questions to design and conduct a discussion exercise is included.

The Goal of the Exercise The goals of the discussion exercise were determined based on the focus of this study, which is contributing to enhance DSOs' ability to conduct effective cybersecurity preparedness exercises that improve collaboration with suppliers during incident management. The exercise were then designed based on these goals.

To improve the collaboration between the DSO and suppliers in incident management by:

- establishing relationships and points of contact
- testing all parties' knowledge of plans and contact points, and establishing a common understanding of plans, roles and responsibilities during

[1] https://www.microsoft.com/en-us/microsoft-teams/group-chat-software

an incident

- identifying potential points of improvement for the coordination and the plans

The main goal and focus of the exercise was to improve the collaboration between the DSO and suppliers in incident management. Additionally, to capture the different aspects of the collaboration, three subgoals that focus on good and clear communication, knowledge and understandings of plans, and points for improvement were added.

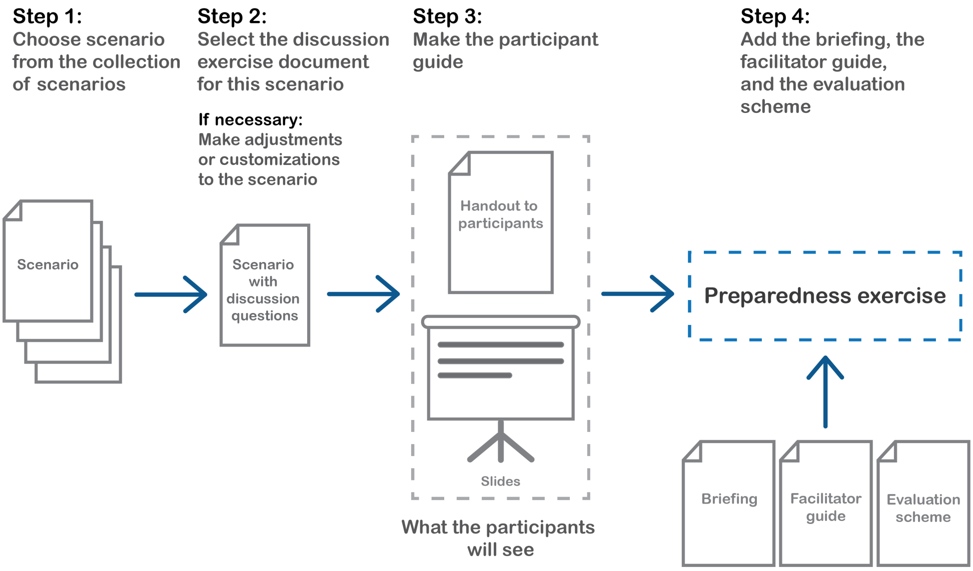

Step 1:
Choose scenario from the collection of scenarios
Step 2:
Select the discussion exercise document for this scenario
If necessary:
Make adjustments or customizations to the scenario
Step 3:
Make the participant guide
Step 4:
Add the briefing, the facilitator guide, and the evaluation scheme
Scenario
Scenario with discussion questions
Handout to participants
Slides
What the participants will see
Preparedness exercise
Briefing
Facilitator guide
Evaluation scheme

Figure 4.1: Explanation of the produced documents, how they are connected and how they are meant to be used.

Discussion exercise For each scenario, a set of associated discussion questions that focus on the collaboration between DSOs and suppliers was created. The scenario, together with the corresponding discussion questions, forms a discussion exercise. The types of questions asked to the participants during the course of the exercise were tailored both to the exercise goals and the participants' roles in the organization. The separation of the collection of scenarios and the discussion exercises into different documents was done to make the scenarios more generalizable by facilitating the use of the scenarios in other types of exercises.

Briefing The briefing is the document that contains the general information regarding the exercise to be conducted. It covers all aspects of the exercise and includes information about time, place, participants, goals, exercise facilitators, necessary preparation and other relevant information. The briefing is distributed to all the participants in advance to make sure that everyone receives the necessary information about the exercise.

Participant Guide This document is what the participants will use during the exercise and contains the information necessary to conduct the exercise, e.g. a slide deck or a document. It contains an introduction to the exercise, including an agenda with time estimates, the exercise's goals and other relevant information regarding how the discussion exercise will be carried out. In addition, the scenario is presented sequentially, where the phases and the related discussion questions are presented one by one in the correct order. The participant guide also includes the questions and aspects to be discussed for the first-impression evaluation.

Facilitator Guide This document contains extra information for the exercise facilitator and explains the role and responsibilities of the facilitator. It contains in-depth information about the scenario and explanations of terms and phrases used in it. In addition, the document contains some topics that the participants should cover in their discussion and a list of additional questions that the facilitator can use to drive the exercise along in the right direction. If a specific plan or procedure is to be tested in the exercise, it can also be beneficial to include a copy of the plan in the facilitator guide.

Evaluation Scheme After the exercise, on the exercise day, we conducted a first-impression evaluation with all the participants. The focus of this evaluation was to uncover how the participants felt the exercise had gone, if they had discovered any possible improvements and what they thought was the most important thing they had learned from the exercise. In addition, an individual questionnaire was sent out to all of the participants the day after. This focused on both the implementation, the content and the exercise's outcome and gave a more structured evaluation of the exercise. The evaluation scheme includes the questions used in both the first-impression evaluation and the questionnaire.

Chapter 5 Data Collection Results

The following chapter presents the data collection results, starting with the interviews in Section 5.1. Table 5.1 shows a summary of these findings. Secondly, the feedback on the scenario drafts from both the DSOs and relevant authorities are introduced in Section 5.2. Finally, there is a presentation of the results from the evaluation of the created and conducted preparedness exercise in Section 5.3.

5.1 Interviews

The findings from the interviews with the four DSOs and the two suppliers are grouped and presented in this section. An overview of the interviewed parties and the participants at each interview can be seen in Figure 5.1. The DSOs will be referred to as DSO A, DSO B, DSO C, and DSO D. DSO A was a small, regional DSO with a close relationship with its suppliers. DSO B was a medium sized DSO, with over 100 000 customers. Both DSO C and D were large organizations with more than 150 000 customers. In all the interviews with the DSOs, the ICT security coordinator participated. The responsibility of this role is to have an overview of all the ICT security work in the organization and function as a contact point to the preparedness authorities, as presented in Section 2.1.2.

The two interviewed suppliers were large organizations who supplied their product to many Norwegian DSOs and will be referred to as supplier A and supplier B. Both interviewees were suppliers of essential ICT systems and equipment for the control and distribution of power to end consumers. The interview with supplier A was done with the organization's principal engineer and acting cybersecurity manager, whereas the business development manager participated from supplier B.

The results from the interviews are divided into the four categories that we created during our data analysis: plans and communication, preparedness exercises, general thoughts on collaboration and attack scenarios. The section presents the results from the interviews with both DSOs and suppliers and highlights how each party relates

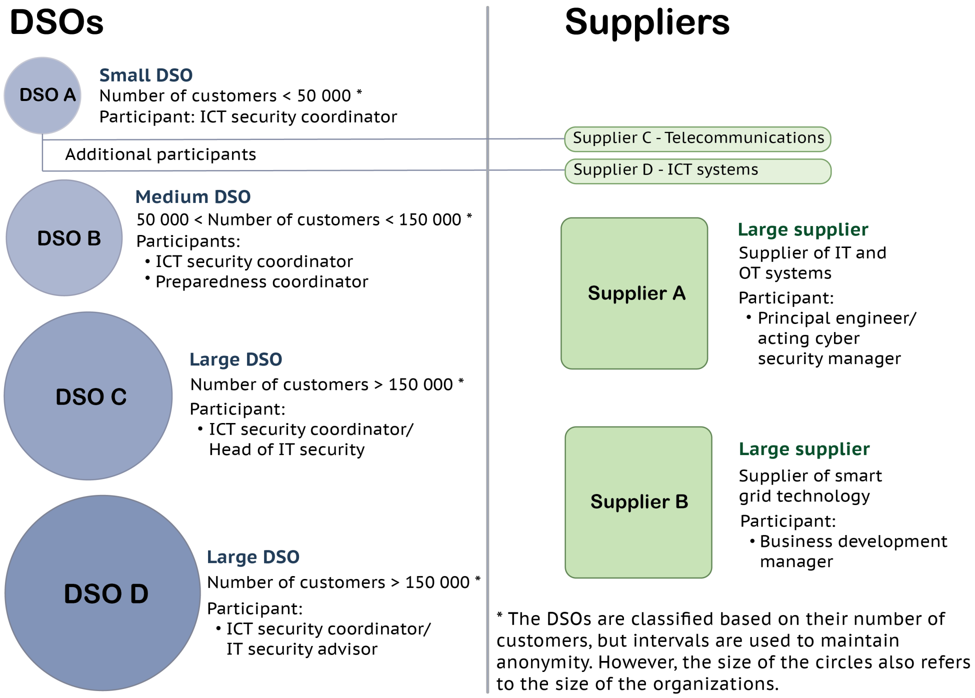

DSOs
Suppliers
DSO A
Small DSO
Number of customers < 50 000 *
Participant: ICT security coordinator
Additional participants
Supplier C - Telecommunications
Supplier D - ICT systems
DSO B
Medium DSO
50 000 < Number of customers < 150 000 *
Participants:
• ICT security coordinator
• Preparedness coordinator
Supplier A
Large supplier
Supplier of IT and OT systems
Participant:
• Principal engineer/ acting cyber security manager
DSO C
Large DSO
Number of customers > 150 000 *
Participant:
• ICT security coordinator/ Head of IT security
Supplier B
Large supplier
Supplier of smart grid technology
Participant:
• Business development manager
DSO D
Large DSO
Number of customers > 150 000 *
Participant:
• ICT security coordinator/ IT security advisor
* The DSOs are classified based on their number of customers, but intervals are used to maintain anonymity. However, the size of the circles also refers to the size of the organizations.

Figure 5.1: Overview of the interviewed parties and the participants at each interview.

to these topics. Relevant quotes from the interviews are included. As the interviews were conducted in Norwegian, each quote is translated from Norwegian to English.

5.1.1 Plans and Communication

It was necessary to gain insight into how the interviewed organizations respond to incidents and how the DSOs communicate with their suppliers and vice versa to make the scenarios and the corresponding exercises as realistic as possible. All of the interviewed organizations have a contingency plan that describes how they should handle unwanted incidents. There is, however, a varying degree of specificity in the plans.

> We do not have an incident management plan that focuses specifically on cyber-related incidents. We have an exercise plan that states that we shall conduct an evacuation exercise, and this is performed annually. We have an established desire to conduct cyber-related exercises.

> – DSO A

DSO A said that they do not have a specific plan for cyber-related incidents. The plan is open and does not describe any specific scenario, and it is largely based on improvisation. In addition to the general contingency plan, DSO B has an incident response plan specific for cyber incidents. The incident response plan includes, among other things, a diagram that describes the process for handling cyber incidents and a description of the different roles and responsibilities. DSO D works closely with some of its suppliers when developing plans and procedures for incident management. Some of the large suppliers have already defined routines that DSO D adopts, whereas they develop the plans together with some of the smaller suppliers. The supplier of the SCADA system has been involved in the development of DSO C's plans for incident response. Neither supplier A nor supplier B had been involved in creating contingency plans with any of their customer DSOs, but they have been asked to consult on occasions. Both of the suppliers have contingency plans for their own organization. When asked about their role during an incident at a customer, supplier A said they have a dedicated cybersecurity team that can assist. Supplier B highlights that the focus on cybersecurity has increased severely over the last 7-8 years and that they run cybersecurity preparedness exercises internally in their organization on a regular basis.

When asked about how they communicate with their suppliers during an incident, DSO A said that their contingency plan includes a prioritized list of people to contact. It is not specified in any agreement with the suppliers, but the people on the list have been informed. DSO B has an agreement with a group of people to contact that alternate on being on call. DSO C has a specified point of contact for all of their important suppliers. In addition, they have agreements on how the suppliers should assist them during incidents for the most important systems. Moreover, during an incident, a contact person is often appointed from the suppliers incident response team. For DSO D, the communication is regulated in the contracts, where both the DSO and suppliers state their requirements for the communication. In addition, they have regular meetings with the suppliers that provide operational and control systems.

Both suppliers have agreements with their customers that state what is expected of them. Supplier A has two types of agreements with their customers, a contingency agreement and a service agreement. Through these agreements, each customer has an appointed contact person and a support team at the supplier. In addition, these agreements specify in which cases there is a need for external support and set a requirement for how quickly the suppliers must be able to provide support in the event of an incident. Similarly, supplier B also has two different types of agreements with its customers; data processor agreement and support agreement. The data processor agreement describes the supply chain, and the customers are able to request an audit of it. The support agreement describes the support the supplier will provide to its customers, and how the dialogue concerning both the delivered systems and services and requests for assistance during incidents should take place.

5.1.2 Preparedness Exercises

All DSOs and suppliers were asked if they have conducted preparedness exercises before and if they have conducted any collaborative exercises to improve the collaboration between DSOs and suppliers. Since it is required in *Kraftberedskapsforskriften* to conduct preparedness exercises annually, all of the DSOs conduct exercises regularly. However, DSO A answered that these exercises mainly focus on aspects like weather and evacuation. They have not conducted preparedness exercises that focus specifically on cybersecurity incidents.

> If an incident occurred, it would be prudent that both of these suppliers are involved in the incident management.
>
> – DSO A

Neither DSO A nor DSO B has conducted preparedness exercises with their suppliers concerning cybersecurity incidents. DSO B had involved suppliers in exercises concerning other topics like contacting helicopters and organizing transportation during emergencies. DSO A stated that it would be necessary to involve the two suppliers (supplier C and supplier D in Figure 5.1) that participated in their interview if a cybersecurity incident should occur. DSO C said that it has happened that suppliers have been involved in preparedness exercises, but this is very rare. It would provide value to involve the suppliers in exercises related to the critical systems since they are the most familiar with the system design and its functions. DSO D, on the other hand, said that they conduct exercises with their suppliers and that this is something that they are dependent upon since they have suppliers in many areas of their operation.

> In the event of cybersecurity incidents, you are dependent on having the best people in each area, and they are often fully booked. Therefore, resource allocation becomes very important when planning an exercise.
>
> – DSO D

When asked which factors can make it easier to conduct exercises together with some of their suppliers, both DSO C and D mentioned that time is an important aspect when planning an exercise. In order to get the right people to participate, it is necessary to start the planning process as early as possible and make sure that the necessary participants set aside time for it in their schedule.

> An exercise for me is not to uncover where we are vulnerable in a technical manner, but where we have shortcomings administratively. The technical errors can be discovered by a penetration test or skilled operators.
>
> – DSO D

DSO D also said that they have experienced that very technical exercises with several planned scenarios are not always the best since the exercise planners do not always know all the details of the specific systems. Hence, the scenarios might end up not being as relevant as first thought. In their experience, it is more beneficial to have tabletop exercises where the participants can make suggestions as to which systems, risks or vulnerabilities they should discuss. Additionally, the focus should be on how the organization manages to handle the incident and not on how the technical personnel are able to discover the error and recover the targeted systems. In that way, one can ensure that the topic being discussed is real and relevant, and the participants will discover where they administratively are lacking a resource or a routine.

> (...) exercises are conducted so that the KBO units can test their whole internal work-chain. We would gladly contribute to the evaluation after an exercise. The KBO unit uses the exercise to test itself, its systems and procedures.
>
> – Supplier A

Supplier A has not participated in any exercises with its customer DSOs directly. The supplier is under the impression that exercises are a suitable way for testing plans and procedures for the individual DSOs. Supplier A works closely with its customers, but are not a part of the preparedness exercises. It has happened that they have functioned as observers during an exercise with their largest customers or been a little involved with alerting. If some function is to be tested, they might also assign a person to act as a stand-by in case something goes wrong. They are responsible for the products they deliver throughout the whole life-cycle, so their role when it comes to exercises is to help with risk assessments in advance and help assess and evaluate after the exercise.

Supplier A does not run internal exercises that focus specifically on cybersecurity within the company, but does perform preparedness exercises for other incidents. The supplier has thorough routines and plans regarding what to do if an incident occurs, both internally and externally. During an incident, the supplier's role is to be available, know what their tasks are, and assist with teams or other resources if necessary.

Similarly, supplier B does not conduct any training session or exercises with DSOs at the moment. However, they train to be able to resist attacks on their own and conduct training sessions on cyber attacks with all employees, as this is a part of the agreements they have with their customers.

5.1.3 General Thoughts on Collaboration

During the interviews, all of the interviewees were asked a general question about what they think may help to improve the collaboration between DSOs and their suppliers in incident management. DSO A highlighted the importance of trust in the DSO-supplier relationship and that they must trust each other to handle a situation effectively. As a consequence of this, the interviewee stated that there is a significant advantage with long-term relations. One of the suppliers (supplier C in Figure 5.1) that participated at DSO A's interview said that it could be beneficial to sit down and ensure that the correct routines for incident management are in place, especially regarding alerting and scaling. When these routines are in place, they could practice together in an exercise to get to know each others' plans. In addition, supplier C stated that there is a general agreement within the industry that exercises are conducted too rarely.

The interviewees at DSO B focused on the importance of clear agreements that describe the collaboration and the level of aid they expect from the supplier. They also highlighted that it is not enough to simply have the agreement. It is necessary to have continuous contact with the suppliers to ensure that they are aware of the agreement's content and ready when it is suddenly needed. In addition, it is important to be aware of changes in staff at both parties and the adjustments this requires in terms of communication and coordination. The interviewees at DSO B also mentioned the importance of establishing precise requirements about expected response time and having a plan for communication if the regular communication lines are down.

> (...) it is important that we have a close relationship with our suppliers and that it is not all based on an agreement that is never used. The day it is needed, it is not certain that the suppliers are aware that it exists.

> – DSO B

Similarly to the interviewees at DSO B, the interviewee at DSO C believes that it is important to be explicit about what is important for them as a customer. DSO D stated that in order to make the collaboration with the suppliers better during incident management, it is effective to have a different routine for ICT incidents, a sidetrack with direct contact, as this creates awareness.

Supplier A stated that collaboration is key within cybersecurity and incidents, and it is necessary to establish structures and collaborate since many stakeholders need to be involved. Similarly, supplier B said that it is all about coordination and emphasizes the importance of having a common understanding of the issues they face.

Q1: Have you ever conducted preparedness exercises with a supplier/DSO?
Q2: Are suppliers involved in the creation of the DSO's incident management plans?
Q3: Do you have a specified contact person at the DSO/supplier?

	Q1	**Q2**	**Q3**
DSO A	No	No	Yes
DSO B	Yes, but not with a focus on cyber related incidents	No	Yes
DSO C	It has happened, but it is very rare	Suppliers of the SCADA system have been involved	Yes
DSO D	Yes	Yes	Yes
Supplier A	No	No	Yes
Supplier B	No	No	Yes

Table 5.1: Summary of findings from interviews.

5.1.4 Attack Scenarios

The interviews were also used to gain insight into relevant attack scenarios that would require involvement from suppliers to handle. We asked both the DSOs and the suppliers questions regarding this, and their answers were used to create the attack scenarios described in Section 4.1. Since risk and vulnerability assessments conducted when creating contingency plans and incident management procedures contains sensitive power system information, the DSOs did not wish to share these with us. However, we received an incident response plan focusing on information security emergencies from DSO B, which gave us some insight into which systems that they consider to be most significant and how they would handle an incident in these systems.

DSO C said that attacks on both SCADA systems and administrative office systems would require the involvement of the suppliers of these systems, as the DSO does not have competency in the operation of these systems. The interviewees provided us with many examples of potential attacks, which components were involved and the potential consequences of the different attacks. To organize the answers, we grouped the examples into four broad categories based on the target or how the attack is performed. The categorization can be seen in Table 5.2.

Additionally, DSO D mentioned that vulnerabilities often are discovered in both internal and external systems without it having been exploited in an attack as far as they know. In this event, the DSO have to investigate whether the vulnerability has been exploited and the system is compromised. In addition, they have to work together to remove the vulnerability. This is also an example of a scenario that would be valuable to have an exercise on to establish some routines on how to proceed.

Cloud services	Attacks that take advantage of the fact that important services and systems are using cloud services.
Social engineering	Attacks that uses some form of social engineering techniques to gain access to systems or to trick employees into performing actions they should not do, like CFO fraud, disclosure of credentials and phishing attacks. These are often used as a way into the systems by attackers.
Attacks on critical control systems	Direct attacks on the SCADA system, SCADA related services or the AMI head-end system, that are critical in order to control the power distribution.
Other	Other attacks like crypto viruses or DDoS attacks were mentioned. In addition, attacks or errors with information or privacy disclosure as a consequence and attacks on social media accounts or websites.

Table 5.2: Categorization of gathered insight into relevant attack scenarios.

5.2 Feedback on the Scenarios

As presented in Section 3.2.1, feedback and evaluation was a part of the scenario development process. In order to validate that the created scenarios will be of value for the industry, we gathered feedback from two DSOs and two relevant authorities.

5.2.1 Feedback From DSOs

We received feedback on the scenarios from DSO A and B. The seven draft scenarios and some specific points that we wanted feedback on were distributed in advance. The feedback to each scenario from the two DSOs are given below. The points that we wanted feedback on were:

- Is there anything you would change or add to the scenarios to make them more realistic? Details, information, how things function in reality, etc.
- Is the level of detail sufficient in terms of relevance?
- Is there anything that could be changed to involve suppliers in a more expedient way?
- Are there any other discussion questions you would like to add or focus on?
- Does it provide any value to include a part that focuses on media management?

Attack on SCADA System The DSOs commented that it varies whether the DSOs have an operations center that is staffed 24 hours a day or only during normal working hours. Therefore, the scenario should either describe two alternatives depending on whether the operations center is staffed or be more general to cover both types of operations centers. In addition, they said that they only have a few substations that are monitored, so to see the error in the SCADA system, these substations have to be involved. Thus, it is not realistic that an operator uses remote access to check the SCADA system and state of the power grid. Instead, it would be natural for them to send out an operator to investigate and that the operator discovers that a large area has lost power.

Ransomware It was suggested that it should be clarified whether the control systems or AMS are affected by the ransomware or just administrative systems. In general, it should be specified which systems are down. Moreover, they suggested including discussion questions that focus on the DSOs policy for extortion attempts, if they have agreements with suppliers that guarantee assistance in this situation, and whether they have assessed which systems should be prioritized in such a situation.

Attack on AMI One of the DSOs commented that in Norway, an external supplier is usually responsible for the head-end system, but that both the DSO and the supplier have access to the power switch functionality. Therefore, they are entirely dependent upon help from the responsible supplier in this scenario. Similarly to the ransomware scenario, it was suggested to add discussion questions that focus on policy for extortion attempts and who has the authority to decide what they do.

Disclosure of Sensitive Power System Information The DSOs did not have much feedback on this scenario. However, they mentioned that in a scenario where information has been stolen or disclosed, it could be important to consider which information should be shared with the public and which communication channels should be used. Therefore, one question about this was added.

Attack on Cloud Services For this scenario, the DSOs thought that it would be relevant to look at all the systems using cloud services. It was commented that if the internet access were to be attacked by a Distributed Denial of Service (DDoS) attack, it would make all the cloud services unavailable. Here it would be relevant to include both the Internet Service Provider (ISP) and the cloud service provider. One of the DSOs commented that it would be interesting to have a question regarding the Service Level Agreement (SLA) in this context.

Defacing of Website In this kind of scenario, it was mentioned that it could be relevant to expand to active hacktivism and escalate it to multiple channels like social media accounts in addition to an attack on the website. The most significant risk in this scenario is that it would lead to a loss of reputation and trust for the DSO, but in general, this is not of the highest priority for a DSO since the most important thing is the security of the power supply. Thus, the events in this scenario are not as critical as some of the other created scenarios.

Exposed Vulnerable Services This scenario was created based on answers in the interview with DSO D held after the first round of feedback on the drafts. Therefore we do not have feedback from all the DSOs on this scenario, but the feedback from industry authorities are given in the next section.

In addition, one of the DSOs mentioned that it would be important to add a question to all of the scenarios about whom they would alert of this incident and at what time, since there is a requirement for the KBO units to alert NVE of these kinds of incidents without *unfounded* delay.

5.2.2 Feedback From Authorities

We also gathered feedback on the scenarios from relevant authorities, KraftCERT and NVE, to validate the value for the industry, not only individual DSOs. The feedback was given in writing, and the specific points that were asked for feedback on were:

- Are there any other aspects that should be considered and added?
- Are the level of detail appropriate and are the scenarios realistic?
- Will the scenarios provide any added value for the industry, not only individual DSOs? Input to changes that can make the scenarios more valuable?
- Will the scenarios contribute to making the exercise relevant for the participating suppliers as well?

Attack on SCADA System KraftCERT commented that the DSOs should have routines for handling the loss of SCADA ("Loss of view"). In order to involve the suppliers in a good way, it is essential to state clearly what and who should be trained in the exercise. In addition, they commented that in scenarios that involve SCADA, it is important to be attentive to highlight the cyber element. Otherwise, it would probably not be handled as a cyber incident. KraftCERT also mentioned that a question about whom the DSO would ask for assistance from should be added, as KraftCERT handles this on many occasions. NVE suggested adding a question about what would be prioritized in this situation, the regaining of power or salvage of the system.

Ransomware In this scenario, KraftCERT suggested that it should be considered to specify the affected services or systems in the first question. KraftCERT also mentioned that it is relevant to include a question about how the DSO would communicate with media, customers, employees, suppliers, and the government. In addition, a question about how to handle the incident if it lasts for a longer period of time (1 week, 1 month, 3 months, etc.) could be included. NVE commented that it should be asked how they would determine if they have an uninfected backup to use for recovery.

Attack on AMI Both NVE and KraftCERT mentioned that it is important to describe the scenarios clearly and concretely to avoid the participants having doubts. For example, it could be difficult for the participants to know whom the scenario refers to when we use the word *they*. In addition, KraftCERT commented that it could also be interesting to turn the last part of the scenario around so that it is the supplier that is compromised. NVE mentioned that the discussion questions in this scenario should include a focus on backup and how they would recover from the attack.

Disclosure of Sensitive Power System Information KraftCERT commented that it should be specified if the SCADA system is only delivered or also operated by an external supplier. The feedback was that several aspects were somewhat unclear (encryption, abnormal traffic, administrative networks vs operational network) in this scenario. Therefore, we should consider rewriting some parts, especially part 2.2. In addition, they said that some discussion questions from part 2.2 might be moved to part 2.1.

Attack on Cloud Services In this kind of scenario, KraftCERT mentioned that it is not realistic that the operation center would be contacted. Instead, the operation center would call the IT department, and so would the other employees in this case. Often, the operator in charge at the operations center does not have the competence to review logs. Depending on the company, the IT department may also lack competence regarding this. NVE commented that it might be unrealistic that all the systems running in the cloud would become unavailable.

Defacing of Website KraftCERT pointed out that the headline of this scenario should be changed to *Defacing of Website* or similar as *fake news* typically refers to lies in the media. Additionally, it should be explicitly stated in the introduction that the website is run by a supplier externally via CMS (Content Management Delivery).

Exposed Vulnerable Services KraftCERT thought it should be specified what kind of system that is affected. One example they gave was the Customer Information System (CIS), as this will involve GDPR and may require involvement from NVE, The Norwegian Data Protection Authority (*Datatilsynet*) and KraftCERT. Furthermore, they mentioned it might be necessary to state more clearly in the scenario that this may be a gateway for the attackers to gain a foothold before moving further in and compromising additional systems. KraftCERT also commented that it might be required to have some additional information and questions for the exercise facilitator if this is not an IT professional, as the exercise may come to a halt if the participants start to discuss the relevance, which systems are affected and so on. A suggestion to a discussion question is what alerting requirements the DSO has in this kind of incident. NVE added that a question asking if this incident would violate the requirements in *Kraftberedskapsforskriften* [Olj19] should be included.

The gathered feedback from both the DSOs and NVE and KraftCERT was reviewed, and we made adjustments to the scenarios. The discussion questions were also updated based on the given feedback. The final drafts of the scenarios are given in Appendix A.

5.3 Evaluation of Preparedness Exercise

The participants evaluated the exercise orally immediately after the exercise and in writing by answering an evaluation form during the following days. This section presents the results from the written evaluation. The questionnaire used to collect the written and structured evaluation can be found in Appendix B. All of the eight participants in the exercise have answered the evaluation. Thus, all of the percentages given below are calculated on the basis that 100 % is 8/8.

The following categories sum up the focus of the evaluation: the exercise goals, the participants, the duration, the digital format, and the scenario and discussion questions used. There were also some questions and feedback that focused more on the organization of the exercise and collaboration with suppliers in general. In addition, the DSO and supplier evaluated their own performance in the exercise, but as this is not relevant for this thesis, it will not be presented in this section.

5.3.1 The Goal of the Exercise

The goal of the exercise was presented in Section 4.2, but the subgoals will be repeated here for the evaluation. First, the participants answered to what degree they felt that the exercise goals were consistent with the participants of the exercise, the format of the exercise, the discussion questions and the attack scenario. For all the mentioned aspects, the participants answered that they coincide in a high to a very high degree with the exercise goals.

In addition, the participants were asked to which degree they felt that the different subgoals of the exercise were met and fulfilled.

Subgoal 1: Establish relationships and points of contact

For the first subgoal, 7 of the participants (87,5 %) answered that they felt this goal was fulfilled to a *high degree*, while 1 of the participants (12,5 %) answered that it was fulfilled to *some degree.*

Subgoal 2: Test all parties' knowledge of plans and contact points, and establish a common understanding of plans, roles and responsibilities during an incident

For the second subgoal, all participants answered that they felt that this subgoal was fulfilled to a high or very high degree. The distribution was that 6 of the participants (75 %) answered *high degree*, and 2 (25 %) answered *very high degree.*

Subgoal 3: Identify potentials points of improvement for the coordination and the plans

Similarly, for the third and final subgoal, all of the participants also agreed that this subgoal was fulfilled to a high or very high degree. Here the distribution was that 3 of the participants (37,5 %) answered *high degree*, and 5 (62,5 %) answered *very high degree*. We see that this is the subgoal that the participants felt were met to the highest degree during the exercise.

5.3.2 Participants

The participants of the exercise were presented in Section 4.2. The evaluation shows that the people and roles that were included in the exercise were appropriate and correct. As we can see in Figure 5.2 the answers were concentrated around the alternatives *high degree* and *very high degree*.

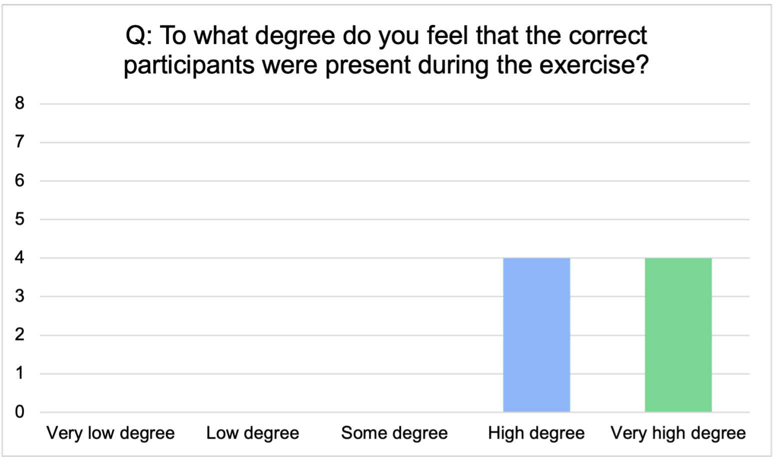


Figure 5.2: The results from the evaluation of whether the right participants were present at the exercise.

The participants were also asked to what degree they felt it was useful to have a collaborative exercise with employees from both the DSO and the suppliers. The results from the DSO showed that 5 out of 6 (83,3 %) felt it was useful to a *high degree* or *very high degree* to have an exercise with the suppliers, while 1 out of 6 (16,7 %) found it useful to *some degree*. From the suppliers, one answered that they found it useful to a *high degree*, while the other to a *very high degree*.

5.3.3 Duration

The participants answered that the allocated time for the exercise was sufficient and appropriate. When asked whether the actual duration of the exercise coincided with the allocated time, the majority felt that the amount of time was just right, as can be seen in Figure 5.3.

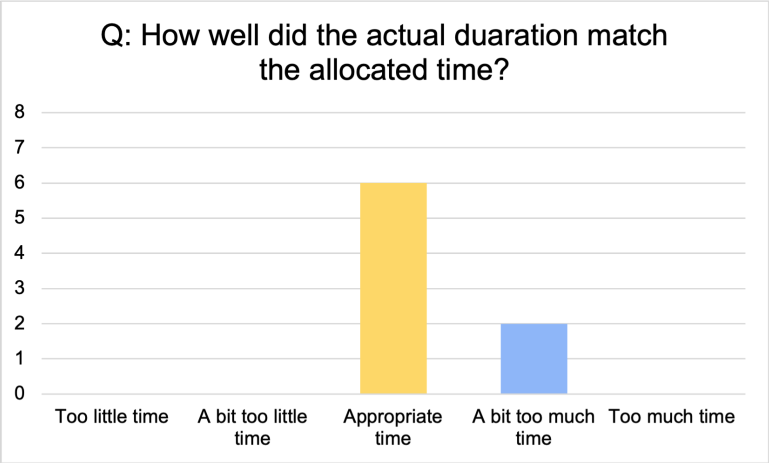


Figure 5.3: The results from the evaluation of the duration of the exercise.

When asked whether the distribution of the allocated time on the different parts of the exercise was appropriate, the participants answered that they had enough time to discuss the questions and the different topics that came up. However, it was commented that the distribution of time to the different parts was a bit skewed, and that this might be because some of the questions that were meant for later parts were discussed prematurely.

5.3.4 The Digital Format

The participants were asked how they thought it was to have a digital exercise. 7 of the participants (87,5 %) answered that it worked well or very well.

6 of the participants (75 %) felt that they were able to speak their opinions whenever they wanted to, and that the digital format hindered them from participating in the discussion to a small to a very small extent. However, when asked if they felt that the digital format influenced the outcome of the exercise, the answers were more scattered (Figure 5.4). 5 of out 8 (62,5 %) felt that it had influenced the exercise in a *low degree* or *very low degree*, whereas the remaining 3 participants (37,5 %) thought it had influenced the outcome in *some degree* or *high degree*.

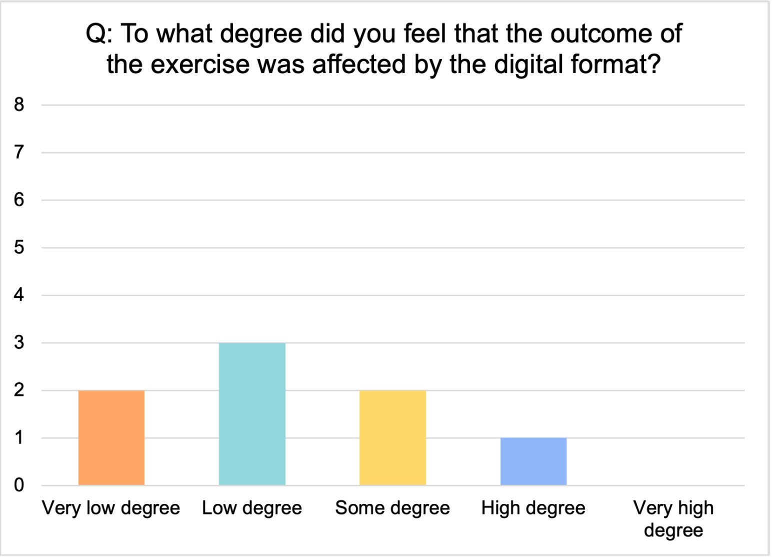


Figure 5.4: The results from the evaluation of the digital format.

In addition, the participants were asked if they could think of both advantages and disadvantages of having a digital exercise compared to a physical exercise. The results are given in Table 5.3.

Advantages	**Disadvantages**
Saved travel time for all participants	Less dynamical discussions among the participants
More flexible: • Easier to find the time for an exercise • Easier to include the suppliers	More difficult to build relationships and familiarity with each other
Gives a stricter structure: • Easier to stick to the agenda • More structure to the discussion and less interruptions	Higher threshold for participating in the discussion with own opinions and comments, especially in the beginning

Table 5.3: Advantages and disadvantages with the digital format in an preparedness exercise.

5.3.5 Scenarios and Discussion Questions

The participants were also asked about the relevance of the scenario and the discussion questions. All the participants answered that the scenario was in *high degree* or *very high degree* relevant for both the goals of the exercise and relevant for them to practice. Here, 5 out of 8 (62,5 %) answered to a *very high degree* and 3 out of 8 (37,5 %) a *high degree* that the scenario was relevant for the goals of the exercise. Whether the scenario was relevant for them to practice on, 7 out of 8 (87,5 %) answered to a *very high degree* and 1 out of 8 (12,5 %) a *high degree.*

> The scenario was credible and broad enough to start good discussions and reflections.
>
> – Exercise participant

The participants were also content with the discussion questions as 50 % felt in a *very high degree* and 50 % in a *high degree* that the discussion questions were relevant for the goals of the exercise.

5.3.6 General Feedback

The Organization of the Exercise The participants were unfamiliar with discussion exercises and the format in which they are held. Some of the participants were clearly prepared for a game exercise, and this caused some friction and confusion in the beginning. To avoid this, it should have been explained more clearly to all the participants in advance what a discussion exercise entails.

Collaboration with Suppliers The participants were also asked some open questions about the collaboration with suppliers, where they were free to write whatever they wanted. The questions they were asked were:

- What do you believe can make it easier to collaborate and coordinate with suppliers during incident management?
- What do you believe can make it easier to conduct exercises with suppliers?

Several of the participants, both from the DSO and the suppliers, mentioned regular meetings and exercises as a success factor to ease collaboration with suppliers during incident management. This will contribute to good relationships and knowledge of each other’s routines. When a good relationship with the suppliers has been established, it could be beneficial to have shared procedures and routines for incident management. Some also highlighted the importance of having a shared view of what is important and how they should proceed to secure it. Furthermore, the significance of having access to key personnel and clearly established points of contacts outside of working hours was also mentioned. During a crisis, it is not easy to get ahold of a supplier if they do not have a contact person that they have a regular and good dialogue with. In general, it seemed to be a common perception that it is crucial to have both close contact and trust in important suppliers.

As an answer to what can make it easier to conduct exercises with suppliers, it was brought up that it often is easier to focus on this if it is facilitated externally, e.g. by being handed an exercise program with two exercises per year. The importance of having a close dialogue with the suppliers and regular workshops was also mentioned. In addition, having a clear division of responsibilities and shared procedures will also be helpful. Generally, it requires openness and trust, and this must continuously be maintained as employees and suppliers may come and go.

In summary, the participants seemed very happy with the exercise. It was mentioned that it was useful, educational and exciting and that it will lead to more exercises and new plans in their company in the future.

Chapter 6 Discussion

In this chapter, the research questions presented in Chapter 1 will be discussed in the light of the created scenarios and exercise from Chapter 4 and the findings from the data collection as presented in Chapter 5. The chapter consists of two sections, where each section will discuss and attempt to answer one of the research questions.

6.1 Research Question 1: Scenarios

> RQ 1: What are scenarios for preparedness exercises that can improve the collaboration between DSOs and suppliers? And how can these be used in exercises?

In this section, we will address the first research question by considering the feedback from the industry and the choices that we made when creating the scenarios and planning the exercise. We will start by focusing on the first part of the research question, which concerns the scenarios. Afterwards, we will move on to the second part discussing the scenarios' usability in exercises considering the results from the conducted exercise.

6.1.1 Scenarios

Here, we will try to answer why the scenarios we have created are suitable for collaborative exercises with the purpose of improving the collaboration between DSOs and suppliers. In addition, we will try to highlight some aspects that are important to consider when creating scenarios for this purpose. The focus when developing the scenarios was to find suitable topics and focus areas that will serve this purpose and enable the conducting of collaborative exercises between the two parties.

Choice of Main Topics

The choice of main topics for the scenarios is essential to make them relevant for collaborative exercises. When working to identify ideas for the main topics for the attack scenarios, we used various sources. Input from the literature study and the interviews gave us insight into existing solutions in other industries and the dependencies in the DSOs' supply chains. In addition, inspiration was gathered by studying previous attacks, both general cyber attacks and attacks on the power grid. We did not have much prior knowledge about the electrical energy sector and which systems are in use. In addition, it is not easy to find information that contains in-depth details about the power supply in literature as much of it is defined as sensitive power system information, as described in Section 2.1.2. Thus, we were highly dependent on the insight we were given during the interviews with DSOs and suppliers.

When selecting the main topics and systems to focus on, we prioritized the input from the DSOs as they are the ones that the scenarios are intended for. Additionally, the DSOs are the ones who have the insight into their dependencies upon suppliers and which incidents they would not be able to handle without involving suppliers. Thus, to make the scenarios suitable for including suppliers, we looked into which suppliers the DSOs have and which systems are generally outsourced to suppliers. Then we either focused on the suppliers and what incidents they would have to consult on or the identified systems and investigated possible attacks against these. As a result, all the scenarios have a main topic that is related to an attack or incident involving a system or service delivered by a supplier.

Based on the gathered input, we developed the first iteration of scenarios before sharing it with the DSOs and industry authorities for feedback. The collaboration with the DSOs during the scenario development was mainly for the initial ideas and feedback on the draft scenarios. It may have been beneficial to have a closer collaboration with one or two DSOs in the development phase and involve them more to gain their insight for added realism and details. However, this could also have resulted in the scenarios being too specific for this DSO and not generalizable for others. This would also have required a lot more time and effort from the DSO's part. Hence, we chose the less involved approach.

Choice of Focus Areas

The focus areas of the scenarios were determined from the interview results and the overarching goal of the thesis: *to improve the collaboration between DSOs and their suppliers during incident response.* The focus areas of the scenarios have to be closely connected with the overarching goal of their use, and we wanted the focus areas to target the challenges in the supplier-DSO relationship. On the one hand, it can be valuable to ensure that the supplier's technical staff can respond to an incident. However, on the other hand, the incident's overall handling depends on the DSO and the supplier collaborating. Therefore, to make the scenarios and exercise fitting for the purpose of this thesis, we chose to focus on the essential aspects of good collaboration on an organizational level.

Several interviewees mentioned that good communication and clear contact points are essential to have a good collaboration with suppliers. They also brought up that the procedures for communication are not always defined in written agreements. Furthermore, even if the procedures are defined, it is not sure that the suppliers are aware of them since they most often have never been used or tested in exercises. Therefore, we put an extra focus on communication and alerting in the scenarios by including this in the description of the incident and the discussion questions. Concerning alerting, we also included a focus on alerting authorities as we found during the literature study and the interviews that the KBO units are obliged to alert NVE of these kinds of incidents without *unfounded* delay. It was also mentioned in the feedback on the draft scenarios to make sure to specify this.

During an incident, it is also important to have a common understanding of the roles and responsibilities of all parties involved, both within the organization and with the suppliers. The interviews revealed that the DSOs and the suppliers have little insight into each other's plans and procedures. Hence, we chose to use this as a focus area. We chose to do this by adding discussion questions focusing on procedures and the responsibilities of different roles and by avoiding specifying too many details about the incident handling in the scenarios. This way, we hoped to enable a discussion of these aspects, as the participants could direct their attention to the existing plans and procedures and discuss how the described incident would be handled. Consequently, the participants will gain insight into the content of the existing plans and the collective understanding of the plans and responsibilities across organizations. Furthermore, this may lead to discoveries of possible improvements for the plans and procedures.

In addition to the focus points already discussed, we chose to include a focus on media handling in some of the scenarios. Since attacks on the power grid will affect large portions of society, it will be necessary to handle external parties such as the media and customers. This may be an external factor that can cause extra stress in an already stressful situation of handling an incident, so the DSO must be prepared for this. It is uncertain how relevant this is with regards to the suppliers, but we chose to include it since it is important to inform the public about incidents properly.

The Choice of Exercise Type

The development of the scenarios was done with a focus on discussion exercises due to the time constraint and the scenario's intended purpose. According to NIST's guide on exercises [GNB$^+$06], discussion-based exercises are suitable for discussing roles during an emergency and familiarising oneself with the content of contingency plans and incident response plans. Functional exercises, on the other hand, allows operational personnel to validate their operational readiness. Hence, designing the scenarios for a discussion exercise better fits our purpose. Additionally, more extensive exercises require a more extended planning period, and the planning process should start at least three months prior to the exercise. Furthermore, it would require substantially more resources from the participating DSO if we were to develop a more extensive exercise. Thus, we chose to put our time into developing multiple scenarios and corresponding discussion exercises that can be more generalizable and used by multiple parties. We believe that this will provide more value to the industry than developing a more extensive exercise that would have to be more specific for one DSO. As presented in Section 2.4.2, discussion exercises can be effective, productive and provide a high yield to the participants while requiring minimal time and resources for planning. In addition, it can be beneficial that the exercise is not too resource-demanding when an important aspect is to include suppliers.

Level of Detail

The level of detail in the scenarios was chosen to make them as generalizable as possible. The aim was to ensure that the scenarios will be useful for multiple DSOs and suppliers, as we believe this will provide the most value for the industry. However, the suitable level of detail depends on how and by whom the scenarios are meant to be used. In a discussion exercise for the management level in an organization, too much focus on the technical details is unnecessary. However, if the scenarios should be used in exercises for the technical staff, more details may be required and the included details must be correct. Since we designed the scenarios for discussion exercises on the organizational level, the necessary amount of technical details was fairly low. However, determining the correct level of detail for our scenarios was essential for the flow of the exercise since discussing ambiguities takes time and attention away from the actual focus areas.

The following choices were made to make the scenarios relevant for multiple DSO and suppliers. The created scenarios only provide a general description of the incident and escalating factors without including too many details, e.g. names of systems, to avoid giving details that are wrong for some DSO. At the same time, it is necessary to include some details, so the users do not have to spend too much time altering the scenarios and thereby deciding not to use them. The level of detail that we have chosen in the scenarios should only require a few adjustments for the scenarios to be customized and ready to use by a specific DSO. We used one of the methods presented in Section 4.1 on the locations where it was necessary to include some details that may vary. The DSO and suppliers that participated in the discussion exercise made a few adaptations to the scenario that we tested. The adaptations done to the scenario can be found in the appendix by comparing the *Ransomware* scenario (A.2) to the slides that includes the scenario used in the exercise with the DSO (B.5). Finding the appropriate level of detail is also important to not lead or provide the participants with answers during the discussion. Therefore, the scenarios are divided into different parts to avoid providing the participants with answers prematurely. This way, the participants can discuss the first part before moving to the next part, where more information is given.

Use of Feedback

To ensure that the scenarios are relevant for the industry and the intended purpose, the process of gathering feedback and input from multiple sources was very helpful. Feedback on the scenarios was gathered from DSOs, NVE and KraftCERT. In this way, it was possible to get feedback from different points of view, strengthening the quality of the scenarios. NVE sees the industry from an overall perspective and can say something about whether the focus is relevant to the industry. KraftCERT has in-depth knowledge of the threat landscape and which attacks are possible based on the technical details of the systems. The DSOs can suggest specific changes that depends on how things are in their systems and with their suppliers. The feedback increases the likelihood that the scenarios can be used by multiple DSOs and suppliers. Without this feedback, the results of this master's thesis would lack reliability, as there would be no link to the actual target group. However, while the input to initial ideas was gathered from four DSOs of different sizes, the feedback on behalf of the DSOs are limited to two specific DSOs.

The provided feedback from the stakeholders resulted in adjustments to both the scenario and discussion questions due to logical shortcomings and lack of competence about how the organizations' systems work. However, when reviewing the feedback and choosing which suggestions to implement, we were conscious to avoid the scenarios being too specific for one DSO. Some of the feedback mentioned that the services and systems should be specified. However, we chose not to include this in the scenario. Instead, we added an explanatory text that includes examples of details that the DSO should consider adding in the scenario depending on which services and systems they use. This way, we avoid the scenario being too specific, but there is also a possibility that this leads to confusion for the participants. The choice of how much to specify was a matter of compromise during the entire development process.

6.1.2 The Usability of the Scenario in Exercises

This section will focus on the second part of research question 1 and discuss the usability of the scenarios in exercises that aim to improve the collaboration with suppliers. The discussion is based on the results from the conducted discussion exercise and findings from the literature study. The *Ransomware* scenario was tested in an exercise with DSO A and two of its suppliers. Due to the Covid-19 pandemic, the exercise was conducted digitally. There were 8 participants in the exercise, six from the DSO and two from the suppliers. The DSO that participated in the exercise is considered relatively small in the context of the Norwegian electrical power industry, which may have impacted the results discussed in this section.

The Exercise Goals

In general, it is important to determine clear goals based on the focus and desired outcome of the exercise. To gain the most from using the created scenarios in an exercise, the exercise planners must first determine the goals and objectives of the exercise based on the focus areas and the supplier they want to involve in the exercise. Then, the most fitting scenario can be chosen and applied in an exercise.

The primary goal of the exercise was determined based on the aim of this thesis: *to improve the collaboration between DSOs and their suppliers during incident response.* To achieve this, three subgoals were defined with the intention to specify the focus areas of the exercise. These were presented in Section 4.2. The subgoals focus on establishing relationships and clear communication, testing the knowledge and understanding of plans, roles and responsibilities during incidents, and identifying areas of improvement.

Since the relationship with the suppliers and a clear point of contact is the basis for all further cooperation, the first subgoal focuses on this. For some of the participants, this might have been clear before the exercise. However, it provides value to make other participants aware of whom to contact, and it may prove crucial in situations where the usual contact points are unreachable. The second subgoal was chosen since the interview results showed that the DSOs and the suppliers have little insight into each other's plans and procedures. In addition, a common understanding of these aspects is essential for good collaboration and incident management. The last subgoal was selected because it is crucial to uncover points of improvement and follow up on these to evolve and get a lasting impact from the exercise. The results from the evaluation of the exercise show that subgoal 3 received the best results regarding fulfilment, which is very good. It shows that the exercise was suitable and allowed discovering points of improvement. In this way, the exercise was already valuable for the participants, but it is important to implement the discovered countermeasures to get lasting value.

The results from the exercise evaluation show that the participants seemed to feel that all the goals were fulfilled to a rather high degree. Thus, pointing in the direction that the *Ransomware* scenario together with the corresponding discussion questions works well to fulfil the goals. Hence, the scenario can be assumed to be suitable for the overarching goal of improving collaboration between DSOs and suppliers and can be used in exercises with similar goals.

The Exercise Material

To ensure that the circumstances surrounding the exercise are optimal, it is important to create the necessary material to support the exercise and ensure that all participants have the information they need. In addition to the scenario and the discussion questions that together constituted the discussion exercise, it was necessary to create the additional exercise documents that were presented in Section 4.2 and can be found in Appendix B. However, we decided that we would not create the additional documents for the other created scenarios that were not used in the discussion exercise. This was because we want the users to decide how they want to use the scenarios and how these documents should be made to avoid putting too many guidelines on how they are supposed to be used. This increases the flexibility and generalizability of the scenarios and makes it easier to adapt them to each organization's needs.

The importance of being prepared to ensure that the exercise and scenario work optimally was displayed during the exercise, and it became clear that some of the exercise documents had some shortcomings. Early in the exercise, it became clear that some of the participants were unsure of what a discussion exercise entails and what the difference between this and other types of exercises are. Therefore, it would have been beneficial to add a description of this in the briefing that was distributed to the participants before the exercise. In addition, at one point during the exercise, the participants started discussing details that were not specified in the scenario or the facilitator guide. They ended up spending some time discussing this detail instead of how they would handle the incident. If additional details had been specified in the facilitator guide, this deviation from the topic could have been avoided. Thus, it is important to spend resources on creating the necessary documentation for the discussion exercise to ensure that the perceived value is as high as possible. Additionally, it is essential to have well thought-out questions for the evaluation to ensure that the selected focus areas are evaluated.

Relevance and Suitableness for Including Suppliers

As presented in Section 5.3.5, when the participants were asked if the scenario was relevant for them to use in an exercise, seven answered to a *very high degree* and one answered to a *high degree*. It was commented that the scenario was realistic and broad enough to start good discussions. In addition, the feedback showed that the majority of the participants from the DSO and the suppliers felt that it was useful to include the suppliers in the exercise. This shows that the scenario was applicable for discussion exercises with suppliers and provided value. However, it is difficult to draw any conclusions about the relevance of the other scenarios from this. Both because only one scenario was tested and since it was only tested with one DSO. This DSO is also a small DSO and the results may therefore not be applicable to DSOs of other sizes. Nevertheless, the different scenarios cover many of the same aspects within incident management and collaboration with suppliers, so it is reasonable to believe that they are suitable for exercises with this focus area. The relevance of the main topic in each scenario may vary from DSO to DSO since this depends on which systems they have and which is outsourced to suppliers.

Type of Exercise

As mentioned, we decided to design the scenarios for discussion exercises, and it was also in a discussion exercise that the *Ransomware* scenario was tested. In the evaluation after the exercise, it was mentioned that the participants who had previous experience with exercises were more used to game exercises. However, since they lacked the proper plans and procedures to deal with a ransomware attack, it was suitable to use a discussion exercise to have a thorough “run-through” of their plans. This allowed them to gain insight into the shortcomings in their plans and the lack of understanding of the content. After that, when they are familiar with the content of the incident management plans and procedures, it may be valuable to use the same scenario in a game exercise to test whether the plans function the way they are intended to in action. At the stage that DSO A was when we had the exercise, it would not bring any value to host a game exercise since they did not have a sufficient understanding of their plans, roles and responsibilities. This indicates that discussion exercises are suitable for exercises together with suppliers where the goal is to improve the understanding of each others’ roles, plans and procedures. In game exercises, functional exercises or full-scale exercises, on the other hand, the shortcomings could easily go unnoticed as these exercises primarily focus on each party’s handling of the incident.

The developed scenarios may also be used in discussion exercises with different goals by adjusting the discussion questions. In addition, they may be used as a starting point in larger and more functional exercises. This will, however, require adaptations to the scenarios and further development of playbooks.

Participants

When conducting exercises, having the right participants from both the DSO and the participating supplier is crucial for the outcome of the exercise. In the conducted discussion exercise, the participants consisted of employees with managerial positions who worked on an organizational level, meaning that they would be to ones that would make the decisions and handle the coordination if an actual incident had occurred. When the scenarios are to be utilized in an exercise where the goal is to improve cooperation, it is natural that the participants are those who have to cooperate in order to handle the incident well across organizations.

In addition, the participants from the suppliers must be the ones that would be contacted and involved during an incident. In the conducted exercise, one representative from two of the DSO's suppliers participated. These were the ones responsible for the information security of their supplied systems and would have to be involved if an incident occurs. It seemed that having two suppliers participating in the same exercise worked well in this case, as they already had a relationship with each other and the DSO. However, it is difficult to know if this would have worked if the two suppliers were large scale suppliers. This might lead to one of the suppliers being obsolete, leading to a loss of motivation for participating in exercises with DSOs. On the other side, it could be valuable for the suppliers to get insight into how the other supplier handles incidents, as they may be required to work together during an incident. Whether or not it is valuable to include multiple suppliers in one exercise depends on several factors, like the relationship between the suppliers and the difference in size. In addition, it depends on whether the scenario and the handling of the incident are suitable for including multiple suppliers that are equally important in the incident management.

As mentioned, there was only one participant from each of the suppliers. On the one hand, this means that only one person at the supplier gains insight into the collaboration. Hence, this person must forward the information to other relevant employees at the supplier. If this is not done properly, the DSO will become very dependent upon one specific person at the supplier. On the other hand, it will clarify whom the DSO should contact and coordinate with if only one from the supplier participates. Nevertheless, it should be considered whether it is possible to include more participants from the suppliers as this will most likely increase the value of the exercise.

The results from the evaluation of the exercise show that the participants felt to a high degree that the relevant participants were present, and there were no comments on additional people that should have been present. The number of participants seemed to be ideal for this DSO as there were enough people to cover the necessary knowledge to get a valuable discussion, while everyone seemed to get the time/place to speak. However, it is important to notice that there may be a difference from organization to organization how many participants is needed to cover the necessary knowledge to ensure a good discussion.

The Digital Format

The digital format that was used for the exercise brings both advantages and disadvantages. As presented in Section 5.3.4, the results from the feedback on the exercise show that most of the participants felt that having a digital exercise worked well. However, when asked if they felt that the digital format influenced the outcome of the exercise, the answers were more scattered. The participants were also asked to list any pros or cons they could think of, presented in Table 5.3 in Chapter 5. It may be debated whether the pros outweigh the cons when the focus is on conducting collaborative exercises with suppliers. If having a digital exercise makes it possible to conduct an exercise that otherwise not would have been conducted, it would provide a significant value even if the outcome of the exercise could have been better if it was conducted physically.

There is reason to believe that the number of participants is an important aspect to consider when discussing how well exercises work digitally, as this may impact the quality of the discussion. If there are many participants, the digital format may make it more difficult to have a good discussion where everyone contributes. How well a digital exercise works could also vary depending on how familiar the participants are with each other. The results from the exercise may have been influenced by the fact that several participants already knew each other pretty well. However, this may have contributed to both positive and negative effects as the quality of the discussion may become both better and worse from this. On the one hand, the participants may feel more comfortable, lowering the threshold for contributing with their own opinions and comments in the discussion. On the other hand, it may also be more interruptions and more challenging to stick to the agenda.

6.2 Research Question 2: Supplier Participation

> RQ 2: Which factors could make it easier for suppliers to participate in preparedness exercises with DSOs?

The results from the interviews were presented in Section 5.1. Regarding participation in exercises, it was revealed that only the largest DSO conducted exercises with its suppliers regularly, whereas the three other DSOs either did not at all or very rarely conduct exercises with their suppliers. The two interviewed suppliers had not participated as active participants in preparedness exercises with their customers. Simultaneously, the DSOs' level of dependence upon suppliers to handle incidents is high [SKP^{+}17], increasing the necessity to involve the suppliers in incident management. In this section, some factors that might make it easier for suppliers to participate in preparedness exercises with the DSOs will be discussed. Both the interviewees and the participants at the discussion exercise were asked this question, and the following discussion is based on the factors mentioned.

The Planning Phase

One of the most integral parts of conducting preparedness exercises is the planning phase. The implementation of this phase greatly affects the outcome and value of the exercise. First, it is important to identify the desired outcome of the exercise, and then decide the objectives and goals of the exercise based on this. Further, the planners have to select a relevant scenario and type of exercise. Based on this, it is essential to make sure that the right participants are available at the time of the exercise. Therefore, as one of the interviewed DSOs mentioned, it is important to start the planning phase in good time before the exercise. This might be especially important in terms of the suppliers that have many DSOs as their customers. In those cases, it is important to contact them well in advance of the exercise to agree on a suitable time so the right people at the supplier are available to participate in the exercise. This makes it easier to plan ahead and increases the probability that they are able to participate.

Furthermore, another thing that could lower the threshold and make it easier for suppliers to participate in exercises is to avoid setting aside too much time for the exercise. It is less challenging to commit to participating in an exercise that will last 3 hours than if they have to set aside a whole day or longer. Thus, it may make it easier to have collaborative exercises if one strives to keep them as short as possible to lower the perceived time cost for the supplier. Moreover, the supplier may also find it easier to spend resources on an exercise if the number of people that have to be involved from the supplier is minimized. To spare one or two employees for a few hours might not be perceived as a problem, but if many employees are removed from their daily tasks, it could be a more significant sacrifice. Of course, if some knowledge from the supplier is lacking due to the few participants, it might influence the outcome and value of the exercise. However, it is better to have a few than no representatives from the supplier.

In addition, a factor that could make it easier for a supplier to participate in exercises is to involve them in the planning phase from the start and increase their ownership of the incident management procedures of the DSOs. Suppose the supplier can ensure from the beginning that the goals of the exercise are suitable for them as well and that it would be relevant for them to practice the handling of the chosen attack scenario. In that case, it may increase the willingness of the supplier to dedicate resources to it. This would naturally increase the workload for the supplier, but it could be a trade-off between resources spent and value received for the supplier.

Recommendation: ***Start the planning phase early and involve the suppliers from the beginning***

Collaborating on Incident Management Plans

According to the ISO/IEC 27035 standard, all external parties that might be needed for support should have access to the documented procedures related to crisis management to ensure quick and effective responses to cybersecurity incidents [Int16]. However, the interviews with the DSOs and the suppliers in this study revealed that there is very little sharing and collaboration between the two parties when it comes to creating the incident management plans and routines.

The consequence of suppliers not being informed of the incident management plans is that the coordination and collaborative decisions during incidents will be more difficult due to a lack of a shared understanding of written or unwritten rules, procedures, routines and roles. Increasing both parties' knowledge of each other's documents and procedures related to incident management can make it easier to collaborate on preparedness exercises in general because it would give them insight into and ownership of the incident management. A way to achieve this is to collaborate on making incident response plans for the system that the supplier delivers and/or operates, and agree on the common routines. In that way, the suppliers would have a central role in the incident management already from the start and could easier be included in further activities like exercises. However, the supplier might be reluctant to this because of the amount of resources and cost it would require for them to collaborate with several of their customers. Still, since their service to most of their customers and the content of the incident response plans will be similar, the suppliers can possibly reduce the amount of work by reusing content and making concrete suggestions.

Recommendation: ***Involve the suppliers when creating incident management plans***

Dedicated Resources

Preparing exercises require a lot of planning and resources, and for the organizers, it will always compete with the other daily and possibly more urgent tasks. Therefore, the planning of exercises is possibly not prioritized by the people responsible for arranging them [LTJ14]. Furthermore, as Eriksen and Gunabala discovered, suppliers are not involved because it requires more planning and resources to involve additional parties in the process [EG20]. Similarly as for the DSOs, exercises consume resources from other parts of the suppliers' services and might not look beneficial enough at first sight. However, it is important to consider that, without suppliers, the handling of an attack scenario will not be as realistic and they will not be able to test the collaboration and develop a mutual understanding [FHT13].

Kraftberedskapsforskriften [Olj19] requires that all KBO units have an ICT security coordinator and a preparedness coordinator in the organization. It would be natural that the people who have these positions at a DSO are responsible for planning and arranging preparedness exercises. However, based on the fact both this and other studies [LTJ14, LTJ16] show that few cybersecurity preparedness exercises are conducted, this might indicate a lack of resources and ICT personnel who can ensure that these types of exercises are conducted in the cybersecurity domain. If this is the case, it is natural that they prioritize conducting internal exercises and that including suppliers in exercises has to come further down the line. Hiring more cybersecurity personnel dedicated to the planning of cybersecurity exercises with suppliers and information security incident management may be an important step to achieve better collaboration with suppliers. This also applies to suppliers, as it could make the collaboration on incident management better if the suppliers also have more dedicated resources to focus on the collaboration and coordination around exercises.

Recommendation: ***Dedicate the necessary resources to manage planning and have the necessary annual exercises***

Type of Exercise

As presented in Section 2.4.2, there are (at least) four different types of exercises. Each comes with different benefits depending on the defined goals of a preparedness exercise. The exercise types also vary in terms of the resources that must be put into the exercise. In general, the more realistic the exercise should be, the more resources have to be put into planning and implementing the exercise. Consequently, as very few collaborative exercises are conducted today, it might be beneficial to start with less resource-demanding exercises, like discussion or game exercises. This is also supported by the fact that the interviewees expressed very little knowledge of each other's plans on both sides, which makes it challenging to run a functional exercise right away. In addition, the less resource-demanding exercises do not require any disruptions of critical systems that could cause interruptions in the power supply, substantially decreasing the cost of an exercise. As the collaboration and familiarity with each other's procedures improve, it could be beneficial to test the knowledge of incident management plans in a more hands-on exercise.

Another aspect to this is that the value of highly technical exercises might not be the highest unless all the conditions for success are present. As DSO D said in its interview, the technical exercises with very detailed scenarios are often not the best since the planner of the exercise might not always know all the necessary details of the different systems, and the scenarios might end up not being as relevant as first thought. The consequence is that the participants are left feeling that they have wasted time and resources on the exercise. A precise and relevant technical exercise would require the involvement of technical employees at the supplier in the planning. This type of exercise would mostly work as a confirmation to the DSO that the supplier's technical personnel can handle an incident on a technical level. However, a prerequisite for the incident to be handled in an acceptable manner is that the incident is handled well on an organizational level with the necessary coordination and collaboration between the DSOs' and supplier's employees. If routines for communication, responding, or alerting are insufficient, or if the responsibilities and roles of the different parties are unclear, it might not help that the technical personnel knows how to solve the problem.

In summary, all of the participants must agree on what one wishes to achieve with the exercise. An exercise that tests the technical operation of systems is very different from exercises that test the communication, collaboration, and procedures during incident management and requires very different participants. Based on the limited experience of having collaborative exercises with suppliers, it might be more beneficial to have exercises that focus on building a relationship and knowledge of each other's plans and procedures. This is also supported by DSO D, which mentioned that it is more valuable to have exercises that enable them to discover where they administratively are lacking a resource or a routine. For this purpose, both discussion exercises and game exercises work well.

> **Recommendation:** ***Start with a less resource demanding exercise in the beginning, to familiarize with each others plans and procedures***

Facilitation

A preparedness exercise can be facilitated internally by employees of the DSO (and supplier) or externally by industry organizations with experience with preparedness exercises. Examples of this kind of organization can be KraftCERT or NVE. On their website, KraftCERT state that they can be of assistance for their members by counselling or participating in preparedness exercises.[1] In the evaluation of the conducted discussion exercise, it was mentioned that it might be easier to have collaborative exercises regularly if the exercises were facilitated externally. If an external party took the responsibility of coordination with both the DSO and supplier

[1] https://www.kraftcert.no/english/tjenester.html

and the planning of the exercise, it would lessen the resource and time demand on the DSO and the supplier. However, to create a relevant exercise, it is necessary to have specific knowledge of the systems, how they work together, and what routines should be tested in an exercise. Thus, it is necessary with active involvement from both the DSO and possibly the supplier in the planning process either way.

External facilitation could be done by facilitating specific exercises or by providing a complete and facilitated exercise program, with 1 to 2 exercises per year. § 2–7.Exercises in *Kraftberedskapsforskriften* [Olj19], as presented in Section 2.1.2, requires that all KBO units have an exercise program that spans over several years. However, there is no specification as to what types of incidents this exercise program should cover. Therefore, there is no guarantee that the KBO units have an exercise program that focuses on cybersecurity incidents. This was mentioned as something that could make it easier to include suppliers in exercises. An externally provided and facilitated exercise program for cybersecurity would increase the feeling of responsibility of the DSO and supplier to carry out the exercises. In addition, the exercise program would enable all participants to set aside the time for the defined exercises well in advance and ensure predictability for both the DSO and the supplier. However, even though this might be a good solution to enable more collaborative exercises, it is not very feasible considering the amount of resources required of the external organization if they were to facilitate two exercises a year for several DSOs. The predictability can still be achieved by making an annual exercise program internally at the DSO for collaborative preparedness exercises on cybersecurity incidents. The scenarios we have created in this thesis could be used for this purpose. The DSO and supplier could simply agree on the scenarios, the format the exercises should be on and select a group of people to implement them.

> **Recommendation:** ***Create a 2-year exercise program with the suppliers with external or internal facilitation***

Lack of Motivation

During the interview with supplier A, we got the impression that the supplier felt that participating in exercises was not a part of their role as a supplier. The supplier did not see the point of participating in exercises. It is challenging to encourage the suppliers to participate in exercises if they have no motivation to do it. One has to ask oneself why the suppliers do not feel like they need to be included in exercises when they play a crucial role during the management of real incidents. It might be easy to think that the benefits of preparedness exercises only fall upon the DSOs. However, suppliers would also benefit from a well-functioning incident management scheme and being able to provide the needed assistance in the event of an incident.

As in all business, it is beneficial to have satisfied customers and a good reputation, as unsatisfied customers are more likely to terminate the collaboration. With the limited amount of customers in the Norwegian market, it is desirable to keep them. Moreover, as several reports have pointed out that it is important to involve suppliers to improve incident management, the suppliers should also feel obliged to offer their assistance. In general, a way to overcome the lack of motivation to participate in exercises can be to make more explicit requirements to the suppliers, either through requirements from the authorities or the DSOs.

Requirements From Authorities As mentioned in Section 2.1.2, *Kraftberedskapsforskriften* [Olj19] requires an annual preparedness exercise in each KBO unit. § *6–5.Procurements* also specifies requirements when it comes to suppliers and their information security. However, it does not address if or how often DSOs should conduct preparedness exercises with suppliers. The combination of the lack of clear requirements from authorities and what seems to be a lack of incentive from the industry might be a reason why so few collaborative exercises are conducted between DSOs and suppliers in Norway. If the regulation had been updated with a requirement that DSOs should have at least one annual cybersecurity exercise with their suppliers, it would send a signal to the sector that this is necessary. Thus, this might become a priority of the DSO and the suppliers' motivation and perception of their role and responsibilities might change.

The advantages of a specified requirement to involve suppliers in exercises would be to ensure that exercises of this type are carried out regularly and that it will be the same for everyone. During the procurement process with new suppliers, both the DSO and supplier will know that participation in cybersecurity preparedness exercises will be a part of the collaboration. The requirements to the preparedness level for cybersecurity incidents will also become more explicit and easier to interpret. However, a possible problem with adding such a requirement is that the suppliers of ICT systems in the electrical power sector might be very different, both in terms of their size and the type of service they deliver. Thus, it is not easy to define a requirement that will be suitable for all parties. In addition, depending on which type of ICT system the supplier delivers, it might not be as relevant or critical to participate in a cybersecurity exercise. Hence, an updated regulation will create the necessary incentive to ensure that exercises are conducted, but it might also cause difficulties for some suppliers and DSOs. Nevertheless, a change in the regulation will force the DSOs to prioritize involving suppliers in exercises, which in turn will result in increased preparedness.

Recommendation: ***The authorities should specify requirements regarding involvement of suppliers in pre-***

paredness exercises

Requirements From DSOs in the Procurement Process Another way to increase the incentive for the suppliers to participate in exercises with DSOs could be to add focus on this in the procurement process. Making it clear to the suppliers that this is something that the DSOs will consider as an important factor when they make a choice might force the suppliers to also pay some attention to this. However, it can be discussed whether the DSOs or the suppliers have the leverage when negotiating a supplier-customer relationship. On the one hand, the DSOs have the power to chose which supplier they want to enter an agreement with based on the terms and conditions the supplier brings to the table. On the other hand, the small number of suppliers in Norway gives the DSOs less of a choice, especially since many of the Norwegian DSOs are small in size, whereas the suppliers often are large multinational companies [Rik21]. Thus, it may be challenging for the DSOs to have an influence on the security requirements and they might be forced to chose the largest and most experienced supplier of a service regardless of their offer when it comes to their involvement in the incident management process. One thing is for sure, it is the DSOs that have to take the initiative to exercises and invite the suppliers, and they cannot rely on suppliers to improve incident management through exercises. They have to initiate participation in exercises themselves, and one way to do this is to add this requirement to the contracts with the suppliers that they would be highly dependent upon if an incident occurs. In this way, the DSOs themselves can control which systems and suppliers they deem it necessary to have preparedness exercises with and who it is not necessary to require this from.

Recommendation: *DSOs should include requirements of participation in preparedness exercises in the contracts with suppliers*

The Availability of Relevant Attack Scenarios

As a final aspect that will make it easier to involve suppliers in preparedness exercises, we would like to mention the availability of relevant attack scenarios. Having access to appropriate and relevant scenarios and other exercise material that focuses on the collaboration between DSOs and suppliers can make it easier to conduct collaborative exercises and see the benefits of participating for both parties. If the material is crafted with a special focus on making them relevant for these exercises, it is easier to believe that the received value will be higher. In addition, the fact that most of the material exists and are ready to use also reduces the amount of resources that the exercise planners have to spend on the planning. Most of the existing exercise and scenario material has little focus on cybersecurity and the involvement of suppliers in incident management. Thus, the scenarios and exercise material created in this study can contribute to cover this need and aid in making it easier to conduct exercises that will improve the collaboration.

Chapter 7 Conclusion

In this thesis, we have examined the Norwegian electrical energy sector and how we can enable suppliers' involvement in preparedness exercises with DSOs. This section provides a conclusion based on the two research questions and suggestions for further research that can be conducted in this research area.

RQ 1: What are scenarios for preparedness exercises that can improve the collaboration between DSOs and suppliers? And how can these be used in exercises?

For the first research question, we have created seven attack scenarios that focus on cyber attacks on some of the systems delivered and operated by suppliers for many Norwegian DSOs. When creating scenarios for this purpose, it is important to consider the following aspects. The main topic has to be closely related to a service or system delivered by a supplier, the focus areas should be important aspects regarding collaboration, and the type of exercise the scenarios are designed for should be suitable for the chosen focus areas. From the data collection, we discovered that important focus areas for the scenarios were procedures for good communication, understanding of roles and responsibilities during incidents, and insight into the contingency and incident response plans. In addition, it is important to consider the target group of the scenarios since the level of detail has to be selected based on whether the participants are the technical or organizational staff.

For all of the created scenarios, it is necessary to involve the supplier of the affected system to recover from the described attack. In that way, the scenarios can improve the collaboration and cohesiveness during incident management by making the parties aware of each other's procedures, resources, and responsibilities. The feedback on the scenarios and the results from the test of one of the scenarios in the conducted discussion exercise shows that the scenarios can be used in exercises and that they are likely to provide value to the industry. Because of the limited number of interviewed DSOs and suppliers, the generalizability might not be as high as desired. However, the validation from NVE and KraftCERT, as authorities in the industry, increase the likelihood of them having value to more than the interviewed DSOs and suppliers.

RQ 2: Which factors could make it easier for suppliers to participate in preparedness exercises with DSOs?

For the second research question, we have discussed seven factors that could enable suppliers to participate in preparedness exercises with their customers. Based on this discussion, we presented recommendations to the industry. These revolve around the involvement of suppliers in the planning of exercises and creation of incident management plans, dedicated resources, less resource-demanding exercises, facilitation, and specified requirements to suppliers either in *Kraftberedskapsforskriften* or in the DSO's contracts with suppliers. Which of these recommendations that can and should be implemented, how they work together and can be combined, and how they affect the collaboration is something that can be researched further.

Additionally, as this study has shown, digital exercises can work well and provide value to the participants. Thus, the use of digital video conferencing platforms can possibly be a factor that could make it easier for suppliers to participate in preparedness exercises with DSOs. This would make it less demanding to conduct exercises when the supplier is located at a different place, and it would also save the time used for traveling. However, this has not been the focus of this study, and further studies should be conducted to draw a conclusion.

Furthermore, the scenarios created in this thesis are designed to be used in discussion exercises. As a result, future work can be to adapt and develop the scenarios to be used in game exercises and more functional exercises. Moreover, this thesis has not investigated attack scenarios that will require the involvement of more than one supplier or attack scenarios that involve an attack on a supplier that leads to consequences for several DSOs. With the supplier concentration in the Norwegian electrical energy sector, this should be further researched in future work.

To summarize, this thesis has contributed with attack scenarios and exercise material for discussion exercises that intend to help improve the collaboration between DSOs and suppliers in incident management. In addition, it discusses factors and provides recommendations that could make it easier for suppliers to participate in preparedness exercises with their customers. However, as there is a lack of standards and guidelines on how suppliers should be included in incident management, it would provide value to continue researching how the collaboration and requirements can be more well-defined. Our research shows that preparedness exercises and the involvement of suppliers in the electrical energy sector in Norway can be further researched in several ways. With the increasing threat of cyber attacks, identifying further factors that could make this industry more prepared to handle cyber attacks will be important.

References

[AAF$^+$08] Petter G. Almklov, Stian Antonsen, Jørn Fenstad, Endre Jacobsen, Agnes Nybø, and Gerd Kjølle. Fra forvaltning til forretning. Restrukturering av norske nettselskaper og konsekvenser for samfunnssikkerhet. Technical report, NTNU Samfunnsforskning AS, December 2008. (In Norwegian).

[ACS19] Alexander Adamov, Anders Carlsson, and Tomasz Surmacz. An Analysis of LockerGoga Ransomware. In *2019 IEEE East-West Design Test Symposium (EWDTS)*, pages 1–5. IEEE, September 2019.

[agi21] agility.im. Incremental VS iterative development? Available online at https://agility.im/frequent-agile-question/difference-incremental-iterative-development/, 2021. Last visited: 01.03.2021.

[And18] Andy Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Available online at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, August 2018. Last visited: 09.03.2021.

[Ant17] Anton Cherepanov and Robert Lipovsky. Industroyer: Biggest threat to industrial control systems since Stuxnet. Available online at https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/, June 2017.

[Bab18] Mohamed Babikir. Convergence Of IT And OT In Energy And Manufacturing. Available online at https://www.digitalistmag.com/cio-knowledge/2018/11/05/convergence-of-it-ot-in-energy-manufacturing-06192743/, November 2018. Last visited: 23.01.2021.

[BM16] Maria Bartnes and Nils Brede Moe. Challenges in IT security preparedness exercises: A case study. *Computers & Security*, 67:280–290, 2016.

[BMH16] Maria Bartnes, Nils Brede Moe, and Poul E. Heedaard. The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, 61:32–45, 2016.

[Bru13] Cyrill Brunschwiler. Advanced Metering Infrastructure Architecture and Components. Available online at https://blog.compass-security.com/2013/02/

advanced-metering-infrastructure-architecture-and-components/, 2013. Last visited: 25.05.2021.

[CMGS12] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. *NIST SP 800-61 Computer Security Incident Handling Guide.* National Institute of Standards and Technology (NIST), 2 edition, August 2012.

[Cor16] The North American Electric Reliability Corporation. Grid Security Exercise: GridEx III Report. Technical report, March 2016.

[Cyb20] Cybersecurity Competence Center Luxembourg. The Cybersecurity Competence Center. Available online at https://www.c3.lu/about/, 2020. Last visited: 10.03.2021.

[DBC06] Barbara DiCicco-Bloom and Benjamin F. Crabtree. The qualitative research interview. *Medical Education*, 40:314–321, 2006.

[Dir16a] Direktoratet for samfunnssikkerhet og beredskap (DSB). Grunnbok: Introduksjon og prinsipper. In *Veileder i planlegging, gjennomføring og evaluering av øvelser*, 2016. (In Norwegian).

[Dir16b] Direktoratet for samfunnssikkerhet og beredskap (DSB). Metodehefte: Diskusjonsøvelse. In *Veileder i planlegging, gjennomføring og evaluering av øvelser*, 2016. (In Norwegian).

[Dir16c] Direktoratet for samfunnssikkerhet og beredskap (DSB). Metodehefte: Spilløvelse. In *Veileder i planlegging, gjennomføring og evaluering av øvelser*, 2016. (In Norwegian).

[Dra17] Dragos Inc. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. Technical report, Dragos Inc., June 2017.

[Eas21] Eastern Peak. Iterative Development Model. Available online at https://easternpeak.com/definition/iterative-development/, 2021. Last visited: 01.03.2021.

[E.D14] E.DSO. Why smart grids? Available online at https://www.edsoforsmartgrids.eu/home/why-smart-grids/, 2014. Last visited: 03.02.2021.

[EG20] Sara Waaler Eriksen and Sarmilan Gunabala. Cybersecurity Incident Management In The Electrical Energy Sector: Involvement Of Suppliers. Master's thesis, The Norwegian University of Science and Technology, 2020.

[Ele15] Electric Power Research Institute (EPRI). *Electric Sector Failure Scenarios and Impact Analyses – Version 3.0.* National Electric Sector Cybersecurity Organization Resource (NESCOR), December 2015.

[ENI21] ENISA. ICS SCADA. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada, 2021. Last visited: 04.05.2021.

[Eur10] European Union Agency for Cybersecurity (ENISA). *Good Practice Guide for Incident Management.* ENISA, December 2010.

[Evj17] Ingar Evjen. What is AMS, AMR & AMI? Available online at http://blog.teleplanglobe.no/what-is-ams-amr-and-ami, 2017. Last visited: 04.05.2021.

[fC19] Center for Cybersikkerhed. Informationssikkerhed i leverandørforhold. Technical report, October 2019. (In Danish).

[FHT13] Robert Floodeen, John Haller, and Brett Tjaden. Identifying a Shared Mental Model Among Incident Responders. In *Seventh International Conference on IT Security Incident Management and IT Forensics 2013*, volume 1, pages 15–25, 2013.

[For21] Fortinet. What Is Operational Technology (OT)? Available online at https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security, 2021. Last visited: 27.01.2021.

[fsobD20] Direktoratet for samfunnssikkerhet og beredskap (DSB). Ovelse.no. Available online at https://ovelse.no/, 2020. (In Norwegian). Last visited: 17.03.2021.

[GLB15] Ingrid Graffer, Maria B. Line, and Karin Bernsmed. Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations. In *Norsk Informasjonssikkerhetskonferanse 2015*, June 2015.

[GNB$^+$06] Tim Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good. *NIST SP 800-84 Guide to Test, Training and Exercise Programs for IT Plans and Capabilities.* National Institute of Standards and Technology (NIST), September 2006.

[GOV15] GOV.UK. Emergency planning and preparedness: exercises and training. Available online at https://www.gov.uk/guidance/emergency-planning-and-preparedness-exercises-and-training, November 2015. Last visited: 16.03.2021.

[HHT$^+$17] Janne Hagen, Ola Hermansen, Øyvind Toftegård, Jon-Martin Pettersen, Roger Steen, and Synnøve Lill Paulen. Regulering av IKT-sikkerhet. Technical Report 26, Norges vassdrags- og energidirektorat (NVE), March 2017. (In Norwegian).

[HT13] Cathrine Hove and Marte Tårnes. Information Security Incident Management: An Empirical Study of Current Practice. Master's thesis, The Norwegian University of Science and Technology, 2013.

[HTLB14] Cathrine Hove, Marte Tårnes, Maria B. Line, and Karin Bernsmed. Information security incident management: Identified practice in large organizations. In *Eighth International Conference on IT Security Incident Management and IT Forensics 2014*, volume 1, pages 27–46, 2014.

[Int16] International Organization for Standardization (ISO). NEK ISO/IEC 27035-1:2016. Technical report, Norsk Elektroteknisk Komité, 2016.

[Int18] International Organization for Standardization (ISO). NEK ISO/IEC 27000:2018. Technical report, Norsk Elektroteknisk Komité, 2018.

[iS17] i SCOOP. Industry 4.0: the fourth industrial revolution – guide to Industrie 4.0. Available online at https://www.i-scoop.eu/industry-4-0/, 2017. Last visited: 27.01.2021.

[iS19] i SCOOP. Smart grids: what is a smart electrical grid – electricity networks in evolution. Available online at https://www.i-scoop.eu/industry-4-0/smart-grids-electrical-grid/, 2019. Last visited: 27.01.2021.

[Kab16] Yasin Kabalci. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews*, 57:302–318, 2016.

[KL18] Elisabeth Kirkebø and Mathias Ljøsne. IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen. Technical Report 90, Norges vassdrags- og energidirektorat (NVE), October 2018. (In Norwegian).

[Kra11] Patrick Kral. *Incident Handler's Handbook*. SANS Institute, December 2011.

[Lar15] Ann-Kristin Larsen. Øvelser - en veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen. Technical Report 39, Norges vassdrags- og energidirektorat (NVE), May 2015. (In Norwegian).

[LM15] Maria B. Line and Nils Brede Moe. Understanding collaborative challenges in IT security preparedness exercises. In *IFIP International Information Security and Privacy Conference*, pages 311–324, 2015.

[Log17] LogRhythm Labs. NotPetya technical analysis. Technical report, 2017.

[LTC12] LTC Marco De Falco. Stuxnet Facts Report: A technical and strategic analysis. Technical report, NATO Cooperative Cyber Defence Centre of Excellence, 2012.

[LTJ11] Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun. Cyber security challenges in smart grids. *IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2, 2011.

[LTJ14] Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun. Information security incident management: Planning for failure. In *Eighth International Conference on IT Security Incident Management & IT Forensics 2014*, volume 1, pages 47–61, 2014.

[LTJ16] Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun. Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations. In *International Journal of Critical Infrastructure Protection*, volume 12, pages 12–26, 2016.

[Mar20] Maria Bartnes. beredskapsøvelse (IT). Available online at https://snl.no/beredskaps\T1\ovelse_-_IT, December 2020. (In Norwegian). Last visited: 16.02.2021.

[MHS20] Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña. *Qualitative Data Analysis: A Methods Sourcebook.* SAGE publications, 4th edition, 2020.

[MJV17] Glenn Murray, Michael N. Johnstone, and Craig Valli. The convergence of IT and OT in critical infrastructure. In *The Proceedings of 15th Australian Information Security Management Conference*, pages 149–155, 2017.

[Nas17] Nasjonal Sikkerhetsmyndighet (NSM). *Sikkerhetsfaglige anbefalinger for tjenesteutsetting*, 1.1 edition, December 2017. (In Norwegian).

[Nas20] Nasjonal Sikkerhetsmyndighet (NSM). *NSMs Grunnprinsipper for IKT-sikkerhet*, 2.0 edition, April 2020. (In Norwegian).

[Nas21] Nasjonal Sikkerhetsmyndighet (NSM). Risiko 2021. Technical report, March 2021. (In Norwegian).

[Nil14] Rannveig Baaserud Nilsen. Øvelse Østlandet 2013: Evalueringsrapport. Technical Report 49, Norges vassdrags- og energidirektorat (NVE), 2014. (In Norwegian).

[Nor16] Norges vassdrags- og energidirektorat (NVE). Smart metering (AMS). Available online at https://www.nve.no/norwegian-energy-regulatory-authority/retail-market/smart-metering-ams/, May 2016. Last visited: 08.02.2021.

[Nor19] Energy Facts Norway. A MODERN AND DIGITAL POWER SUPPLY SYSTEM. Available online at https://energifaktanorge.no/en/norsk-energibruk/ny-teknologi-i-kraftsystemet/, 2019. Last visited: 02.02.2021.

[Nor20] Norges vassdrags- og energidirektorat (NVE). Sammendrag av nøkkeltallene for nettselskapene. Available online at https://www.nve.no/media/11301/sammendrag.pdf, December 2020. (In Norwegian). Last visited: 08.02.2021.

[Olj12] Olje- og energidepartementet. Meld. St. 14 (2011–2012) Vi bygger Norge – om utbygging av strømnettet. Available online at https://www.regjeringen.no/no/dokumenter/meld-st-14-20112012/id673807/?ch=2, March 2012. (In Norwegian).

[Olj16] Olje- og energidepartementet. Meld. St. 25 (2015–2016) Kraft til endring – Energipolitikken mot 2030. Available online at https://www.regjeringen.no/no/dokumenter/meld.-st.-25-20152016/id2482952/?ch=1, April 2016. (In Norwegian).

[Olj19] Olje- og energidepartementet. Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften). Available online at https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157, January 2019. (In Norwegian).

[oM20] Commonwealth of Massachusetts. Emergency Preparedness Exercises and Training. Available online at https://www.mass.gov/emergency-preparedness-exercises-and-training, 2020. Last visited: 10.02.2021.

[Ran19] Dr Richard Randel. Exercise PowerPlay: Post Exercise Report. Technical report, June 2019.

[Rik21] Riksrevisjonen. Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen, March 2021. Document 3:7 (2020–2021). (In Norwegian).

[RM16] Colin Robson and Kieran McCartan. *Real World Research.* John Wiley & Sons Ltd, 4th edition, 2016.

[Rob16] Robert M. Lee and Michael J. Assante and Tim Conway. Analysis of the cyber attack on the ukrainian power grid. Technical report, SANS and E-ISAC, 2016.

[SKP$^+$17] Lars Erik Smevold, Øystein Korum, Eirik Pettersen, Øystein Hop, Jan-Ivar Andreassen, Olav Vikøren, Solgun Furnes, Ståle Risem-Johansen, Maria Rodahl Johansen, Kåre Flatland, Bente Hoff, Janne Hagen, Jon Martin Storm, and Namrah Azam. Informasjonssikkerhetstilstanden i energiforsyningen. Technical Report 90, Norges vassdrags- og energidirektorat (NVE), December 2017. (In Norwegian).

[Ste19] Steve Livingston and Suzanna Sanborn and Andrew Slaughter and Paul Zonneveld. Managing cyber risk in the electric power sector. Technical report, Deloitte, 2019.

[Sym18] Symantec. Executive Summary: 2018 Internet Security Threat Report. Technical report, Symantec, March 2018. (Volume 23).

[Sym19] Symantec. Executive Summary: 2019 Internet Security Threat Report. Technical report, Symantec, February 2019. (Volume 24).

[Tjo17] Aksel Tjora. *Kvalitative forskningsmetoder i praksis.* Gyldendal Akademisk, 2017. (In Norwegian).

[Wue14] Candid Wueest. Targeted Attacks Against the Energy Sector. White paper, Symantec, January 2014. (Version 1.0).

Appendix A Scenarios

Here follows the created scenarios. In *A.1 Collection of Scenarios*, all of the scenario descriptions are gathered in one document. In addition, the individual scenarios with corresponding discussion questions are included in document A.2 - A.8. All documents are written in both Norwegian and English.

A.1 Collection of Scenarios

A.2 Ransomware

A.3 Attack on SCADA System

A.4 Attack on AMI

A.5 Disclosure of Power Sensitive Information

A.6 Attack on Cloud Services

A.7 Exposed Vulnerable Services

A.8 Defacing of Website

A.1 Collection of Scenarios

Scenariobank

På norsk

Ransomware

Del 1
Angripere har fått tilgang til nettverket til nettselskapet og har muligheten til å bevege seg fritt gjennom dette. Gjennom sin tilgang til nettet, har angriperne beveget seg videre inn i systemene og blant annet fått tilgang til serverplattformer.

Del 2
En lørdag ettermiddag, oppdages det at flere systemer låses og en melding om løsepengekrav dukker opp på skjermene til nettselskapet. Både servere, andre viktige systemer og informasjon er kryptert. Dette gjelder både systemer levert av leverandører og egne systemer.

Etter undersøkelser viser det seg at angripernes vei inn i nettverket var via et phishing angrep mot en ansatt i nettselskapet.

Del 3
I media skrives det om at nettselskapet har blitt utsatt for et cyberangrep. Det spekuleres i at store deler av systemene er satt ut av spill og at det vil få konsekvenser for strømleveransen. Bekymrede kunder ringer inn for å høre om dette vil påvirke deres strømtilførsel.

Angrep på SCADA systemet

Del 1
Kunder ringer inn til nettselskapet og varsler om at det er strømbrudd i et område. Det er første juledag og kundene er midt i julefeiringen. Vakthavende foretar sjekk av kommunikasjon og kjører diagnose på SCADA: Ingen alarm om at noe er feil har gått, og alt på skjermene viser normal drift. For å undersøke nærmere, sender vakthavende på driftssentralen ut en operatør til området det gjelder. Operatøren oppdager at det er et stort område som er uten strøm og melder fra om dette.

Del 2
En time senere ringer flere kunder og forteller om at det er strømløst i andre områder, til tross for at det fremdeles ikke har gått noen alarmer for unormal aktivitet på driftssentralen. Dere mistenker at noe må være galt, og vurderer både massiv system- eller

kommunikasjonsfeil og skadelig programvare i SCADA-systemet som mulige årsaker. Vakthavende får ikke lenger tilgang til systemet, men ser på skjermene at det er aktivitet. Beredskapsleder blir nå koblet inn i hendelsen, og det vurderes å sette beredskap. Leverandør av SCADA-systemet må kobles inn for å foreta en total-diagnose av systemet.

Del 3

Media har nå kastet seg over nyheten og rapporterer som store strømbrudd som forstyrrer julefreden. Mange kunder er fortvilet og stresset for at 1. juledags-middagen ryker. Media krever en uttalelse fra nettselskapet.

Angrep på AMI

Del 1

Nettselskapet har smarte digitale strømmålere installert hos alle sine kunder. Disse strømmålerne er levert av en bestemt leverandør, som har ansvar for både maskin- og programvaren. *Head-end systemet* er lokalisert **[on-prem hos nettselskapet/i cloudservices]** og er også levert av samme leverandør. Både nettselskapet og leverandøren har tilgang til bryterfunksjonaliteten i strømmålerne.

En formiddag får ansatte på driftssentralen inn varsler om uregelmessigheter i strømmålingene som sendes inn fra et fåtall kunder. På servicedesken hos nettselskapet får de henvendelser fra kunder på spredte lokasjoner som har opplevd at strømmen har blitt borte. Ved forsøk på å fikse det kommer det bare opp en feilmelding i systemet. Det tas kontakt med operasjonsansvarlig for å spørre om hva som burde gjøres.

Del 2

Noen dager senere slås strømmen av hos ⅓ av kundene og angriperne går ut i media og annonserer at de har kommet seg inn i sentralsystemet til nettselskapet (head-end systemet) og installert malware på alle strømmålerne deres. Dette gir de fjerntilgang til alle bryterne, og de krever en stor sum penger for å ikke slå av de resterende strømmålerne.

Det oppdages at angripernes vei inn i nettverket har vært via brukerinformasjonen til en ansatt (social engineering eller utro tjener).

Del 3

NRK melder nå at det har skjedd et hackerangrep mot nettselskapet og dere ringes ned av fortvilte kunder som har mistet strømtilførselen. Det spekuleres også i at bakgrunnen for angrepet er at en ansatt **[i nettselskapet/hos leverandøren]** har blitt utsatt for sosial manipulasjon.

Kraftsensitive opplysninger på avveie

Del 1

Nettselskapet kontaktes av KraftCERT som informerer om at kraftsensitiv informasjon fra selskapet har blitt publisert i et hackerforum. Foreløpig skal det kun være snakk om noen få dokumenter.

Del 2

Informasjonen som er lekket er informasjon om SCADA-systemene til nettselskapet som er driftet av en ekstern leverandør. Det er derfor uvisst om det er leverandøren eller nettselskapet sine servere som er angrepet.

Det oppdages det at det har vært noe unormal trafikk ut av nettverket til **[leverandøren/nettselskapet]** mot internett i løpet av de to foregående nettene, men at det ikke har vært nok til at overvåkningssystemene har slått ut. Personen på vakt tilkaller ytterligere driftspersonell og ber leverandøren om å undersøke nærmere. I tillegg til de dokumentene som er publisert er det flere dokumenter som har blitt sendt ut av nettverket, men det vanskelig å finne ut hvilke dokumenter det er snakk om. Dere må finne ut hvilke dokumenter som er på avveie og sørge for at angriperne ikke har mulighet til å stjele flere kraftsensitive dokumenter.

Del 3

For å hindre at hackerne fortsetter å ha tilgang til nettverket og servere med sensitiv informasjon kreves det en resetting av en del systemer.

Angrep på skytjenester

Del 1

Nettselskapet benytter seg av skytjenester for enkelte av sine systemer, både interne og eksterne ut mot kunde, og er avhengige av stabilt internett fra ISP for at disse skytjenestene fungerer som de skal.

En dag etter lunsj får de ansatte i nettselskapet opp en feilmelding i systemene og oppdager at internettforbindelsen er borte. Dermed kommer de seg ikke inn i viktige systemer som er satt ut i skyen. De får derfor ikke gjort arbeidsoppgavene sine, og varsler IT-avdelingen om situasjonen.

Del 2

Ved å inspirere loggen ser dere at det er et uvanlig høyt antall innkommende forespørsler som konsumerer hele kapasiteten i nettverket til nettselskapet. Et distribuert tjenestenektangrep (DDoS) har gjort mange av systemene som kjører på skytjenester utilgjengelige.

Del 3

Hvis ikke snakket om: Trafikken fra angriperne strømmer stadig inn og systemene har nå allerede vært nede i flere timer, det er derfor viktig at dere får gjenopprettet internettforbindelsen.

Eksponerte sårbare tjenester

Del 1

Ved en penetrasjonstest oppdages det at et av systemene til nettselskapet som **[leveres/driftes]** av en leverandør benytter seg av en sårbar tjeneste som er eksponert ut mot omverdenen. Systemet har vært sårbart over en lengre periode, og det er ikke godt å si om det har blitt utnyttet av noen eller ikke. Dette systemet inneholder sensitiv informasjon som potensielt kan ha blitt stjålet av angripere, dersom nettselskapet har vært et mål for et angrep som har utnyttet denne sårbarheten.

Del 2

Dere finner ingen tegn på at sårbarheten faktisk har blitt utnyttet i et angrep mot nettselskapet. Det er allikevel nødvendig å sørge for at sårbarheten ikke kan utnyttes i senere tid. Det er viktig å være klar over at en slik sårbarhet også kan fungere som en inngang inn i selskapet for videre kompromittering.

Defacing av nettside

Del 1

De ansatte i servicedesken kommer på jobb som vanlig på mandag morgen. En kunde ringer inn og forteller om at han/hun har reagert på noe merkelig informasjon som ligger på forsiden av nettsiden til nettselskapet. Når vakthavende går inn og sjekker, ser han at forsiden er endret til å vise “Hvorfor burde du boikotte selskaper som **[Nettselskapet]** som bidrar til vindkraftutbygging i Norge?”. Nettsiden driftes **[delvis/fullstendig]** av en ekstern leverandør.

Del 2

Det oppdages at miljøaktivister har hacket nettsidene til nettselskapet og endret informasjonen på forsiden. Hackerne har i tillegg lagt inn sperrer som hindrer nettselskapet i å endre informasjonen. Flere og flere kunder ringer inn om den merkelige forsiden. **[Nettsiden leveres og driftes av en ekstern leverandør/Deler av infrastrukturen til nettsiden leveres og driftes av en ekstern leverandør]**, og nettselskapet ser seg nødt i å kontakte leverandøren og spørre om hjelp.

Collection of Scenarios

In English

Ransomware

Part 1

The attackers have gained access to the DSO's network and can move freely through it. Through their access to the network, the attackers have moved further into the systems and, among other things, gained access to server platforms.

Part 2

A Saturday afternoon, it is discovered that several systems are being locked, and a message with a ransom demand appears on the DSO's screens. Servers, other important systems and information have been encrypted, and both systems delivered by suppliers and the DSO's systems have been affected.

After investigating, it is uncovered that the attackers' path into the network was via a phishing attack against an employee of the DSO.

Part 3

The media is reporting that the DSO has been subjected to a cyber attack. It is speculated that large parts of the systems have been compromised and that it will have consequences for the power supply. Concerned customers are calling in to check whether this will affect them.

Attack on SCADA System

Part 1

Customers are calling the DSO and reporting that there is an outage. It is Christmas Day, and the customers are in the middle of the holiday celebrations. The operator in charge at the operations center checks the communication and runs a diagnostic of SCADA: No alarm of an error has gone off, and the screens are reporting normal operations. To investigate further, an operator is dispatched to the area in question. The operator discovers that a large area is without power and reports this to the operations center.

Part 2

An hour later, more customers call in and report of outages in other areas, despite the fact that there are still no alarms regarding abnormal activity at the operations center. You suspect that something must be wrong, and consider both massive system- or communications failure and malware in the SCADA systems as possible causes. The operator in charge can no longer access the system, but can see that there is activity on the screens. The preparedness coordinator is now informed of the situation, and it is considered to declare it an emergency. The supplier of the SCADA system needs to be contacted and perform a thorough diagnostic of the entire system.

Part 3

The media is now all over the incident and reports of major outages that disrupt the celebrations. A great number of customers are concerned that the festivities will be cancelled. The media is demanding that the DSO make a statement.

Attack on AMI

Part 1

The DSO has digital smart meters installed at all their customers’ homes. The meters are supplied by a specific supplier responsible for both the hardware and the software. The head-end system is located **[on-prem at the DSO/ in the cloud]** and is provided by the same supplier. Both the DSO and the supplier have access to the switch (relay) functionality in the electricity meters.

One morning, the employees at the operations center are alerted about irregularities in the electricity readings that are received from several customers. At the service desk, they are receiving calls from customers in scattered locations who have lost power. When trying to fix this, an error message appears in the system. The operation manager is contacted to ask what should be done.

Part 2

A few days later the power is turned off for ⅓ of the customers, and the attackers have contacted the media to announce that they have entered the central part of the DSOs system (head-end system) and installed malware in all the DSOs’ smart meters. This gives remote access to all the switches in the meters, and they demand a large sum of money not to turn off the remaining smart meters.

It is discovered that the attackers' way into the network has been through the use of one employee's credentials (social engineering or insider).

Part 3

The media is now reporting a cyber attack against the DSO, and you are receiving calls from desperate customers who have lost their power. It is speculated that the cause of the attack is that an employee **[of the DSO/of the supplier]** has been subjected to a social engineering attack.

Disclosure of Power Sensitive Information

Part 1
The DSO is contacted by KraftCERT, which has discovered that sensitive power system information about the company has been published on a hacker forum. At this point, only a few documents have been disclosed.

Part 2
The information that is leaked is about the DSO’s SCADA systems which are operated by an external supplier. Therefore, it is unknown whether it is the supplier or the DSOs servers that have been attacked.

It is discovered that there has been some abnormal traffic going out to the internet from the **[suppliers/DSOs]** network the last two nights, but the surveillance systems have not detected it. The person on duty calls for additional operational personnel and asks the supplier to investigate. In addition to the documents already published, more documents have been sent out of the network, but it is difficult to identify which documents. You must figure out which documents have been stolen and make sure that the attackers cannot steal more sensitive power system documents.

Part 3
To prevent the attackers from continuing to have access to the network and servers with sensitive power system information a reset of several systems is required.

Attack on Cloud Services

Part 1
The DSO is making use of cloud services for some of their systems, both internal and external related to customers, and is dependent on a stable internet connection from their ISP for the cloud services to work as intended.

One day after lunch, some employees at the DSO come across an error message in the systems and discover that the internet connection is offline. Consequently, they are not able to access important systems that are located in the cloud, nor able to do their tasks. They alert the IT department about the situation.

Part 2
By inspecting the logs, it is discovered that an unusually high amount of incoming requests is consuming the entire capacity of the DSOs network. A distributed denial-of-service attack (DDoS) has made many of your systems running in the cloud unavailable.

Part 3
If not already covered: The traffic from the attackers is constantly flowing in and the systems have been unavailable for several hours. Therefore, it is important that you reinstate the internet connection.

Exposed Vulnerable Services

Part 1

During a penetration test, it is discovered that one of the DSO' systems, which is **[delivered/operated]** by a supplier, uses a vulnerable service that is exposed to the outside world. The system has been vulnerable over a longer period of time, and it is not clear whether an adversary has exploited it. Since the system contains sensitive information, this could potentially have been stolen by attackers if the DSO has been the target of an attack that exploits this vulnerability.

Part 2

You find no evidence that the vulnerable service has been exploited in an attack against the DSO. However, it is still necessary to remove the vulnerability from the system to ensure that attackers cannot exploit it in the future. It is important to consider that such a vulnerability could be used by attackers as a gateway into the DSO's systems to compromise other systems in the future.

Defacing of Website

Part 1

The employees at the service desk arrive at work as usual on Monday morning. A customer calls in and explains that he/she has reacted to some strange information on the front page of the DSOs website. When one of the employees goes in and checks, he sees the front page has been changed to show "Why should you boycott companies like **[DSO]** that contribute to wind power development in Norway?". The website is **[partly/entirely]** operated by an external supplier.

Part 2

After some investigation, it is discovered that environmental activists or "hacktivists" have hacked the DSO's website and changed the information on the front page. The hackers have also added hindrances that prevent the DSO from changing the information. More and more customers are calling in about the strange front page. **[The website is delivered and operated by an external supplier / Parts of the infrastructure for the website are delivered and operated by an external supplier]**, and the DSO finds itself forced to contact the supplier and ask for help.

A.2 Ransomware

Ransomware

På norsk

Det er med vilje utelatt en del detaljer (for eksempel hvordan varsling foregår: via telefon, via e-post, via egen meldingstjeneste, osv.) i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere hvordan det gjøres hos dere under en øvelse for at alle skal bli klar over hva som er prosedyrene.

Ved bruk i en øvelse så kan det også spesifiseres nærmere hvilke(t) system som er rammet. Eksempler er: KIS, NIS, ERP, DMS, etc.

Bakgrunnsteppe og innledende scenario

Angripere har fått tilgang til nettverket til nettselskapet og har muligheten til å bevege seg fritt gjennom dette. Gjennom sin tilgang til nettet, har angriperne beveget seg videre inn i systemene og blant annet fått tilgang til serverplattformer.

Q: Hvilke veier kan angripere ha benyttet inn i systemene?

Q: Hvordan kunne det blitt oppdaget at uvedkommende har fått tilgang til systemene? Av hvem?

> Q: Hva kan hver enkelt part være i stand til å oppdage og hvordan ville de blitt varslet?

Scenario Del 2

Scenario del 2.1

En lørdag ettermiddag, oppdages det at flere systemer låses og en melding om løsepengekrav dukker opp på skjermene til nettselskapet. Både servere, andre viktige systemer og informasjon er kryptert. Dette gjelder både systemer levert av leverandører og egne systemer.

Q: For de 3 viktigste systemene og aktiva dere har: Diskuter hvor kritisk det er hvis dette blir rammet og hva konsekvensene av denne hendelsen ville være.

> Q: Har dere en plan for å operere uten disse systemene for å opprettholde driften?
>
> Q: Hva om hendelsen varer over et lengre tidsrom (1 uke, 1 måned, 3 måned, osv.)?

Q: Hva har dere av backup og redundans?

Q: Har det blitt gjort en vurdering av hvilke systemer som skal prioriteres gjenopprettet først i en slik situasjon?

Q: Hvilken intern informasjon er dere avhengig av? Finnes det backup av dette?

Q: Hvilken ekstern informasjon er dere avhengig av? Finnes det backup av dette?

Q: Hvordan gjenoppretter dere fra backup? Hvor lang tid vil gjenopprettingen ta før de ulike systemene er operative igjen?

Q: Hvordan ville dere gått frem for å finne ut hvor langt tilbake i backupene dere må gå for å finne en uinfisert versjon av systemet (om mulig)?

Q: Har har dere trent på gjenoppretting i praksis? Hvordan?

Q: Hvordan ville dere kommunisert internt i organisasjonen? Med ledelsen, med ansatte?

Q: Har dere policy for håndtering av utpressingsforsøk?

Q: Hvem har myndighet til å avgjøre om det skal utbetales løsepenger?

Q: Hvem må involveres for å håndtere denne situasjonen?

Q: Hvordan blir disse kontaktet?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: Hvilken del av beredskapsplanene vil slå inn i dette tilfellet?

Q: Hva er prosedyrene for håndtering av mistet tilgang til systemer og nettet?

Q: Hvordan foregår kommunikasjonen dere imellom, når nettverket er nede?

Q: Er det inngått avtaler med leverandør(er) som sikrer bistand i en slik situasjon?

Q: Hvem vil dere varsle om denne hendelsen og når?

Scenario del 2.2

Etter undersøkelser viser det seg at angripernes vei inn i nettverket var via et phishing angrep mot en ansatt i nettselskapet.

Q: Hvilke prosedyrer har dere for å beskytte mot denne typen angrep? Hos leverandørene også.

Scenario Del 3

I media skrives det om at nettselskapet har blitt utsatt for et cyberangrep. Det spekuleres i at store deler av systemene er satt ut av spill og at det vil få konsekvenser for strømleveransen. Bekymrede kunder ringer inn for å høre om dette vil påvirke deres strømtilførsel.

Q: Hvordan ville dere håndtere kommunikasjon med eksterne aktører, slik som media og kunder?

Q: Hvem har ansvar for dette?

Q: Hvilken informasjon ville dere gått ut med offentlig?

Ransomware

In English

In some parts of the scenario, details have been left out on purpose (for example, how alerting is done: via phone, via e-mail, via message service, etc.). This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

When the scenario is used in an exercise, it can also be specified in more detail which system(s) is affected. Examples are: CIS, NIS, ERP, DMS, etc.

Background and initial incidents

The attackers have gained access to the DSO's network and can move freely through it. Through their access to the network, the attackers have moved further into the systems and, among other things, gained access to server platforms.

Q: Which paths could the attacks have taken into the systems?

Q: How could it be discovered that unauthorized persons have gained access to the systems? By whom?

> Q: What can each of you (DSO, supplier) be able to discover, and how would you be notified?

Scenario part 2

Scenario part 2.1

A Saturday afternoon, it is discovered that several systems are being locked, and a message with a ransom demand appears on the DSO's screens. Servers, other important systems and information have been encrypted, and both systems delivered by suppliers and the DSO's systems have been affected.

Q: For the three most important systems and assets that you have: Discuss how critical it would be if this system is affected and what the consequences of that would be.

> Q: Do you have a plan for how you would maintain operation without these systems?
> Q: What if the incident spans over a longer period (a week, a month, three months, etc.)?
> Q: Do you have backups of your systems and sufficient redundancy?

Q: Has an assessment been made of which systems should be prioritized restored first in such a situation?

> Q: What internal information are you dependent on? Do you have a backup of that?

Q: What external information are you dependent on? Do you have a backup of that?

Q: How do you recover from backup? How long will the recovery take before the various systems are operational again?

Q: How would you determine how far back in your backups you have to go to ensure that you have an uninfected version (if possible)?

Q: Have you trained on recovery of systems in practice? How?

Q: How would you communicate internally in the organization? With the management, with the employees?

Q: Do you have a policy for handling extortion attempts?

Q: Who has the authority to decide whether to pay a ransom?

Q: Who needs to be involved in handling this incident?

Q: How will they be contacted?

Q: Who is responsible for what? What are the necessary roles to be filled in this case?

Q: What part of your contingency plans will apply in this case?

Q: What are the procedures for dealing with lost access to systems and the network?

Q: How will you communicate when the network is down?

Q: Do you have any agreements with the supplier(s) to ensure assistance in such a situation?

Q: Who will you notify about this incident and when?

Scenario part 2.2

After investigating, it is uncovered that the attackers' path into the network was via a phishing attack against an employee of the DSO.

Q: Which procedures do you have to protect against this type of attack? At the suppliers as well.

Scenario part 3

The media is reporting that the DSO has been subjected to a cyber attack. It is speculated that large parts of the systems have been compromised and that it will have consequences for the power supply. Concerned customers are calling in to check whether this will affect them.

Q: How would you handle the communication with external parties, such as the media and customers?

Q: Who would be responsible for this?

Q: What information would you give to the public?

A.3 Attack on SCADA System

Angrep på SCADA systemet

På norsk

Det er med vilje utelatt en del detaljer (for eksempel hvordan varsling foregår: via telefon, via e-post, via egen meldingstjeneste, osv.) i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere hvordan det gjøres hos dere under en øvelse for at alle skal bli klar over hva som er prosedyrene.

Bakgrunnsteppe og innledende scenario

Kunder ringer inn til nettselskapet og varsler om at det er strømbrudd i et område. Det er første juledag og kundene er midt i julefeiringen. Vakthavende foretar sjekk av kommunikasjon og kjører diagnose på SCADA: Ingen alarm om at noe er feil har gått, og alt på skjermene viser normal drift. For å undersøke nærmere, sender vakthavende på driftssentralen ut en operatør til området det gjelder. Operatøren oppdager at det er et stort område som er uten strøm og melder fra om dette.

Q: Hvilke vurderinger bør vakthavende gjøre basert på situasjonen?

Q: Hvem burde informeres om denne hendelsen/avviket? Hvilken informasjon har de behov for?

Q: Hvilke aktiviteter burde eventuelt bli satt i gang for å finne årsaken til at det tydeligvis vises feil status på skjermene?

Q: Er det noen beredskapsmessige tiltak dere ville igangsatt? I så fall hvilke?

Scenario del 2

En time senere ringer flere kunder og forteller om at det er strømløst i andre områder, til tross for at det fremdeles ikke har gått noen alarmer for unormal aktivitet på driftssentralen. Dere mistenker at noe må være galt, og vurderer både massiv system- eller kommunikasjonsfeil og skadelig programvare i SCADA-systemet som mulige årsaker. Vakthavende får ikke lenger tilgang til systemet, men ser på skjermene at det er aktivitet. Beredskapsleder blir nå koblet inn i hendelsen, og det vurderes å sette beredskap. Leverandør av SCADA-systemet må kobles inn for å foreta en total-diagnose av systemet.

Q: Hva er førsteprioritet, å få tilbake strømmen eller å redde systemet?

Q: Hvordan ville dere gått frem for å avgjøre hva som er årsaken til systemfeilen?

Q: Hvem vil måtte hentes inn på jobb og involveres?

Q: Hvem vil dere varsle om denne hendelsen og når?

Q: Hvem vil man be om assistanse fra?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: Hvordan vil kommunikasjonen foregå, hvordan påvirkes dette av at folk har fri fra jobb?

Q: Hvilke konsekvenser vil denne hendelsen ha for virksomheten?

Q: Hva bør iverksettes av tiltak?

Scenario del 3

Media har nå kastet seg over nyheten og rapporterer som store strømbrudd som forstyrrer julefreden. Mange kunder er fortvilet og stresset for at 1. juledags-middagen ryker. Media krever en uttalelse fra nettselskapet.

Q: Hvem ville fått ansvar for å håndtere eksterne aktører, slik som media og kunder?
    Q: Dersom denne personen er utilgjengelig, hvem ville da fått ansvaret?

Q: Hvordan ville dere gått frem for å informere samfunnet?

Q: Hva ville dere informert om i en uttalelse?
    Q: Hvordan ville dere kvalitetssikret talepunktene?

Attack on SCADA System

In English

In some parts of the scenario, details have been left out on purpose (for example, how alerting is done: via phone, via e-mail, via message service, etc.). This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

Background and initial incidents

Customers are calling the DSO and reporting that there is an outage. It is Christmas Day, and the customers are in the middle of the holiday celebrations. The operator in charge at the operations center checks the communication and runs a diagnostic of SCADA: No alarm of an error has gone off, and the screens are reporting normal operations. To investigate further, an operator is dispatched to the area in question. The operator discovers that a large area is without power and reports this to the operations center.

Q: What assessments should the operator in charge do based on the situation?

Q: Who should be informed about this incident? What information should they be given?

Q: What activities should be initiated to uncover why the screens are displaying the wrong status?

Q: Would you initiate any countermeasures based on this information? If so, which measures?

Scenario part 2

An hour later, more customers call in and report of outages in other areas, despite the fact that there are still no alarms regarding abnormal activity at the operations center. You suspect that something must be wrong, and consider both massive system- or communications failure and malware in the SCADA systems as possible causes. The operator in charge can no longer access the system, but can see that there is activity on the screens. The preparedness coordinator is now informed of the situation, and it is considered to declare it an emergency. The supplier of the SCADA system needs to be contacted and perform a thorough diagnostic of the entire system.

Q: What would be prioritized, to regain power or to salvage the system?

Q: How would you proceed to uncover the cause of the system error?

Q: Who would have to be called into work?

Q: Who would you notify of this incident and when?

Q: Who would you ask for assistance?

Q: Who is responsible for what? What are the necessary roles to be filled in this case?

Q: How will you communicate? Is this affected by the fact that several employees have the day off?

Q: What consequences would this incident have for the organization?

Q: What countermeasures should be implemented?

Scenario part 3

The media is now all over the incident and reports of major outages that disrupt the celebrations. A great number of customers are concerned that the festivities will be cancelled. The media is demanding that the DSO make a statement.

Q: Who would be responsible for handling external parties, such as the media and customers?

> Q: In the case that this person is unavailable, who would then be in charge?

Q: How would you proceed to inform the public?

Q: What information would you give in a statement?

> Q: How would you assure the quality of the talking points?

A.4 Attack on AMI

Angrep på AMI

På norsk

Det er med vilje utelatt en del detaljer (for eksempel hvordan varsling foregår: via telefon, via e-post, via egen meldingstjeneste, osv.) i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere under øvelsen hvordan det gjøres hos dere for at alle skal bli klar over hva som er prosedyrene.

Bakgrunnsteppe og innledende scenario

Nettselskapet har smarte digitale strømmålere installert hos alle sine kunder. Disse strømmålerne er levert av en bestemt leverandør, som har ansvar for både maskin- og programvaren. *Head-end systemet* er lokalisert **[on-prem hos nettselskapet/i cloudservices]** og er også levert av samme leverandør. Både nettselskapet og leverandøren har tilgang til bryterfunksjonaliteten i strømmålerne.

En formiddag får ansatte på driftssentralen inn varsler om uregelmessigheter i strømmålingene som sendes inn fra et fåtall kunder. På servicedesken hos nettselskapet får de henvendelser fra kunder på spredte lokasjoner som har opplevd at strømmen har blitt borte. Ved forsøk på å fikse det kommer det bare opp en feilmelding i systemet. Det tas kontakt med operasjonsansvarlig for å spørre om hva som burde gjøres.

Q: Hva kan dette indikere? Hva ville dere mistenkt?

Q: Hvordan ville organisasjonen gått frem for å finne årsaken til disse hendelsene?

Q: Hvem ville måtte bli involvert for å finne ut av dette?

Scenario del 2

Scenario del 2.1

Noen dager senere slås strømmen av hos ⅓ av kundene og angriperne går ut i media og annonserer at de har kommet seg inn i sentralsystemet til nettselskapet (head-end systemet) og installert malware på alle strømmålerne deres. Dette gir de fjerntilgang til alle bryterne, og de krever en stor sum penger for å ikke slå av de resterende strømmålerne.

Q: Hvilke konsekvenser ville dette angrepet fått?

Q: Har dere en policy for håndtering av utpressingsforsøk?

Q: Hvem har myndighet til å avgjøre om det skal utbetales løsepenger?

Q: Hvilke deler av beredskapsplanene deres og prosedyrene deres for hendelseshåndtering ville slått inn ved dette scenariet?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: Hvordan ville dere gått frem for å få kontakt med alle som må involveres?

Q: Hvordan ville dere gått frem for å løse dette problemet? Hva ville dere hatt behov for av hjelp fra leverandørene av sentralsystemet?

Q: Hva finnes av backup og redundans?

Q: Har dere mulighet til å gjenopprette fra backup? Hvor lang tid vil gjenopprettingen ta før de ulike systemene er operative igjen?

Q: Har har dere i praksis trent på gjenoppretting? Hvordan?

Q: Har leverandøren behov for å involvere ytterligere underleverandører for å håndtere situasjonen?

Q: Hvem vil dere varsle om denne hendelsen og når?

Scenario del 2.2

Det oppdages at angripernes vei inn i nettverket har vært via brukerinformasjonen til en ansatt (social engineering eller utro tjener).

Q: Hvilke prosedyrer har dere for å forhindre dette, både hos egne ansatte og hos leverandører som leverer kritisk infrastruktur til dere?

Scenario del 3

NRK melder nå at det har skjedd et hackerangrep mot nettselskapet og dere ringes ned av fortvilte kunder som har mistet strømtilførselen. Det spekuleres også i at bakgrunnen for angrepet er at en ansatt **[i nettselskapet/hos leverandøren]** har blitt utsatt for sosial manipulasjon.

Q: Hva er prosedyrene for håndtering av eksterne aktører ved en hendelse?

Q: Hvem ville hatt ansvar for å håndtere media?

Q: Hvordan ville dere gått frem for å informere eksterne aktører, slik som media og kunder? Hva ville dere informert om?

Attack on AMI

In English

In some parts of the scenario, details have been left out on purpose (for example, how alerting is done: via phone, via e-mail, via message service, etc.). This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

Background and initial incidents

The DSO has digital smart meters installed at all their customers' homes. The meters are supplied by a specific supplier responsible for both the hardware and the software. The head-end system is located **[on-prem at the DSO/ in the cloud]** and is provided by the same supplier. Both the DSO and the supplier have access to the switch (relay) functionality in the electricity meters.

One morning, the employees at the operations center are alerted about irregularities in the electricity readings that are received from several customers. At the service desk, they are receiving calls from customers in scattered locations who have lost power. When trying to fix this, an error message appears in the system. The operation manager is contacted to ask what should be done.

Q: What can this indicate? What would you suspect?

Q: How would the organization proceed to find the cause of these incidents?

Q: Who would have to get involved to find out?

Scenario part 2

Scenario part 2.1

A few days later the power is turned off for ⅓ of the customers, and the attackers have contacted the media to announce that they have entered the central part of the DSOs system (head-end system) and installed malware in all the DSOs' smart meters. This gives remote access to all the switches in the meters, and they demand a large sum of money not to turn off the remaining smart meters.

Q: What consequences would this attack have?

Q: Do you have a policy for handling extortion attempts?

Q: Who has the authority to decide whether to pay a ransom?

Q: What parts of your contingency plans and incident management procedures would apply in this scenario?

Q: Who is responsible for what? What are their roles?

Q: How would you go about contacting everyone involved?

Q: How would you proceed to solve this problem? What assistance would it require from the suppliers?

Q: Do you have backups of your systems and sufficient redundancy?

Q: Do you have the ability to recover from backup? How long will the recovery take before the various systems are operational again?

> Q: Have you trained on recovery of systems in practice? How?

Q: Does the supplier need to involve additional subcontractors to handle the situation?

Q: Who will you notify about this incident and when?

Scenario del 2.2

It is discovered that the attackers' way into the network has been through the use of one employee's credentials (social engineering or insider).

Q: Which procedures do you have in place to prevent this, both regarding your own employees and the employees at the suppliers who provide critical infrastructure to you?

Scenario part 3

The media is now reporting a cyber attack against the DSO, and you are receiving calls from desperate customers who have lost their power. It is speculated that the cause of the attack is that an employee **[of the DSO/of the supplier]** has been subjected to a social engineering attack.

Q: Which procedures do you have for the management of external parties (the media, customers, etc.) during an incident?

Q: Who would be responsible for handling the media?

Q: How would you go about informing the external parties, such as the media and customers? What information would you give to the public?

A.5 Disclosure of Sensitive Power System Information

Kraftsensitive opplysninger på avveie

På norsk

Det er med vilje utelatt en del detaljer (for eksempel hvordan varsling foregår: via telefon, via e-post, via egen meldingstjeneste, osv.) i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere under øvelsen hvordan det gjøres hos dere for at alle skal bli klar over hva som er prosedyrene.

Bakgrunnsteppe og innledende scenario

Nettselskapet kontaktes av KraftCERT som informerer om at kraftsensitiv informasjon fra selskapet har blitt publisert i et hackerforum. Foreløpig skal det kun være snakk om noen få dokumenter.

Q: Hvilke konsekvenser kan dette få?

Q: Hvordan ville dere gått frem for å undersøke hva som har skjedd?

Q: Vil dette innebære en beredskapssituasjon for virksomheten? Hvis ikke - hvilke eskalerende faktorer skal til for at det blir det?

Scenario del 2

Scenario del 2.1

Informasjonen som er lekket er informasjon om SCADA-systemene til nettselskapet som er driftet av en ekstern leverandør. Det er derfor uvisst om det er leverandøren eller nettselskapet sine servere som er angrepet.

Q: Har dere en beredskapsplan som vil benyttes i dette tilfellet?

Q. Hvem må involveres?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: På hvilke lokasjoner er kraftsensitiv informasjon lagret?

Q: Hvordan vil dere gå frem for å undersøke hvor dokumentene er stjålet fra?

Q: Hvordan vil koordineringen mellom dere foregå?

Scenario del 2.2

Det oppdages det at det har vært noe unormal trafikk ut av nettverket til **[leverandøren/nettselskapet]** mot internett i løpet av de to foregående nettene, men at det ikke har vært nok til at overvåkningssystemene har slått ut. Personen på vakt tilkaller ytterligere driftspersonell og ber leverandøren om å undersøke nærmere. I tillegg til de dokumentene som er publisert er det flere dokumenter som har blitt sendt ut av nettverket, men det vanskelig å finne ut hvilke dokumenter det er snakk om. Dere må finne ut hvilke dokumenter som er på avveie og sørge for at angriperne ikke har mulighet til å stjele flere kraftsensitive dokumenter.

Q: Hvordan vil dere gå frem for å håndtere denne situasjonen? Hvem har ansvaret?

Q: Hva har det å si for dere hva slags type informasjon som har blitt lekket? For eksempel beredskapsplaner, ROS-analyser, informasjon om SCADA-systemet eller annen type sensitiv informasjon.

Q: Hva vil dette ha å si for hvordan dere håndterer situasjonen?

Q: Hvilke konsekvenser kan dette få?

Q: Hvem vil dere varsle om denne hendelsen og når?

Scenario del 3

For å hindre at hackerne fortsetter å ha tilgang til nettverket og servere med sensitiv informasjon kreves det en resetting av en del systemer.

Q: Hvem må involveres for å få til dette?

Q: Hva er viktig å tenke på? Hvilke tiltak må iverksettes?

Disclosure of Sensitive Power System Information

In English

In some parts of the scenario, details have been left out on purpose (for example, how alerting is done: via phone, via e-mail, via message service, etc.). This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

Background and initial incidents

The DSO is contacted by KraftCERT, which has discovered that sensitive power system information about the company has been published on a hacker forum. At this point, only a few documents have been disclosed.

Q: What consequences could this have?

Q: How would you proceed to investigate what has happened?

Q: Will this constitute an emergency situation for the company? If not - which escalating factors are necessary to make it one?

Scenario part 2

Scenario part 2.1

The information that is leaked is about the DSO's SCADA systems which is operated by an external supplier. Therefore, it is unknown whether it is the supplier or the DSOs servers that have been attacked.

Q: Do you have a contingency plan that would be used in this case?

Q. Who must be involved?

Q: Who is responsible for what? What are their roles?

Q: In which locations are sensitive power system information stored?

Q: How would you proceed to investigate where the documents have been stolen from?

Q: How will the coordination between the DSO and the supplier take place?

Scenario part 2.2

It is discovered that there has been some abnormal traffic going out to the internet from the **[suppliers/DSOs]** network the last two nights, but the surveillance systems have not detected it. The person on duty calls for additional operational personnel and asks the supplier to investigate. In addition to the documents already published, more documents have been sent out of the network, but it is difficult to identify which documents. You must figure out which documents have been stolen and make sure that the attackers cannot steal more sensitive power system documents.

Q: How will you proceed to handle the situation? Who is in charge?

Q: What impact does what type of information that has been leaked have? Example contingency plans, risk analyzes, information about the SCADA system or other types of sensitive information.

Q: How will this impact how you handle the situation?

Q: What consequences may this have?

Q: Who would you alert about this incident and when?

Scenario part 3

To prevent the attackers from continuing to have access to the network and servers with sensitive power system information a reset of several systems is required.

Q: Who must be involved to achieve this?

Q: What is important to keep in mind? Which measures must be implemented?

A.6 Attack on Cloud Services

Angrep på skytjenester

På norsk

Det er med vilje utelatt en del detaljer (for eksempel hvordan varsling foregår: via telefon, via e-post, via egen meldingstjeneste, osv.) i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere hvordan det gjøres hos dere under en øvelse for at alle skal bli klar over hva som er prosedyrene.

Bakgrunnsteppe og innledende scenario

Nettselskapet benytter seg av skytjenester for enkelte av sine systemer, både interne og eksterne ut mot kunde, og er avhengige av stabilt internett fra ISP for at disse skytjenestene fungerer som de skal.

En dag etter lunsj får de ansatte i nettselskapet opp en feilmelding i systemene og oppdager at internettforbindelsen er borte. Dermed kommer de seg ikke inn i viktige systemer som er satt ut i skyen. De får derfor ikke gjort arbeidsoppgavene sine, og varsler IT-avdelingen om situasjonen.

Q: Hva kan dette indikere?

Q: Hvilke vurderinger burde vakthavende gjøre basert på situasjonen?

Q: Hvilke aktiviteter burde igangsettes for å finne ut hva som er årsaken til dette?

Q: Hvem tar dere kontakt med?

Scenario del 2

Ved å inspirere loggen ser dere at det er et uvanlig høyt antall innkommende forespørsler som konsumerer hele kapasiteten i nettverket til nettselskapet. Et distribuert tjenestenektangrep (DDoS) har gjort mange av systemene som kjører på skytjenester utilgjengelige.

Q: Hvem har kompetanse og mulighet til å inspisere loggene og oppdage denne hendelsen?

Q: Basert på hvilke systemer dere har ute i skyen, hva ville vært konsekvensene av at disse systemene er utilgjengelige?

Q: Hvem må involveres for å løse opp i dette?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: Hvilke avtaler har dere som angår angrep på disse tjenestene?

Q: Er det noen beredskapsmessige tiltak dere ville igangsatt? I så fall hvilke?

Q: Hvem vil dere varsle om denne hendelsen og når?

Scenario del 3

Hvis ikke snakket om: Trafikken fra angriperne strømmer stadig inn og systemene har nå allerede vært nede i flere timer, det er derfor viktig at dere får gjenopprettet internettforbindelsen.

Q: Hvordan ville dere gått frem for å gjenopprette internettforbindelsen?

I tillegg ønsker ledelsen ønsker at det skal ses på tiltak for å hindre slike hendelser i fremtiden.

Q: Hvem må involveres i dette arbeidet?

Q: Hvilke typer tiltak ville dere gjennomført?

Attack on Cloud Services

In English

In some parts of the scenario, details have been left out on purpose (for example, how alerting is done: via phone, via e-mail, via message service, etc.). This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

Background and initial incidents

The DSO is making use of cloud services for some of their systems, both internal and external related to customers, and is dependent on a stable internet connection from their ISP for the cloud services to work as intended.

One day after lunch, some employees at the DSO come across an error message in the systems and discover that the internet connection is offline. Consequently, they are not able to access important systems that are located in the cloud, nor able to do their tasks. They alert the IT department about the situation.

Q: What can this indicate?

Q: Which assessments should be done by the operator in charge based on this situation?

Q: Which activities should be initiated to discover the cause of the situation?

Q: Who would you contact?

Scenario part 2

By inspecting the logs, it is discovered that an unusually high amount of incoming requests is consuming the entire capacity of the DSOs network. A distributed denial-of-service attack (DDoS) has made many of your systems running in the cloud unavailable.

Q: Who has the ability and competence to inspect the logs and discover this incident?

Q: Based on which systems you have in the cloud, what would the consequences of this incident be?

Q: Who must be involved to solve the situation?

Q: Who has the responsibility for what? What are their roles?

Q: Which agreements are in place that concerns attacks on these services?

Q: Are there any countermeasures that you would initiate? Which?

Q: Who would you alert about this incident and when?

Scenario part 3

If not already covered: The traffic from the attackers is constantly flowing in and the systems have been unavailable for several hours. Therefore, it is important that you reinstate the internet connection.

Q: How would you proceed to restore the internet connection?

In addition, the management wishes that an investigation into countermeasures that can prevent these incidents in the future should be conducted.

Q: Who should/must be involved in this work?

Q: Which countermeasures would you implement?

A.7 Exposed Vulnerable Services

Eksponerte sårbare tjenester

På norsk

Det er med vilje utelatt en del detaljer i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere hvordan det gjøres hos dere under en øvelse for at alle skal bli klar over hva som er prosedyrene.

Scenario del 1

Ved bruk i en øvelse så kan det spesifiseres nærmere hvilket system som er rammet. Eksempler er: KIS, NIS, ERP, osv. Det kan også spesifiseres om det er kraftsensitiv informasjon eller personopplysninger som finnes i det sårbare systemet.

Ved en penetrasjonstest oppdages det at et av systemene til nettselskapet som **[leveres/driftes]** av en leverandør benytter seg av en sårbar tjeneste som er eksponert ut mot omverdenen. Systemet har vært sårbart over en lengre periode, og det er ikke godt å si om det har blitt utnyttet av noen eller ikke. Dette systemet inneholder sensitiv informasjon som potensielt kan ha blitt stjålet av angripere, dersom nettselskapet har vært et mål for et angrep som har utnyttet denne sårbarheten.

Q: Hva innebærer hendelsen for virksomheten? Hvilken skade kan hendelsen potensielt medføre?

Q: Energiloven og kraftberedskapsforskriften stiller krav til taushetsplikt og beskyttelse av kraftsensitiv informasjon, ville dette vært et regelbrudd?

Q: Hva slags type informasjon kan ha kommet på avveie?

Q: Hvem ville dere varslet om dette og når? Hvilke varslingskrav har dere?

Q: Hvordan ville dere gått frem for å undersøke om systemet er kompromittert?

Q: Hvem ville måtte blitt involvert i dette scenariet?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Scenario del 2

Dere finner ingen tegn på at sårbarheten faktisk har blitt utnyttet i et angrep mot nettselskapet. Det er allikevel nødvendig å sørge for at sårbarheten ikke kan utnyttes i senere tid. Det er viktig å være klar over at en slik sårbarhet også kan fungere som en inngang inn i selskapet for videre kompromittering.

Q: Hvordan går dere frem for å gjennomføre dette?

Q: Hvem må involveres?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: Hva bør iverksettes av tiltak?

Exposed Vulnerable Services

In English

In some parts of the scenario, details have been left out on purpose. This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

Scenario part 1

When this scenario is used in an exercise, it can be specified which system(s) is affected by the incident. Examples are: KIS, NIS, ERP, etc. You can also specify whether the vulnerable system contains sensitive power system information or personal data.

During a penetration test, it is discovered that one of the DSO' systems, which is **[delivered/operated]** by a supplier, uses a vulnerable service that is exposed to the outside world. The system has been vulnerable over a longer period of time, and it is not clear whether an adversary has exploited it. Since the system contains sensitive information, this could potentially have been stolen by attackers if the DSO has been the target of an attack that exploits this vulnerability.

Q: What does this incident mean for the organization? What damage can it potentially cause?

Q: The Norwegian Energy Emergency Preparedness regulation contains requirements for confidentiality and protection of sensitive power system information, would this be a violation of the regulation?

Q: What kind of sensitive information could have been disclosed? What are the consequences?

Q: Who would you notify of this incident and when? What requirements of notification do you have?

Q: How would you proceed to investigate whether the system has been compromised?

Q: Who would have to be involved in the management of this incident?

Q: Who is responsible for what? What are their roles?

Scenario part 2

You find no evidence that the vulnerable service has been exploited in an attack against the DSO. However, it is still necessary to remove the vulnerability from the system to ensure that attackers cannot exploit it in the future. It is important to consider that such a vulnerability could be used by attackers as a gateway into the DSO’s systems to compromise other systems in the future.

Q: How would you proceed to remove the vulnerability and secure the systems again?

Q: Who needs to be involved?

Q: Who is responsible for what? What are their roles?

Q: What measures should be implemented?

A.8 Defacing of Website

Defacing av nettside

På norsk

Det er med vilje utelatt en del detaljer i scenariet. Dette er for at dere enten kan gjøre små justeringer og tilpasninger for å gjøre scenariet mer passende for dere eller at dere kan diskutere hvordan det gjøres hos dere under en øvelse for at alle skal bli klar over hva som er prosedyrene.

Bakgrunnsteppe og innledende scenario

De ansatte i servicedesken kommer på jobb som vanlig på mandag morgen. En kunde ringer inn og forteller om at han/hun har reagert på noe merkelig informasjon som ligger på forsiden av nettsiden til nettselskapet. Når vakthavende går inn og sjekker, ser han at forsiden er endret til å vise "Hvorfor burde du boikotte selskaper som **[Nettselskapet]** som bidrar til vindkraftutbygging i Norge?". Nettsiden driftes **[delvis/fullstendig]** av en ekstern leverandør.

Q: Hva innebærer hendelsen for virksomheten?

Q: Hvilken skade kan hendelsen potensielt medføre?

Q: Hvordan ville dere gått frem for å finne ut årsaken til endringen og hvem som har gjort det?

Scenario del 2

Det oppdages at miljøaktivister har hacket nettsidene til nettselskapet og endret informasjonen på forsiden. Hackerne har i tillegg lagt inn sperrer som hindrer nettselskapet i å endre informasjonen. Flere og flere kunder ringer inn om den merkelige forsiden. **[Nettsiden leveres og driftes av en ekstern leverandør/Deler av infrastrukturen til nettsiden leveres og driftes av en ekstern leverandør]**, og nettselskapet ser seg nødt i å kontakte leverandøren og spørre om hjelp.

Q: Hvilke beredskapsplaner har dere som dekker hendelser som dette?

Q: Hvordan vil kommunikasjonen med leverandøren av nettsiden foregå?

Q: Hvem har ansvar for hva? Hva er rollefordelingen?

Q: Hva bør iverksettes av tiltak?

Defacing of Website

In English

In some parts of the scenario, details have been left out on purpose. This is done so that you either can make small adaptations or customizations to make the scenario more suitable for your organization or so you can discuss how this would have been done in your organization during the exercise so all participants become aware of this.

Background and initial incidents

The employees at the service desk arrive at work as usual on Monday morning. A customer calls in and explains that he/she has reacted to some strange information on the front page of the DSOs website. When one of the employees goes in and checks, he sees the front page has been changed to show "Why should you boycott companies like **[DSO]** that contribute to wind power development in Norway?". The website is **[partly/entirely]** operated by an external supplier.

Q: What does this incident mean for the organization?

Q: What damage can this incident potentially cause?

Q: How would you go about finding out the reason for the change and who did it?

Scenario part 2

After some investigation, it is discovered that environmental activists or “hacktivists” have hacked the DSO’s website and changed the information on the front page. The hackers have also added hindrances that prevent the DSO from changing the information. More and more customers are calling in about the strange front page. **[The website is delivered and operated by an external supplier / Parts of the infrastructure for the website are delivered and operated by an external supplier]**, and the DSO finds itself forced to contact the supplier and ask for help.

Q: What contingency plans do you have that covers incidents such as this?

Q: How will the communication with the supplier of the website and web server take place?

Q: Who is responsible for what? What are their roles?

Q: What measures should be implemented?

Appendix B
Exercise Documents

Here follows the documents for the exercise. The first document is a guide that explains how stakeholders can use the scenarios and related discussion questions to design and conduct a discussion exercise. The other documents can function as templates on which documents should be prepared in the event of an exercise and what they should contain. The documents in the appendix are those that were used in the conducted digital exercise, so they contain information for an exercise with *Ransomware* as the scenario.

B.1 How-To Guide for Using the Scenarios

B.2 Briefing

B.3 Facilitator Guide

B.4 Evaluation Scheme

B.5 Participants Guide

B.1 How-To Guide for Using the Scenarios

This guide will explain how stakeholders can use the scenarios and related discussion questions to design and conduct a discussion exercise. The scenarios are designed with the intent to be used in joint exercises with DSOs and suppliers in the electrical energy sector.

The scenarios and discussion questions are created for discussion exercises but can easily be adapted to more resource-demanding exercises such as game-, functional- and full-scale exercises.

Step 0: Determine the exercise staff that will plan and design the discussion exercise and select an exercise facilitator and a data collector.

- The facilitator's responsibility will be to guide the discussion, keep the exercise on track and lead the final evaluation.
- The data collector's responsibility is to collect information and decision points during the exercise and the evaluation to develop a follow-up report.

Step 1: Define the goals and objectives of the exercise based on the focus area(s) of the exercise. It is important to consider what you want to achieve by conducting the exercise. Below you can find examples of goals that can be defined to improve the collaboration with suppliers, which you can use for an exercise:

- Establish relationships and points of contact
- Test all parties' knowledge of plans and contact points, and establish a common understanding of plans, roles and responsibilities during an incident
- Establish effective communication and enhanced information sharing practices
    - internally and/or externally
- Develop protective measures and countermeasures
- Identify organizational gaps
- Identifying potential points of improvement for the coordination and the plans

Step 2: Choose the scenario from the collection of scenarios you want to use in the exercise. Here it is important to have the focus area(s) of the exercise in mind and select the scenario that will enable you to test this.

- If necessary, make adjustments to customize the scenario to better fit your organization and your intent.

Step 3: Based on the exercise's selected goals, the exercise staff should also adjust the discussion questions for the scenario. Take a look at the scenarios' corresponding examples of discussion questions, select the ones that fit your focus area(s) and adapt the others to better fit your goals and objectives.

Step 4: Invite the participants. It is essential that the right people from both the DSO and the supplier are present at the exercise. Here, it may be helpful to consider who would have to be involved in the incident management if the described incident in the scenario were to happen.

- It is important to invite the participant well in advance to ensure that they can participate.
- It is beneficial if someone from the supplier can assist in the design and planning of the exercise to increase their received value from the exercise.

Step 5: Create and prepare the other exercise documents:

- *Briefing*: An informative document distributed to the participants in advance of the exercise. It includes an agenda, the goals and objectives of the exercise, the scenario, information about the participants, and other logistics information.
- *Facilitator guide*: A handbook to the exercise facilitator on how to guide the discussion exercise. It should contain the goals and objectives of the exercise, the selected scenario supplemented with additional information and definitions of used terms and phrases, and additional discussion questions to keep the discussion on track.
- *Evaluation scheme*:
  - Oral first impression evaluation: Reflection questions directly after the exercise to discuss the first impressions of the participants regarding the organization, implementation and value of the exercise.
  - Questionnaire: A structured form that the participants answer individually after the exercise.
- *Participant guide*: Slides or a document that the participants will use during the exercise. This will contain the agenda of the exercise, repeat the goals and objectives of the exercise, and present the phases of the scenario and related discussion questions sequentially.

B.2 Briefing

Discussion exercise: Challenging ICT-attack, Ransomware

Time and place

Time: 10:00 - 14:00, Thursday 15th of April
Place: Digitally via Teams

Duration

3-4 hours, included evaluation

Exercise type

Discussion exercise

General scenario

Ransomware

Participants

DSO:

- CEO
- CFO
- ICT security coordinator
- Preparedness coordinator and quality- and innovation manager
- Division manager for utility customers
- Operations center manager
- …

Supplier 1:

- ICT security manager
- …

Supplier 2:

- ICT security manager
- …

Exercise goals

Improve the collaboration between the DSO and the suppliers during incident management through:

- establishing relationships and points of contact
- testing all parties' knowledge of plans and contact points, and estab-lishing a common understanding of plans, roles and responsibilities during an incident

- identifying potentials points of improvement for the coordination and the plans
- mapping the risk and consequence of such and incident and the DSOs and suppliers ability to handle the situation

Exercise objectives

- Roles and responsibilities
- Coordination and cooperation
- Routines for alerting

Exercise management and other central roles

Discussion leader:
Evaluator:
Recorders:

Preparations and implementation

- Read through relevant material for IT incident management: Contingency plans, contact lists, agreements etc.
- The exercise will be based on a scenario which is divided into 3 parts: Background and initial scenario, main part, wrap-up.

Speaker queue

We will use a form of speaker queue, by using the "Raise hand"-function in Teams if it is necessary. This means that "Raise hand" should be used if you wish to say something in a discussion where someone else is speaking and there are more people that wish to speak. However, if no one is speaking it is fine to grab/take the word without raising your hand first.

In the case where one wants to ask a clarifying question you may write "Question" in the chat, and this will be prioritized in the queue.

To avoid background noise all the participants should normally mute themselves when they are not speaking.

Evaluation and follow-up

- Immediately after the exercise it is allocated time for a joint "first-impression" evaluation. Therefore you are encouraged to take some notes during the exercise if you notice something that is working well or you see something that is missing. The evaluation is included in the time estimate (3-4 hours). This will be the responsibility of the evaluator.
- There will also be issued an individual questionnaire to all the participants the following day to make a more structured evaluation of both the organization and the implementation of the exercise.

To gain the most from the exercise it is important to identify points of improvement by evaluating how the exercise went, and write a report that summarizes these points. It is also necessary to make sure that these points of improvements are paid attention to and that the changes are implemented.

Other relevant information

- Have something to take notes with and on available
- Turn on your camera (unless you have a slow internet connection, then it may help to turn off the camera)

B.3 Facilitator Guide

The role and responsibilities of the exercise facilitator:

The exercise facilitators's main task during the exercise is to lead the discussion.

In order to achieve as good a discussion as possible, the discussion facilitator should strive to [1]:

- *See to that all parties is given time to speak*
- *Consider rules, like a speaker queue instead of a free discussion*
- *Be structured, objective, calm, clear, and attentive to the participants wishes*
- *Assess which discussions that is valuable and should continue, and which should be terminated*
- *Assist the data collector during the exercise so that the evaluation report becomes complete and reflects what was said during the exercise*

Tasks:

- Welcome the participants and give a short introduction
  - Explain how the exercise will be conducted
  - Present the rules for the speaker queue
  - Other relevant information/rules the participants should be aware of
- Present/repeat the goals of the exercise
- Present the different parts of the scenario and the corresponding discussion questions
- Guide the discussion and make sure that it stays on topic

About the scenario

This is an example of what an exercise facilitator guide can look like. The following section should contain relevant background information to the given scenario, describing how the attack might have occurred, similar incidents that have happened in real life, explanations of concepts or systems in the scenario, etc.

In this scenario the attackers have gained access to the DSO’s network, and further gained access to the databases and servers. The compromise of IT systems is becoming increasingly common for Norwegian organizations.

There are different ways the attackers could have gained access to the systems. One option is scanning against open sources (OSINT – open source intelligence) (E.g. IP-addresses) to find ways into the systems. Another is social engineering attacks such as stealing credentials from employees or tricking employees into downloading viruses from attachments, software, etc.

Attackers might attempt to compromise an organization's infrastructure to gain access to data and information or to simply gain a foothold in the organization's systems. Often attackers are hiding their presence in the system for a long time, before they reveal themselves by performing actions that are detected. The time in hiding is used to lock the grip on the computer system, and to gain additional access to gather and steal more information.

The scenario in this discussion exercise is a fictitious ransomware attack and focuses on what would happen in your organization if such an event should occur. A ransomware attack is an attack that encrypts information stored on computers and typically the attackers demand a large sum of money, in bitcoin or another crypto currency, to unlock the information. The virus can infect through the opening of malicious email attachments, downloading unreliable software, trojan horses or false updates. The Norwegian aluminum producer Norsk Hydro was hit by the ransomware LockerGaga combined with an attack against Active Directory (AD), the user and login system, in 2019. During these kinds of attacks, the systems might be unavailable for several weeks depending on the amount and quality of backups, and it can take months before the victims are back to normal operations.

Both the situation in the systems and preliminary consequences are described in the scenario. You should discuss what happens if the situation escalates and which further consequences this may have for your organization.

Aspects that should be discussed during the exercise:

(If these themes are not discussed the exercise facilitator should lead the discussion in this direction)

- Contingency plans
- Communication between the DSO and supplier during incident management
- Roles and responsibilities

Examples of questions to drive the discussion along:

This is an example of how the exercise facilitator guide can be. The following section should contain relevant discussion questions that supplement the discussion questions given to the participants in the exercise. The exercise facilitator might use these questions to steer the discussion in the right direction if they are veering off topic and to drive the exercise along if necessary.

Scenario Part 1

- Is the internal netflow monitored to uncover abnormal activity (information leakage and unintended access)?
- Is it availability, confidentiality or integrity that is most important for the information handling in your organization, or is it a combination?
- Does your organization have contact with a CERT that could assist you in uncovering such incidents?

Scenario Part 2

- What risk assessments has your organization done regarding these types of incidents?

- Do you have contingency plans for these types of incidents?
- Has your organization prepared a strategy or policy for how to deal with these types of incidents?
- Who would you call for assistance in such a situation? Authorities, organizations, etc.
- Are you equally dependent on the security routines of your supplier in this case, as you are on your own security?
- How would you proceed to uncover how long the attackers have had access to your systems, in order to decide how old the backups you use have to be?
- Do you have the required competency to manage to restore the systems based on your backups? Who are you dependent on when it comes to recovery?
- How do you inform your own employees during this type of incident?
- What is important external information for your organizations during these types of incidents?
- What types of internal information in your organizations is vital to keep in such an incident, and how should you manage this?
- How is your information secured (redundancy, local servers, access control systems)
    - Is there any other way you should secure your systems?
- Which national policies concerning information security may impact your organization regarding such an incident?

Scenario Part 3

- Will it be necessary for your organization to have a dialogue with the media in such an incident? Why?

[1]:https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_diskusjonsovelse.pdf

B.4 Evaluation Scheme

Joint Evaluation - First impression evaluation directly after the exercise

This is a short oral review of the immediate experiences after the exercise. It is based on a few predefined questions that focus on the exercise's main goals.

Q1: Would we have been able to handle this incident in a good way?

Q2: What could be improved, and how?

Q3: What are the most important takeaways from this exercise?

Q4: Was it useful to conduct the exercise together with a supplier?

Individual Questionnaire - The following day

Q: Who did you represent during the exercise?

- Supplier
- DSO

The organization of the exercise

The goals

Q: To what extent do you feel that the goals of the exercise matched:

- … who participated in the exercise? *Scale from Very little to Very Much.*
- … how the exercise was conducted? *Scale from Very little to Very Much.*
- … the discussion questions? *Scale from Very little to Very Much.*
- … the scenario? *Scale from Very little to Very Much.*

Q: To what degree do you feel that the goal "Establishing relations and points of contact" was fulfilled?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: To what degree do you feel that the goal "Testing all parties' knowledge of plans and contact points, and establishing a common understanding of plans, roles and responsibilities during an incident" was fulfilled?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: To what degree do you feel that the goal "Identifying potential points of improvement for the coordination and the plans" was fulfilled?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: To what degree do you feel that the goal "Mapping the risk and consequence of such an incident and the DSOs and suppliers ability to handle the situation" was fulfilled?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Participants

Q: To what degree do you feel that the correct participants were present during the exercise?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: Was anyone missing? Why? *Text*

Duration

Q: How well did the actual duration match the allocated time?

- Too much time
- A bit too much time
- Appropriate
- A bit too little time
- Too little time

Q: How well did the distribution of time fit each part? Was there enough time for the evaluation? *Text*

The relevance of the scenario and the discussion questions

Q: To what degree was the scenario relevant for the goals of the exercise?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: To what degree was the scenario relevant for you to practice?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: Do you have any other feedback to the scenario that was used in the exercise? *Text*

Q: To what degree were the discussion questions relevant for the goals of the exercise?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: Were there any discussion points or aspects that you felt were missing during the exercise? *Text*

The digital format

Q: How well did it work to conduct the exercise digitally?

- Very good
- Good
- Average
- Poor
- Very poor

Q: To what degree did you feel that you were able to speak your opinions whenever you wanted to?

- Very high degree
- High degree

- Some degree
- Low degree
- Very low degree

Q: To what degree did you feel that the digital format hindered you from participating in the discussion the way you wanted to?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: To what degree did you feel that the outcome of the exercise was affected by the digital format?

- Very high degree
- High degree
- Some degree
- Low degree
- Very low degree

Q: Can you think of any positive sides by conducting the exercise digitally instead of physically? *Text*

Q: Can you think of any negative sides by conducting the exercise digitally instead of physically *Text*

Generally

If from a DSO: To what extent do you think it was beneficial to include the supplier in this exercise?

- Very much
- Much
- Some
- Little
- Very little

If from a supplier: To what extent do you think it was beneficial for you as a supplier to participate in the exercise?

- Very much
- Much
- Some
- Little
- Very little

What was your most important takeaway from the exercise? *Text*

On a general basis, what do you believe could make it easier to collaborate with suppliers and coordinate during incident management? *Text*

On a general basis, what do you believe could make it easier to conduct exercises together with suppliers? *Text*

Do you have any additional feedback on the implementation of the exercise? *Text*

About the conduction of the exercise

Q: How well were your plans fit to handle this incident? Were the plans suitable and in compliance with the handling?

- Very good
- Good
- Average
- Poor
- Very poor

Q: Were the plans used in an appropriate manner?

- Yes
- No
- Partly
- Other

Q: Were the plans familiar to all the participants?

- Yes
- No
- Partly
- Other

Q: Did you discover any flaws/points of improvement with the plans? In that case what? *Text*

Q: How would the coordination between the different actors that participated in the exercise work during an incident? (DSO and supplier)

- Very good
- Good
- Average
- Poor
- Very poor

Q: What was good/not good?*Text*

Q: What could have improved this? *Text*

Q: How good are your routines for alerting?

- Very good
- Good
- Average
- Poor
- Very poor

Q: How was the discussion during the exercise? (Multiple answers possible)

- Effective
- Thorough
- General
- In an appropriate way
- We reached a common understanding
- We used existing plans
- We included the suppliers to solve the tasks

Q: Is there a clear allocation of responsibilities and roles during these types of incidents?

- Yes
- No
- Partly
- Other

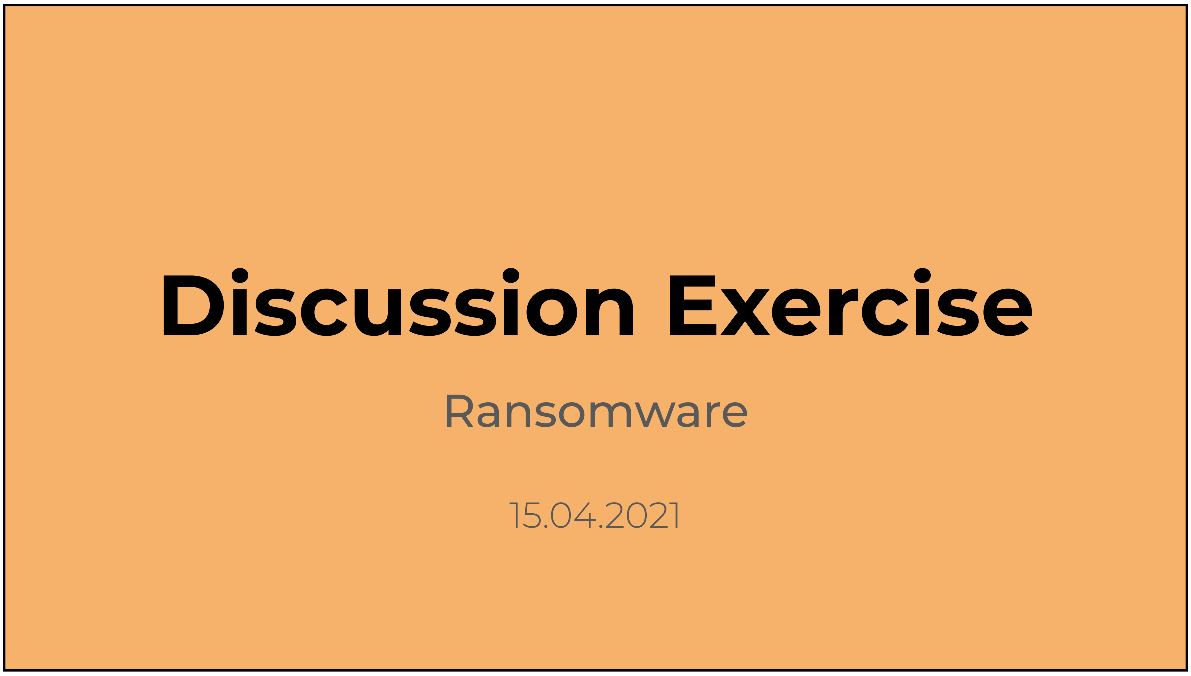
Q: What was your experience of the outcome of the exercise?

- Very good
- Good
- Average
- Poor
- Very poor

Q: Do you have any suggestions for concrete measures to be taken or points of improvement? *Text*

Q: Do you have any suggestions for what it could be useful to practice on the next occasion? Attack scenarios, use of specific plans, etc. *Text*

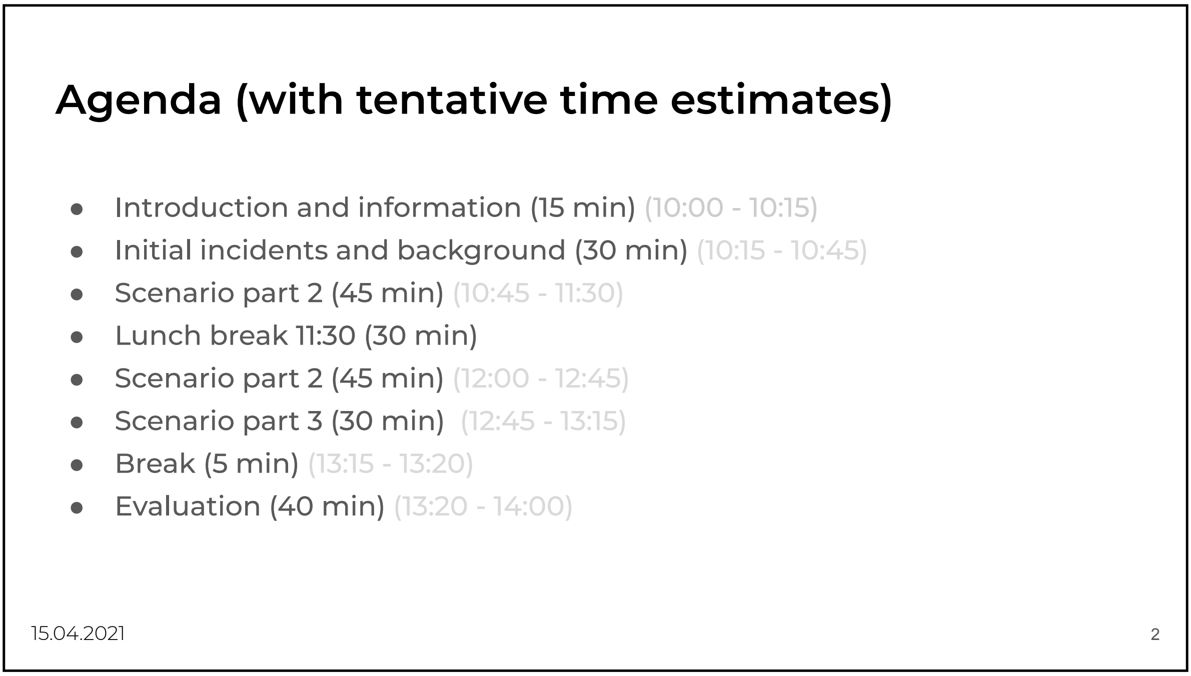
Q: Do you have any other feedback? *Text*



Discussion Exercise

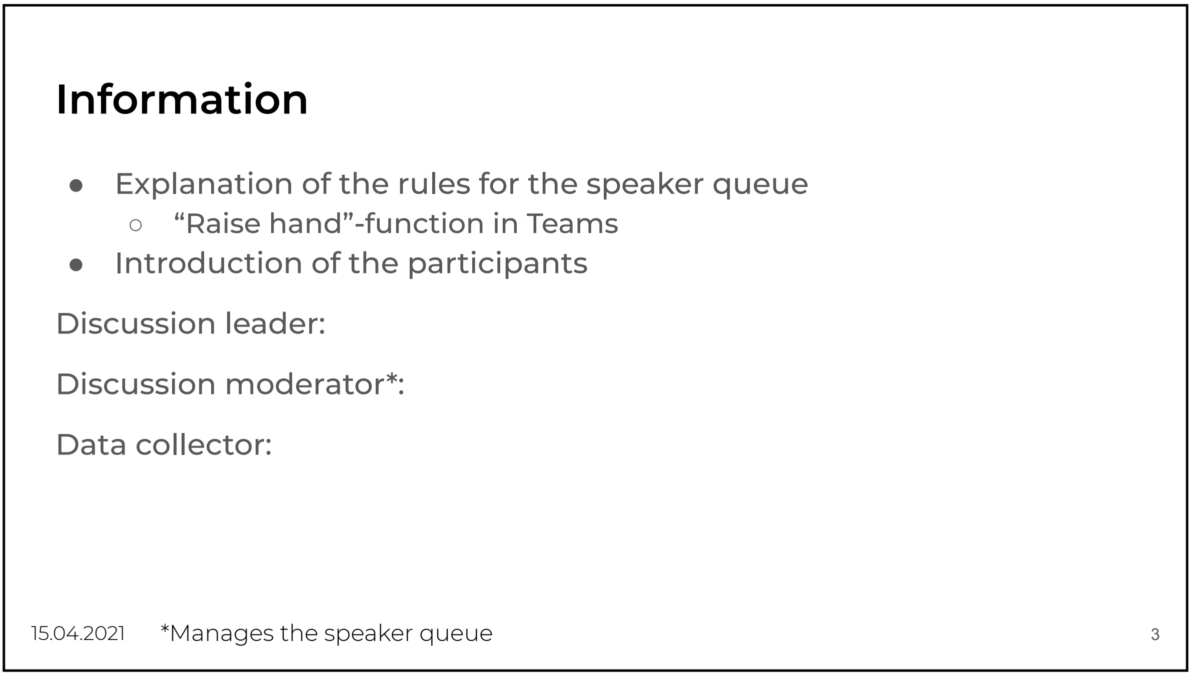
Ransomware

15.04.2021



Agenda (with tentative time estimates)

- Introduction and information (15 min) (10:00 - 10:15)
- Initial incidents and background (30 min) (10:15 - 10:45)
- Scenario part 2 (45 min) (10:45 - 11:30)
- Lunch break 11:30 (30 min)
- Scenario part 2 (45 min) (12:00 - 12:45)
- Scenario part 3 (30 min) (12:45 - 13:15)
- Break (5 min) (13:15 - 13:20)
- Evaluation (40 min) (13:20 - 14:00)



Information

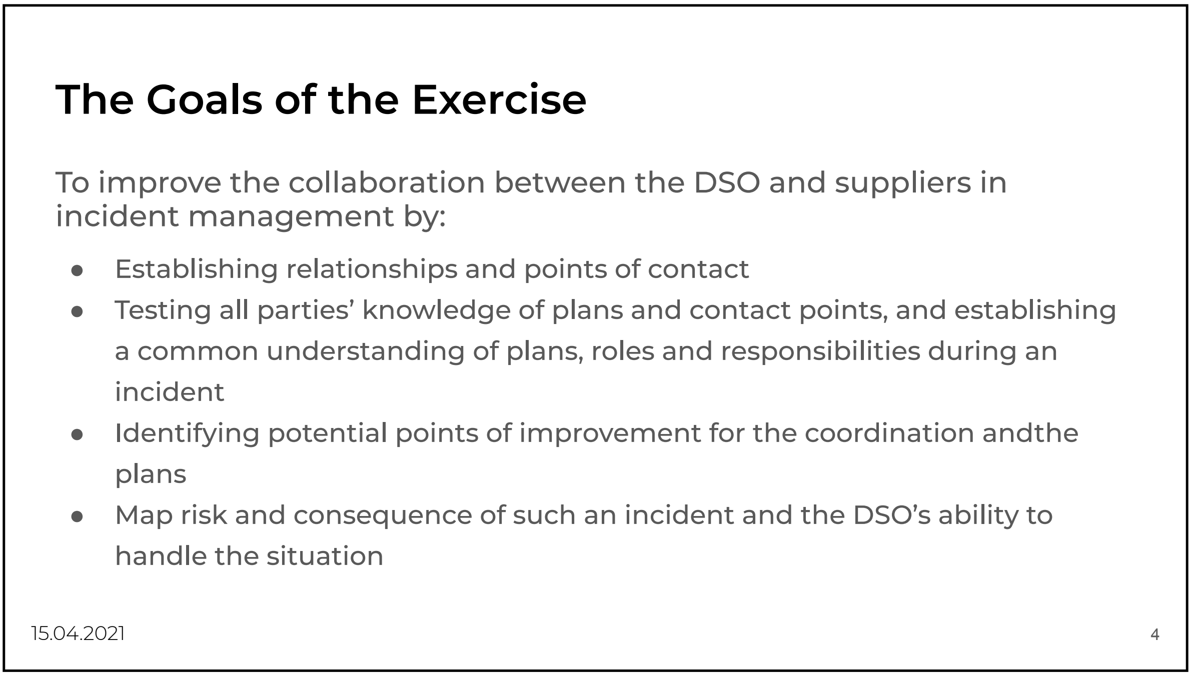
- Explanation of the rules for the speaker queue
    - “Raise hand”-function in Teams
- Introduction of the participants

Discussion leader:

Discussion moderator*:

Data collector:

*Manages the speaker queue



The Goals of the Exercise

To improve the collaboration between the DSO and suppliers in incident management by:

- Establishing relationships and points of contact
- Testing all parties’ knowledge of plans and contact points, and establishing a common understanding of plans, roles and responsibilities during an incident
- Identifying potential points of improvement for the coordination andthe plans
- Map risk and consequence of such an incident and the DSO’s ability to handle the situation

Background and Initial Incidents

The attackers have gained access to the DSO’s network and are able to move freely through it. Through their access to the network, the attackers have moved further into the systems and gained access to server platforms both at Supplier 1 and, our own DMS-servers.

The attackers have gained access to the DSO’s network and are able to move freely through it. Through their access to the network, the attackers have moved further into the systems and gained access to server platforms both at Supplier 1 and, our own DMS-servers.

Q: How could this be discovered? By who?

Q: What can Supplier 1, Supplier 2 and the *DSO* be capable of discovering and how would you be notified?

Scenario Part 2.1

A Saturday afternoon, it is discovered that several systems are being locked and a message with a ransom demand appears on the DSO's screens. Application servers, databases and file servers are encrypted. Both servers at Supplier 1 and our own DMS-servers are hit. CIS, ERP, NIS and DMS is amongst the affected systems. But, SCADA is not affected.

A Saturday afternoon, it is discovered that several systems are being locked and a message with a ransom demand appears on the DSO's screens. Application servers, databases and file servers are encrypted. Both servers at Supplier 1 and our own DMS-servers are hit. CIS, ERP, NIS and DMS is amongst the affected systems. But, SCADA is not affected.

Q: Which are the three most important systems and assets that you have? For each of these

> Q: Discuss how critical it would be if this system is affected and what the consequences of that would be.

Q: Do you have plans and policies for handling extortion attempts?

> Q: Who has the authority to decide whether to pay a ransom?

LUNCH BREAK (30 min)

A Saturday afternoon, it is discovered that several systems are being locked and a message with a ransom demand appears on the DSO’s screens. Application servers, databases and file servers are encrypted. Both servers at Supplier 1 and our own DMS-servers are hit. CIS, ERP, NIS and DMS is amongst the affected systems. But, SCADA is not affected.

- Q: How would this incident be handled?
  - Q: Who must be involved to handle the incident?
  - Q: How are these contacted?
  - Q: Who is responsible for what? What are the necessary roles to be filled?
  - Q: How critical/what are the consequences of administrative systems like IFS and Customer being unavailable?
    - Q: What kind of contingency plans and emergency routines exists to handle this?
  - Q: What are the consequences of DMS and Netbas being unavailable?
  - Q: Do you have a plan to handle this?
    - Q: Which part of your contingency plans will apply in this case?
    - Q: How does the communication between the involved parties take place, if the network is down?
      - Q: Which collaboration does this demand? Who can contribute with what?

A Saturday afternoon, it is discovered that several systems are being locked and a message with a ransom demand appears on the DSO's screens. Application servers, databases and file servers are encrypted. Both servers at Supplier 1 and our own DMS-servers are hit. CIS, ERP, NIS and DMS is amongst the affected systems. But, SCADA is not affected.

Q: Has an assessment been made of which systems should be prioritized restored first in such a situation?

Q: What kind of backup and redundancy do you have?

Q: Do you have any agreements with the supplier(s)that will ensure assistance in such a situation?

Q: Who will you notify about this incident and when?

Scenario Part 2.2

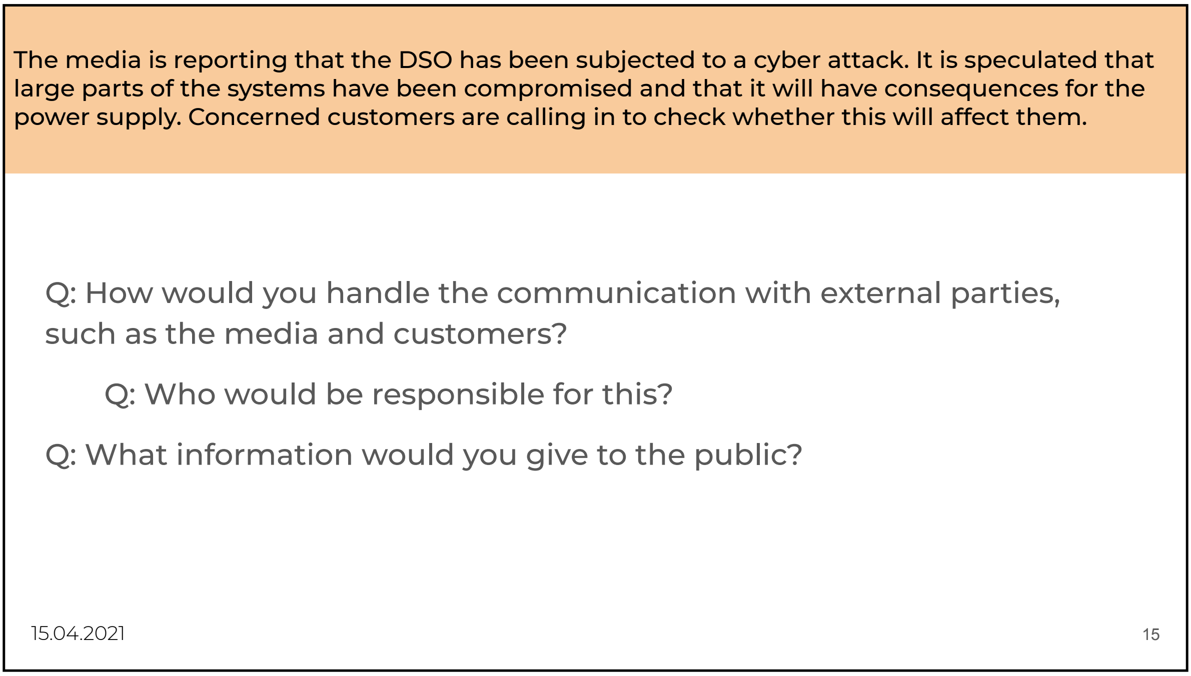
After investigating, it is uncovered that the attackers' path into the network was via a phishing attack against an employee of the organization.

After investigating, it is uncovered that the attackers' path into the network was via a phishing attack against an employee of the organization.

Q: What procedures do you have to protect against this type of attack? At the suppliers as well.

Scenario Part 3

The media is reporting that the DSO has been subjected to a cyber attack. It is speculated that large parts of the systems have been compromised and that it will have consequences for the power supply. Concerned customers are calling in to check whether this will affect them.

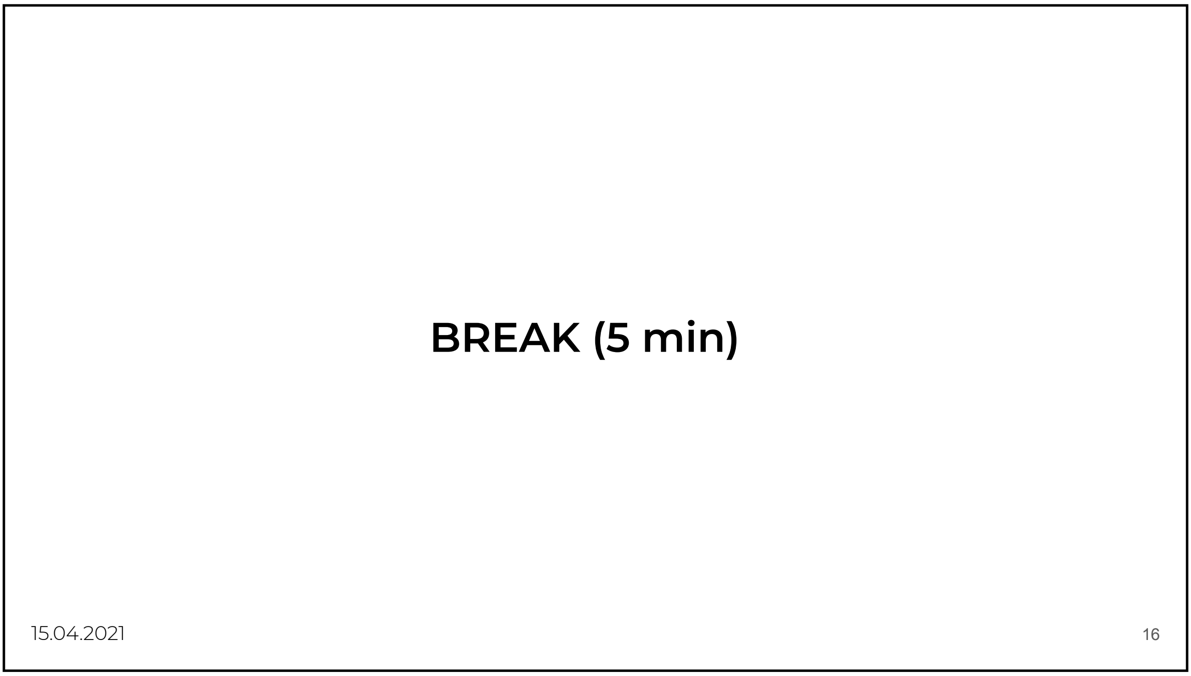


The media is reporting that the DSO has been subjected to a cyber attack. It is speculated that large parts of the systems have been compromised and that it will have consequences for the power supply. Concerned customers are calling in to check whether this will affect them.

Q: How would you handle the communication with external parties, such as the media and customers?

Q: Who would be responsible for this?

Q: What information would you give to the public?



BREAK (5 min)

First Impression Evaluation

Q1: Would we have been able to handle this incident in a good way?

Q2: What could be improved, and how?

Q3: What are the most important takeaways from this exercise?

Q4: Was it useful to conduct the exercise together with a supplier?

Feedback to the exercise

Feedback on ...

- The format
- The exercise staff
- The information given beforehand
- The exercise in general
- etc.

Wrap-up

Thanks for participating!

An individual questionnaire will be sent out by email tomorrow.

Appendix C

Interview Guides

Here follows the interview guides.

C.1 Interview Guide DSO

C.2 Interview Guide Supplier

C.1 Interview Guide DSO

This interview guide was used in the interviews with the DSOs. The intent of the questions were to gain insight into both what the situation is today regarding the collaboration between DSOs and suppliers when it comes to incident management, as well as to gain insight into things that will make it easier for us to make the scenarios as realistic as possible. The interviews were held in Norwegian, so this is the translated interview guide.

Introduction to the interview

Thank you for taking the time to meet with us today and for helping us gain insight into your organization and your industry!

We are both master students at Communication Technology at NTNU in Trondheim, and are taking a specialization within information security. This spring we are writing our master's thesis, which focuses on the collaboration between DSOs and suppliers during incident management in the electrical energy sector in Norway, and how preparedness exercises with relevant scenarios can improve this.

We will start to ask some questions about you and your role, before we will proceed with the following topics:

- *Your suppliers*
- *Incident management and preparedness exercises*
- *Attack scenarios*
- *Closing questions and wrap-up*

We can inform you that we will not record this interview, only take notes. Afterwards, we will send you a draft of the results in our master's thesis when this is ready, so you can read through it and correct any misunderstandings.

Questions

Introduction

- What is your role in the organization?
    - How long have you worked there?
    - What are your areas of responsibility in the organization?

About the organization

- How many customers do you have?
- How many employees do you have?

- To which degree do you believe that your organization is vulnerable to cybersecurity incidents?

Suppliers

- Which suppliers of IT systems and components do you have?
    - How many?
    - What do they deliver?
- Which supplier is the most critical?
- How do you communicate with these suppliers?
- Do you have any agreements or guarantees about how the suppliers should assist you in case of an incident that involves their product/service?
- How much insight do you have into the security of the products delivered by a supplier?
    - Do you check or revise if it corresponds to the demands of the contract?
- How confident are you that the supplier has the capacity to provide the guaranteed resources in case of an incident? If they have contracts with many DSOs and have promised the same resources and aid to everybody, what happens if many DSOs require help at the same time?

Plans and exercises

- Have suppliers been involved in the development of plans and procedures for incident management that involves their products?
    - **If not;** do they have insight into what your plans say?
    - How were the plans developed?
    - When were the plans last revised?
- Which procedures do you have for the contact with suppliers during incident management?
- (How) are suppliers involved in training and exercises today?
    - **If "not much" or not at all;** why not?
    - Are multiple suppliers involved at the same time?
    - How are the plans and procedures used in these exercises?
- Do you think that suppliers should be involved in exercises with DSOs?
    - Which benefits do you see from including suppliers in training and exercises?

- What factors do you think could make it easier to arrange exercises together with some of your suppliers?

In case of an incident

- Who has the responsibility for detecting and reporting incidents?
- Who has the (main) responsibility for making decisions and assessments during an incident?
- Which procedures do you have for evaluating the handling after an incident?
    - Who uses this information and what is it used for?
    - Is suppliers involved in this?

Scenarios

- Can you provide some examples of attack scenarios or incidents that would require involvement of suppliers?
    - Which supplier and service/component is involved?
    - How dependent are you upon the supplier during the incident management in this scenario? What are you dependent on?
    - Which consequences does this have?
    - Who has the (main) responsibility for making decisions and assessments during this incident?
- Does there exist examples of incidents that involve multiple suppliers? In that case, do they cooperate?
- Have you conducted a risk and vulnerability assessment that we could have a look at?

Closing

- Do you have any ideas for factors that could make the collaboration with the suppliers better and easier when it comes to incident management and exercises?
- Would it be OK if we contact you with any follow-up or clarification questions?
- Do you have any other feedback to us?

C.2 Interview Guide Supplier

This interview guide was used in the interviews with the suppliers. The intent of the questions were to gain insight into both what the situation is today regarding the collaboration between DSOs and suppliers when it comes to incident management, as well as to gain insight into things that will make it easier for us to make the scenarios as realistic as possible. The interviews were held in Norwegian, so this is the translated interview guide.

Introduction to the interview

Thank you for taking the time to meet with us today and for helping us gain insight into your organization and your industry!

We are both master students at Communication Technology at NTNU in Trondheim, and are taking a specialization within information security. This spring we are writing our master's thesis, which focuses on the collaboration between DSOs and suppliers during incident management in the electrical energy sector in Norway, and how preparedness exercises with relevant scenarios can improve this.

We will start to ask some questions about you and your role, before we will proceed with the following topics:

- *Incident management and preparedness exercises*
- *Attack scenarios*
- *Your subcontractors*
- *Closing questions and wrap-up*

We can inform you that we will not record this interview, only take notes. Afterwards, we will send you a draft of the results in our master's thesis when this is ready, so you can read through it and correct any misunderstandings.

Questions

Introduction

- What is your role in the organization?
    - How long have you worked there?
    - What are your areas of responsibility in the organization?

About the organization

- How many Norwegian DSOs do you have as customers?
- What type of service or product do you deliver to the DSOs?
- Do you believe that your organization is in danger of a cybersecurity breach?

    - Do you believe that anyone would be interested in targeting your organization as a step in a supply chain attack against Norwegian DSOs?

About exercises and incident management

- Have you been involved in creating plans for incident management with your customers/DSOs?
    - Are you aware of the plans and what they say?
    - Have you ever made your own plans and then handed them over to the customer?
- Do you have an incident management plan in case of incidents in your systems (that affects your customers)?
- Do you have any agreements or contracts with the DSOs that dictates how you must assist during incident response if an attack where your systems are involved occurs?
- What insights do the DSOs have into your cybersecurity level?
    - Do they check if you comply with the cybersecurity requirements stated in the contract?
- How do you communicate with the DSOs? Do you have a dedicated contact person?
    - Is this any different during incidents?
- Are you certain you will be able to provide customers the guaranteed resources when needed? If you have contracts with several DSOs and have promised the same aid to all, what happens if several DSOs need help simultaneously?
- Have you participated in any preparedness exercises or validation of plans for incident management with DSOs?
    - **If not;** why?
    - Do you think suppliers should be included in exercises?
    - Do you feel that your organization would benefit or receive something in return from participating in exercises with the DSOs?
    - Is there a problem participating in exercises with DSOs because there are so many in total?
- Do you conduct cybersecurity exercises on your own?
- What would it take for it to be easier for you to participate in exercises with the DSOs that are your customers?
- What do you think is the supplier’s role during an incident at a DSO?

- Have there been occurrences of incidents at your customers where your systems have been involved?
    - Who discovered the incident?
    - When/how was it alerted?
    - How was the incident handled?
    - Which components were involved in the incident?

Scenarios

We want to create relevant and realistic scenarios that can be used in preparedness exercises. These scenarios will focus on incidents that will require collaboration between the DSO and the suppliers.

- Do you have any examples of attack scenarios that involve the products you supply to DSOs?

Subcontractors

- How many subcontractors do you have?
    - What do they deliver?
- How dependent are you of your subcontractors if an incident should occur?
- Would an incident at one of your customers also require assistance from your subcontractors as well?

Closing

- Do you have any ideas for factors that could make the collaboration with the suppliers better and easier when it comes to incident management and exercises?
- Would it be OK if we contact you with any follow-up or clarification questions?
- Do you have any other feedback to us?

Mari Langås & Sanna Løfqvist

Cybersecurity Preparedness Exercises in Smart Grid: Collaboration With Suppliers During Incident Response

NTNU
Norwegian University of
Science and Technology