With a Little Help from Your Friends: Collaboration with Vendors During Smart Grid Incident Response Exercises

Mari Langås
marilangaass@gmail.com
IIK, NTNU
Trondheim, Norway

Sanna Løfqvist
sannalofqvist@hotmail.com
IIK, NTNU
Trondheim, Norway

Basel Katt
basel.katt@ntnu.no
IIK, NTNU
Gjøvik, Norway

Thomas Haugan
thomas.haugan@ntnu.no
Department of Electric Power Engineering, NTNU
Trondheim, Norway

Martin Gilje Jaatun
martin.g.jaatun@sintef.no
Department of Software Engineering, Safety and Security, SINTEF Digital
Trondheim, Norway

ABSTRACT

The introduction of Information and Communications Technology (ICT) into conventional power grids has resulted in a digitalized smart grid, enabling a more efficient and robust operation. However, it can also lead to increased risk and new threats due to more complex systems and longer supply chains. Recent events indicate that the electrical power grid is an attractive target, promoting the need for well-prepared incident management processes that involve external vendors. This paper 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 vendors in preparedness exercises.

CCS CONCEPTS

• **Security and privacy → Distributed systems security**.

KEYWORDS

Smartgrid, cyber security, incident management, training, vendors

ACM Reference Format:
Mari Langås, Sanna Løfqvist, Basel Katt, Thomas Haugan, and Martin Gilje Jaatun. 2021. With a Little Help from Your Friends: Collaboration with Vendors During Smart Grid Incident Response Exercises . In *European Interdisciplinary Cybersecurity Conference (EICC), November 10–11, 2021, Virtual Event, Romania.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3487405.3487654

1 INTRODUCTION

The electrical power grid is considered one of the most vital critical infrastructures in modern society and almost all societal functions rely on electric power for their operation. Smart grid makes the operation 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 vendors, 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 consequences of attacks [4].

The electrical energy sector is one of the most frequently targeted sectors by cyber attackers [14]. According to the national threat assessment *Risiko 2021* [10], the Norwegian electrical energy infrastructure is at risk from espionage and data breaches from both state actors and criminals. The introduction of smart grid blurs the line between OT and 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.

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 vendors creates a need for close collaboration between all involved parties in the supply chain when an incident occurs, especially the vendors of the affected systems. In a report on the customer and vendor relationships in the electrical energy sector from the NVE [7], they recommend that Norwegian DSOs conduct preparedness exercises with their vendors. However, Eriksen and Gunabala [6] investigated the collaboration of DSOs and their vendors in the management of potential cybersecurity incidents in their Process Control Systems (PCS). According to their findings, vendors are rarely involved in cybersecurity preparedness exercises, even though there is a need for it. Few studies have investigated the challenges [2], as well as potential improvements [3] of information security incident management training. Other reports discussed preparedness exercises conducted in the energy sector [11, 12] and their results. The literature lacks dedicated work focusing on the involvement of vendors together with DSOs, which is the motivation for this project [8].

EICC, November 10–11, 2021, Virtual Event, Romania

ACM ISBN 978-1-4503-9049-1/21/11…$15.00
https://doi.org/10.1145/3487405.3487654

In order to answer this question, this work aims at studying the various factors that are important to consider when including vendors in preparedness exercises. This has been done by conducting interviews with Norwegian DSOs together with their vendors. The vendors in question provided telecommunications services, IT systems, IT and OT systems, and smart grid technology, respectively. Then, the results of these interviews were used to inform the development of a set of incident preparedness scenarios covering seven of the most relevant attacks on the energy sector. One of these scenarios was chosen and a discussion exercise was conducted with one of the interviewed DSOs, which involved the relevant vendors. The conducted discussion exercise was evaluated in two steps, (1) a first-impression evaluation the same day of the exercise, and (2) written evaluation that was conducted after the exercise. We summarise the main contributions of this work as follows:

- Qualitative analysis about the the involvement of vendors in cybersecurity preparedness exercises, together with DSOs
- Development of seven exercise scenarios related to the most relevant cybersecurity attacks in the energy sector
- Qualitative evaluation of conducting one exercise that involves both DSO and its vendors.

The remainder of this paper is structured thus: We provide relevant background in Section 2. In Section 3, we present results from interviews with DSOs and their vendors. In Section 4 we present the scenarios developed, and in Section 5 the exercise that was carried out with a DSO and its vendors is described. Finally, Section 7 concludes the paper.

2 BACKGROUND

Preparedness exercises are usually divided into four types [5, 9]: discussion exercises, game exercises, functional exercises, and full-scale exercises. **Discussion exercises** are often also referred to as tabletop exercises; no physical measures are taken during the exercise, and there should be no contact with non-participants during the exercise. **Game exercises** typically divide the participants into teams based on their role or function, and the teams are physically separated in different rooms or locations. **Functional exercises** require a simulation of some functions that have been identified as essential to manage real events. **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.

3 INTERVIEWS

The findings from the interviews with the four DSOs and the two vendors are grouped and presented in this section (see Table 1 for a summary). 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 vendors. 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 interviews with the DSOs, the ICT security coordinator participated. An extract from the interview guide can be found in Appendix A.

The two interviewed vendors were large organizations who supplied their products to many Norwegian DSOs, and will be referred to as vendor A and vendor B. The interview with vendor A was conducted with the organization's principal engineer and acting cybersecurity manager, whereas the business development manager participated from vendor B. This section presents the results from the interviews with both DSOs and vendors.

3.1 Plans and Communication

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

DSO A said that they do not have a specific plan for cyber-related incidents[1]. The plan they do have is open and does not describe any specific scenario, and it is largely based on improvisation. DSO B has an incident response plan specific for cyber incidents, which includes the process and the roles and responsibilities. DSO D works closely with some of its vendors when developing plans and procedures for incident management, either by adopting routines from the vendors or by developing the plans together. The vendor of the SCADA system has been involved in the development of DSO C's plans for incident response. Neither vendor A nor vendor 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 vendors have contingency plans for their own organization.

DSO A said that their contingency plan includes a prioritized list of people to contact. It is not specified in any agreement with the vendors, 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 vendors. Moreover, during an incident, a contact person is often appointed from the vendor's incident response team. For DSO D, the communication is regulated in the contracts, where both the DSO and vendors state their requirements for the communication. In addition, they have regular meetings with the vendors that provide operational and control systems.

Both vendors have agreements with their customers that state what is expected of them. Vendor 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 vendor. In addition, these agreements set a requirement for how quickly the vendors must be able to provide support in the event of an incident. Similarly, vendor 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 vendor 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.

[1]We can note that this does not seem to fulfil §6.9.d of the Regulation on Security and Preparedness [13].

3.2 Preparedness Exercises

All DSOs and vendors were asked if they have conducted preparedness exercises before and if they have conducted any collaborative exercises with vendors. Since it is required in *Kraftberedskapsforskriften* [13] 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.

Neither DSO A nor DSO B has conducted preparedness exercises with their vendors concerning cybersecurity incidents. DSO B had involved vendors in exercises concerning other topics like organizing transportation during emergencies. DSO A stated that it would be necessary to involve the vendors if a cybersecurity incident should occur. DSO C said that it has happened that vendors have been involved in preparedness exercises, but this is very rare. It would provide value to involve the vendors 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 vendors and that this is something that they are dependent upon since they have vendors in many areas of their operation.

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.

DSO D also said that they have experienced that very technical exercises 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 handles incidents 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.

Vendor A has not participated in any exercises with its customer DSOs directly, although they work closely with them. The vendor is under the impression that exercises are a suitable way for testing plans and procedures for the individual DSOs. Since they are responsible for the products they deliver throughout the whole life-cycle, they view their role when it comes to exercises to be to help with risk assessments in advance and help assess and evaluate after the exercise. Vendor A does not run internal exercises that focus specifically on cybersecurity within the company, but does perform preparedness exercises for other incidents. The vendor has thorough routines and plans regarding what to do if an incident occurs, both internally and externally.

Similarly, vendor 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.

3.3 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 vendors in incident management. DSO A highlighted the importance of trust in the DSO-vendor relationship 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 vendors that participated at DSO A's interview said that it could be beneficial to ensure that the correct routines for incident management are in place, especially regarding alerting, before conducting a collaborative exercise. Moreover, the vendor 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 vendor. Beside the agreement, they think that it is necessary to (1) have continuous contact with the vendors to ensure that they are aware of the agreement's content and ready when it is suddenly needed, (2) be aware of changes in staff at both parties and the adjustments this requires in terms of communication and coordination, and (3) establish precise requirements about expected response time and having a plan for communication if the regular communication lines are down.

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 vendors better during incident management, it is effective to have a different routine for ICT incidents, a sidetrack with direct contact, as this creates awareness.

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

3.4 Attack Scenarios

The interviews were also used to gain insight into relevant attack scenarios that would require involvement from vendors to handle. We asked both the DSOs and the vendors questions regarding this, and their answers were used to create the attack scenarios described in Section 4. For confidentiality reasons, the DSOs did not wish to share risk assesments with us. However, we received an incident response plan 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 IT systems would require the involvement of the vendors 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.

DSO D mentioned that vulnerabilities often are discovered in both internal and external systems before any known attack. In this event, the DSO has to investigate whether the vulnerability

Table 1: Summary of findings from interviews.

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

	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	vendors of the SCADA system have been involved	Yes
DSO D	Yes	Yes	Yes
vendor A	No	No	Yes
vendor B	No	No	Yes

has been exploited, and they have to work together to remove the vulnerability. This is also an example of a valuable exercise scenario to establish some routines on how to proceed.

4 SCENARIOS

This section presents the created scenarios for discussion exercises. The scenarios have been created based on input from interviews with DSOs and vendors and feedback from industry authorities. The data collection results are presented in Section 3. The associated exercise documents will be presented in Section 5.

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 vendors in exercises. Together with the corresponding discussion questions, the scenarios form a discussion exercise with the goal of improving the collaboration between DSOs and vendors 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 for DSOs, we have tried to make it clear to the users that they can choose the alternative that best suits 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.

The attacks that were covered in the seven scenarios created are (1) ransomware, (2) attack on SCADA system, (3) attack on Advanced Metering Infrastructure (AMI), (4) disclosure of sensitive power system information, (5) attack on cloud services, (6) exposed vulnerable service, and (7) defacing of website. Below, we briefly describe the seven scenarios created:

(1) **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 vendors. 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 vendors. 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 [1], hence displaying realism and relevance.

(2) **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 vendor 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.

(3) **Attack on AMI**
This scenario covers an attack on the DSO's Advanced Metering Infrastructure (AMI) that is provided by a vendor. 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.

(4) **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 vendor delivers the SCADA system, it is unknown whether the hackers have obtained the information from the DSO's or the vendor'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.

(5) **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.

(6) **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.

(7) **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 vendor is involved with the operation of the website.

Feedback on the scenarios was gathered from DSO A and B. The seven draft scenarios and some specific points that we wanted feedback on were distributed in advance. 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 gathered feedback from the DSOs, NVE and KraftCERT was reviewed, and we made adjustments to the scenarios. The discussion questions were also updated based on the given feedback.

5 EXERCISE

The preparedness exercise was conducted with DSO A to validate the *Ransomware* scenario in the situation it is intended to be used.The exercise was held in the form of a discussion exercise, and due to the Covid-19 pandemic, it was held digitally using an online tool. 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 vendors participated; the head of information security from one vendor and the ICT security coordinator from the other. Hence, there were eight participants in the exercise in total. The goals of the exercise were to improve the collaboration 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 improvement for coordination and plans.

In order to conduct the discussion exercise, we created the necessary documentation and plans for the implementation, which are described below.

5.1 Scenarios and Questions

For each scenario, a set of associated discussion questions that focus on the collaboration between DSOs and vendors 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 documents of scenarios and the discussion exercises was done to make the scenarios more generalizable so scenarios can be used in other types of exercises.

Selected discussion questions for the *Ransomware* scenario are included in Appendix B.

5.2 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.

5.3 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 to be discussed in the first-impression evaluation.

5.4 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.

5.5 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.

6 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. All of the eight participants in the exercise answered the evaluation. Thus, all of the percentages given below are calculated on the basis that 100 % is 8/8. In the following, we will discuss the exercise evaluation divided into five categories. The results of the DSO and vendor self-evaluation is out of scope of this paper.

6.1 Participants

The evaluation shows that the people and roles that were included in the exercise were appropriate and correct. 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 vendors. 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 vendors, while 1 out of 6 found it useful to *some degree*. From the vendors, one answered that they found it useful to a *high degree*, while the other to a *very high degree*.

6.2 Duration

The participants answered that the allocated time for the exercise was sufficient and appropriate, and that the actual duration of the exercise coincided with the allocated time (maximum 4 hours, including evaluation). When asked whether the distribution of the time on the different parts of the exercise was appropriate, it was commented that the distribution was a bit skewed, and that this might be because some of the questions that were meant for later parts were discussed prematurely.

6.3 The Digital Format

The participants were asked how they thought it was to have a digital exercise. 7 of the participants answered that it worked well or very well, and 6 felt that they were able to speak their opinions whenever they wanted to. However, when asked if they felt that the digital format influenced the outcome of the exercise, the answers were more scattered. 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 2.

Table 2: Advantages and disadvantages with the digital format in an preparedness exercise.

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 vendors	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

6.4 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 highly relevant for both the goals of the exercise and relevant for them to practice.

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.

6.5 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 vendors. The participants were also asked some open questions about the collaboration with vendors, 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 vendors during incident management?
- What do you believe can make it easier to conduct exercises with vendors?

Several of the participants mentioned regular meetings and exercises as a success factor to ease collaboration with vendors during incident management. This will contribute to good relationships and knowledge of each other's routines. 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.

It seems easier to focus on exercises with vendors if it is facilitated externally, e.g. by being handed an exercise program with two exercises per year. 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 vendors 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. Being a new type of cross-organizational exercise for many, which opened the eyes to new perspectives in crisis management, made the overall results and feedback of the exercise positive. More studies and exercises are required to unveil the challenges that need to be taken into account in these types of collaboration exercises.

7 CONCLUSION

We have examined how we can enable vendors' involvement in preparedness exercises with DSOs.

We have created seven attack scenarios that focus on cyber attacks on systems delivered and operated by vendors for many Norwegian DSOs. When creating scenarios for this purpose, it is important to ensure that the main topic is closely related to a service or system delivered by a vendor, 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. 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.

For all of the created scenarios, it is necessary to involve the vendor 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 vendors, 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 vendors.

A data analysis resulted in seven factors that could enable vendors to participate in preparedness exercises with their customers. These revolve around the involvement of vendors in the planning of exercises and creation of incident management plans, ensuring dedicated resources for incident management and exercise planning, making use of less resource-demanding exercises, external facilitation, and specified requirements to vendors either in *Kraftberedskapsforskriften* or in the DSO's contracts with vendors. 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.

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 vendors to participate in preparedness exercises with DSOs, making it less demanding to conduct exercises when remote vendors, and it would also save the time used for traveling.

Finally, our study shows that, in practice, there is a lack of standards and guidelines on how vendors should be included in incident management, especially in the electrical energy sector in Norway. Thus, it is important to continue researching how the collaboration and requirements can be more well-defined and standardized. With the increasing threat of cyber attacks, identifying further factors that could make this industry more prepared to handle cyber attacks is important.

ACKNOWLEDGMENTS

This work has been supported by WP2 of CINELDI – Centre for intelligent electricity distribution, an 8-year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI WP2 partners.

REFERENCES

[1] Alexander Adamov, Anders Carlsson, and Tomasz Surmacz. 2019. An Analysis of LockerGoga Ransomware. In *2019 IEEE East-West Design Test Symposium (EWDTS)*. IEEE, Piscataway, NJ, 1–5. https://doi.org/10.1109/EWDTS.2019.8884472

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

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

[4] Karin Bernsmed, Martin Gilje Jaatun, and Christian Frøystad. 2019. Is a Smarter Grid Also Riskier?. In *Security and Trust Management. STM 2019*. Springer, Cham, 36–52.

[5] Direktoratet for samfunnssikkerhet og beredskap (DSB). 2016. Metodehefte: Spilløvelse. Available online at https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/ovingsveileder/metodehefte_spillovelse.pdf. In *Veileder i planlegging, gjennomføring og evaluering av øvelser (Guide to planning, executing and evaluation exercises)*. (In Norwegian).

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

[7] Elisabeth Kirkebø and Mathias Ljøsne. 2018. *IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen (ICT security in procurement and outsourcing in the energy sector)*. Technical Report 90. Norges vassdrags- og energidirektorat (NVE). https://publikasjoner.nve.no/rapport/2018/rapport2018_90.pdf (In Norwegian).

[8] Mari Langås and Sanna Løfqvist. 2021. *Cybersecurity Preparedness Exercises in Smart Grid: Collaboration With Suppliers During Incident Response*. Master's thesis. Norwegian University of Science and Technology (NTNU).

[9] Ann-Kristin Larsen. 2015. *Øvelser - En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen (Exercises – a guide for planning and executing exercises in the power sector*. Technical Report 39. Norges vassdrags- og energidirektorat (NVE). (In Norwegian).

[10] Nasjonal Sikkerhetsmyndighet (NSM). 2021. *Risiko 2021 (Risk 2021)*. Technical Report. Norwegian National Security Agency. (In Norwegian).

[11] NERC. 2016. *Grid Security Exercise: GridEx III Report.* Technical Report. The North American Electric Reliability Corporation. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/04/GridEX-NERC-GridEx-III-Report.pdf
[12] Rannveig Baaserud Nilsen. 2014. *Øvelse Østlandet 2013: Evalueringsrapport (Exercise Eastern Norway 2013: Evaluation Report).* Technical Report 49. Norges vassdrags- og energidirektorat (NVE). https://publikasjoner.nve.no/rapport/2014/rapport2014_49.pdf (In Norwegian).
[13] Olje- og energidepartementet. 2019. Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften) (Regulation on security and preparedness in the power sector). Available online at https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157. (In Norwegian).
[14] Steve Livingston and Suzanna Sanborn and Andrew Slaughter and Paul Zonneveld. 2019. *Managing cyber risk in the electric power sector.* Technical Report. Deloitte.

A EXTRACT FROM DSO INTERVIEW GUIDE

See Langås and Løfqvist [8] for the complete interview guide.

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?

Vendors

- Which vendors 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 vendors?
- Do you have any agreements or guarantees about how the vendors 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 vendor?
  - Do you check or revise if it corresponds to the demands of the contract?
- How confident are you that the vendor 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 vendors been involved in development of incident management plans and procedures that involve 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 vendors during incident management?
- (How) are vendors involved in training and exercises today?
  - If "not much" or not at all; why not?
  - Are multiple vendors involved at the same time?
  - How are the plans and procedures used in these exercises?
- Do you think that vendors should be involved in exercises with DSOs?
  - Which benefits do you see from including vendors in training and exercises?
- What factors do you think could make it easier to arrange exercises together with some of your vendors?

In case of an incident

- Who is responsible 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?
  - Are vendors involved in this?

B SELECTED DISCUSSION QUESTIONS FOR RANSOMWARE SCENARIO

See Langås and Løfqvist [8] for a more extensive list, also covering other scenarios.

- Which paths could the attacks have taken into the systems?
- How could it be discovered that unauthorized persons have gained access to the systems? By whom?
- What can each of you (DSO, supplier) be able to discover, and how would you be notified?
- 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.
- Do you have a plan for how you would maintain operation without these systems?
- What if the incident spans over a longer period (a week, a month, three months, etc.)?
- Do you have backups of your systems and sufficient redundancy?
- Has an assessment been made of which systems should be prioritized restored first in such a situation?
- What internal information are you dependent on? Do you have a backup of that?
- What external information are you dependent on? Do you have a backup of that?
- How do you recover from backup? How long will the recovery take before the various systems are operational again?
- How would you determine how far back in your backups you have to go to ensure that you have an uninfected version (if possible)?
- Have you trained on recovery of systems in practice? How?
- How would you communicate internally in the organization? With the management, with the employees?
- Do you have a policy for handling extortion attempts?
- Who has the authority to decide whether to pay a ransom?
- Who needs to be involved in handling this incident?
- How will they be contacted?
- Who is responsible for what? What are the necessary roles to be filled in this case?
- What part of your contingency plans will apply in this case?
- What are the procedures for dealing with lost access to systems and the network?
- How will you communicate when the network is down?
- Do you have any agreements with the supplier(s) to ensure assistance in such a situation?
- Who will you notify about this incident and when?