Challenges in IT Security Preparedness Exercises: A Case Study

Maria Bartnes[a,b,1,2,*], Nils Brede Moe[b]

[a] *Department of Telematics,*
Norwegian University of Science and Technology
N-7491 Trondheim
[b] *SINTEF ICT, N-7465 Trondheim*

Abstract

The electric power industry is currently implementing major technological changes in order to achieve the goal of smart grids. However, these changes are expected to increase the susceptibility of the industry to IT security incidents. IT security preparedness exercises are not commonly performed in the electric power industry, even though this industry is considered part of society's critical infrastructure. Resolving an IT security incident requires interdepartmental collaborations between various categories of personnel, and to successfully achieve this, training is required. The process of preparing a response to incidents enhances the nature of collaboration, coordination, and communication within an organization. Our objective is to understand the challenges faced when performing IT security preparedness exercises, as challenges experienced during these exercises affect the response process during a real incident. By improving the exercises, the response capabilities would be strengthened accordingly. We have designed a multiple-case study with six teams in three organizations. We collected data by performing semi-structured interviews, participant observations, and from process artifacts. We identified six main challenges involving team composition and external expert involvement, goal definition, documentation, and time management. In summary, there are many ways of conducting preparedness exercises. Therefore, organizations need to both optimize current exercise practices and experiment with new ones in order to ensure continuous learning and improvement; hence, they can be adequately prepared to respond to IT security incidents.

Keywords: Information security, Incident management, Preparedness

[*] Corresponding author
Email addresses: `maria.bartnes@sintef.no` (Maria Bartnes), `nils.b.moe@sintef.no` (Nils Brede Moe)

[1] Tel.: +47-45218102, Fax: +47-73593350

[2] This work is funded primarily by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*. Partial funding has been provided by the Norwegian Research Council under Grant no. 217528 (DeVID). The authors would like to thank the three DSOs that participated in this study.

exercises, Self-managing teams, Training, Decision-making

1. Introduction

Making preparations for information-security incident management requires training. Basic structures such as well-documented procedures and clear definitions of roles and responsibilities need to be in place, but during an incident, there is no time to study documentation in order to determine the most appropriate response strategies. Involved personnel need to be well trained and well experienced, and they should therefore be able to make the right decisions under pressure (Hollnagel, 2009), as incorrect decisions may cause the incident to escalate and lead to severe consequences.

The electric power industry is currently implementing major technological changes in order to achieve smart grids. These changes involve the application of new technologies for monitoring and control, higher connectivity, and to realize greater integration between different kinds of IT and control systems. However, this will increase the vulnerability to attacks and the potential consequences of attacks (Line, 2013). At the same time, current threat reports show that targeted attacks are on the rise, and critical infrastructures are attractive targets (Batchelder et al., 2014). However, recent studies of the electric power industry show that preparedness exercises for IT security incidents are not commonly performed (Line et al., 2014b,a), although there are guidelines that direct how to plan for and perform such exercises (Grance et al., 2006; NVE, 2015). The reasons for not performing such exercises appear to relate to the understanding of potential threats and consequences, and more pressing tasks tend to receive higher priority. Even though exercises are not performed, personnel from both the IT and the industrial control departments express confidence in their organization's incident-response capabilities.

In highly integrated IT and control systems, IT security incidents are complex, and some degree of competence is therefore needed in order to resolve any situation that may occur. Further, responding to IT security incidents requires that experts in the organization rapidly form a team and adopt a collaborative and speedy decision-making process.

Motivated by the importance of collaborative training in directing any response to information-security incidents, and the apparent problem associated with adopting such training, in our study, we adopt the following research question:

What are the challenges associated with performing tabletop exercises for IT security incidents?

We describe and reflect on the challenges of performing tabletop exercises in three organizations in the electric power industry. Further, we discuss how these challenges may affect the incident-management process during a real-life incident, and we provide recommendations for how to reduce these challenges in a simulated setting.

The work presented in this paper extends a former study by Line and Moe (2015) on collaborative challenges in IT security preparedness exercises.

The paper is structured as follows. In Section 2, we describe related work on preparedness exercises. In Section 3, we present the research method and our case context, while in Section 4, we summarize the observations made during the case study. The challenges are discussed in Section 5 along with recommendations for preparedness exercises. In Section 6, we conclude the paper.

2. Background

The purpose of an emergency preparedness exercise is to strengthen the response capabilities of an organization by enabling that personnel are adequately trained to respond to situations that deviate from normal operations. While there is a need for a set of standard written plans and procedures, during an emergency, there is a need for a more dynamic process, which requires coordination and improvisation, is capable of handling exceptions and violations, and which recognizes the importance of experienced incident handlers. The reliance on predefined documentation is referred to as Model 1 in the use of safety rules and procedures, while enabling the development of new rules based on persons? practical experience is referred to as Model 2 Hale and Borys (2012). One way of developing Model 2 is by performing exercises. Below, we focus particularly on tabletop exercises, as well as coordination and improvisation in the incident-response process.

2.1. Tabletop exercises

Tabletop exercises prepare personnel to respond to emergency situations. They allow for discussions about the roles, responsibilities, procedures, coordination, and decision-making processes, and are a reasonably cost-efficient way of reviewing and learning documented plans and procedures for responding to incidents. Tabletop exercises are usually performed in a classroom without the use of any specific equipment. A facilitator presents a scenario and initiates the discussion. According to the National Institute of Standards and Technology (NIST), a tabletop exercise should consist of the following four phases: (1) Design the event by identifying objectives and participants, (2) Develop the scenario and guides for the facilitator and the participants, (3) Conduct the exercise, and (4) Perform an evaluation by debriefing and identifying lessons learned (Grance et al., 2006), cf. Figure 1. As a training method, tabletop exercises suffer from the weakness in that it does not provide practical demonstrations of the effects of an incident, and neither does it test the true response capabilities of the emergency management process (FEMA, 2003).

[Figure 1 about here.]

Members of a response team do not always possess all the knowledge and skill required for optimum response handling. More commonly, there are aspects of the response for which external expertise would be helpful. When there is a need for external resources, we require a system that makes those resources accessible to the response unit. This may appear straightforward, but it is often challenging because of the need for collaboration between departments and organizations. The specific nature of the assistance required depends on both the technical and business impact of the threat. To understand the gaps in the knowledge and how to design the organization to support the response unit, organizations need to perform exercises frequently and evaluate their outcome (Bartnes et al., 2016).

A realistic exercise requires a realistic scenario. However, creating realistic scenarios is challenging (Hove et al., 2014), and even though an exercise may successfully respond to a given scenario, there are no guarantees that there will be a successful response to a real emergency situation (Rykkja, 2014).

2.2. Coordination in preparedness exercises

Not only is there a need for the structure of the response team to foster competent performance and for the availability of necessary material resources, but the response team itself needs to be able to coordinate the work in an effective matter. The coordination of work and the making of joint decisions are therefore important aspects of the incident-response process, and hence are also important aspects of preparedness exercises. The response to an IT security incident usually involves the collaboration of personnel from different parts of an organization to solve complex problems. "Coordination is management of interdependencies between activities" (Malone and Crowston, 1994) and coordination mechanisms are organizational arrangements that allow individuals to realize a collective performance (Okhuysen and Bechky, 2009). Interdependencies include the sharing of resources, synchronization of activities, and prerequisite activities. Coordination challenges in the incident-response process are functions of the complexity, e.g., processes and technology. Collaborative decision making that involves experts with diverse backgrounds and goals is thus a characteristic of preparedness exercises.

Three basic coordinating mechanisms appear to describe the fundamental ways in which organizations can coordinate their work (Mintzberg, 1989):

1. *Mutual adjustment:* based on the simple process of informal communication
2. *Direct supervision:* one person takes responsibility for the work of others by issuing instructions and monitoring their actions
3. *Standardization* - of which there are four types: work processes, output, skills (as well as knowledge) and norms

While the mechanisms may be at times be substituted with each other, they are all typically present in relatively well-developed organizations. In the area of IT security incident response, all of these coordinating mechanisms are important. Different task complexities require different coordination mechanisms

(Mintzberg, 1989). Simple attacks are easily coordinated by mutual adjustment, but when the incident response becomes more complex, direct supervision and/or standardization tends to be added, and takes precedence as the primary means of coordination. Then, when the incident response becomes very complex, mutual adjustment tends to become primary again, but in combination with the others.

In its pure form, mutual adjustment requires all parties to communicate with everyone else (Groth, 1999). Therefore, if mutual adjustment is employed as the primary coordinating mechanism when responding to an incident, the team or network needs to be compact, and because communication capabilities are limited, they also have to be small.

Further, the response to an IT security incident requires creativity as there may be multiple correct solutions, and a number of uncertainties and interdependencies need to be considered. In creative work, the progress towards completion can be difficult to estimate (Kraut and Streeter, 1995) because the identification of the interdependencies between different pieces of work may be uncertain or challenging. Therefore, it is difficult to know who should be involved in the work, and whether there is a correct order in which parties should complete their own specialized work (Okhuysen and Bechky, 2009). Further, in creative work, it is essential to improve the knowledge transactions between team members. This is captured in a transactive memory system (TMS), a shared cognitive system for encoding, and storing and retrieving knowledge between members of a group (Lewis and Herndon, 2011). TMS can be understood as a shared understanding of who knows what and also as the degree to which we can differentiate between individual knowledge sets.

Coordination can be either predefined or situated (Lundberg and Tellioğlu, 1999). Predefined coordination takes place prior to the situation being coordinated, and can be understood as what Hale and Borys (2012) refer to as Model 1 and an incident response scheme, as described by ISO/IEC 27035 – *Information security incident management* (ISO/IEC, 2011). It typically involves establishing written or unwritten rules, routines, procedures, roles, and schedules. On the other hand, situated coordination occurs when a situation is unknown and/or unanticipated, such as when an IT security incident strikes, and it can be understood as Model 2 (Hale and Borys, 2012). Those involved in the situation do not know in advance how they should contribute. They lack knowledge about what is to be achieved, who should perform each task, how the work should be divided, the sequence in which the sub-activities should be done, when to act, etc. Consequently, they have to improvise and coordinate their efforts in an ad hoc manner. In most collaborative efforts, there is a combination of predefined and situated coordination. For example, involved actors may already know the goal, but not who should perform each task, or they may know who should do each task but not when it is to be done. To compensate for the absence of predefined knowledge regarding the actual unfolding of activities in an exercise, the participants must update themselves on the status of the situation.

To handle a crisis, not only does the team need to coordinate their work, but they also need to take decisions together and be responsible for managing and monitoring their own processes and tasks being executed, i.e., they need to be able to self-manage (Hackman, 1986).

3. Method

The goal of this research is to explore and provide insight into challenges experienced during IT security preparedness exercises. Therefore, it is important to study such exercises practically. We designed a holistic multiple-case study (Yin, 2009) of three IT security preparedness exercises in three different organizations. According to Yin, case studies are the preferred research strategy when a "question is being asked about a contemporary set of events over which the investigator has little or no control" [ibid p. 9].

When conducting a multiple-case study, we followed the five-step process proposed by Yin (2009):

1. *Case study design:* objectives are defined and the case study is planned
2. *Preparation for data collection:* procedures and protocols for data collection are defined
3. *Collecting evidence:* execution of data collection for the studied case
4. *Analysis of collected data*
5. *Reporting*

We planned the introduction of the security preparedness exercises in collaboration with organizations that were to be subjects of this study, making it possible to collect and analyze data similarly across all companies. Case studies can be based on any mix of quantitative and qualitative evidence, and having multiple sources of evidence ensures construct validity and enables triangulation. In this study, we relied on the triangulation of data sources. The first author conducted participant observations in all of the companies, and also collected documents. Examples of documentation were plans for IT security incident responses and illustrations of IT and control networks. An example of physical artifacts is the retrospective board. In each of the organizations, we carried out interviews with the facilitators immediately after the exercise. The process of data collection is described as follows Section 3.1. We analyzed and presented the data, as described in Section 3.2. Further, we presented the scenario used in the exercises, and finally, the case context for our study, i.e., the three organizations and the groups of participants from each organization, are described in Sections 3.3 and 3.4, respectively.

3.1. Data collection

In order to understand the challenges associated with performing tabletop exercises for IT security incidents, the first author acted as a participant observer Robson (2011) studying leadership, decision-making, and involvement. Before presenting the scenario to the participants, she facilitated a plenary session in which the participants were asked about their expectations for the exercise.

The expectations were written on a white board and revisited during the review. Then, she listened in on the group discussions.

To understand the decision process during the five phases and the contributions made by the group members, we made notes specifically regarding the following issues:

- *Leadership*: does anyone take leadership of the discussions?
- *Obtaining information*: how does the group collect necessary information?
- *Decision-making*: how do the group members make decisions? Do they ensure consensus?
- *Certainty*: How certain do the group members appear to be of the decisions that they make?
- *Participation*: Do all participants take part, or are there a few dominant ones?

A review was facilitated after the exercise, where all participants reflected on what worked well and what could have been done differently. Their expectations, which had been identified prior to the exercise, were discussed, and we determined whether they had been fulfilled as well as the reasons. For this session, we used a brainstorming technique based on yellow stickers, and ensured that all participants were given the chance to share their opinions. We also discussed whether their prior expectations had been fulfilled and the accompanying reasons. After the review, the first author performed semi-structured interviews (Robson, 2011) with the facilitators to learn how they experienced the exercise and to discuss whether their expectations were met.

3.2. Data analysis

The authors used a variety of strategies to analyze the data material. One strategy was to describe the preparedness exercises in its context in a narrative in order to understand what had occurred during the exercises. In the analysis, we emphasized the interpretation of events by different participants in the exercises. In this study, we compared the observations, the outcome of the review, and the interviews. By doing this, we observed some patterns (themes), which we then identified, analyzed, and reported using thematic analysis. By analyzing these patterns, we identified the challenges associated with performing tabletop exercises for IT security incident responses.

The first author wrote a summary report for each organization. These reports described observations made during the exercise, as well as the results from the plenary sessions before and after the exercise, i.e., expectations discussed in advance and upon review. Recommendations for future exercises were provided for each organization based on their individual experiences. The reports were sent to the organizations for feedback.

3.3. Scenario

In our study, we used one scenario that was developed and recommended by the authorities[3] for all three organizations. This scenario describes an information security incident that escalated through five phases:

1. An abnormally large amount of data is sent from the organization's network to external recipients.
2. Two weeks later, the supplier of the power automation systems wants to install a patch. The contact is made in a way that is different from what is specified in the service agreement.
3. Three months after the first event, one location suffers from a power outage. The monitoring systems do not display any alarms.
4. Customers start calling as more locations begin to suffer from power outages. The monitoring systems still do not display any alarms.
5. Mobile communications and Internet connections are down.

This list presents the main events for each phase, and more details were included in the description of the scenario presented to the participants. The participants were given 20 min to discuss each phase before they were given information about the next phase. For each phase, the participants had to describe how they would interpret the events and which actions they would take. The facilitator was responsible for checking the time and ensuring that the exercise progressed. If the discussion among the participants went slowly, he would ask questions to ensure that the discussion continued. Further, each phase had a couple of checkpoints for each phase. Examples of such checkpoints include whether the participants would be able to associate the second phase with the first one, as they had occurred two weeks apart, and similarly with the third phase, whether they would have been able to remember the two first phases when the third phase occurred three months later.

3.4. Case context

The three organizations in our study are Norwegian Distribution System Operators (DSOs), and they are among the ten largest DSOs in Norway. For organizations A and B, this was their first execution of such a collaborative exercise for IT security. Organization C had performed a similar exercise once before, and the Emergency Management Team performs preparedness exercises regularly for a variety of incident types. However, one or two persons from each of these DSOs had previously participated in a tabletop exercise arranged by the authorities.

None of the organizations were familiar with the ISO/IEC 27035 (ISO/IEC, 2011) and hence, none had implemented an information security incident management process based on this standard. Up till recently, this has not been important as IT systems have not traditionally been part of their most critical

[3] Norwegian Water Resources and Energy Directorate (NVE)

operations, and they have not experienced any major IT security incidents that have triggered the need for looking to this standard. Below, we present the organizations and discuss how each of them set up their exercise. We also list all participants and the number of years of experience in the organization, cf. Table 1.

Organization A. Three areas of expertise were represented in this exercise: IT operations, industrial control systems, and network infrastructure. Nine participants were present, including the Preparedness Coordinator[4], a representative from an external supplier of power automation systems, and the facilitator.

Organization B. Fourteen participants represented three different areas of expertise: IT, control systems, and control room operations. For the exercise, they were divided into three groups, each of which had one observer. In Table 1, "GO" indicates who was the group observer. The intention was to have all three areas of expertise represented in each group, but because of last-minute changes, which were due to unforeseen business-related events, group 1 did not have anyone from control systems. The HSE/Quality/Preparedness Coordinator, who has more than 20 years of experience, visited all three groups, and is therefore not listed in the table in any one specific group.

Organization C. Twelve employees took part in the exercise. Five belonged to the Emergency Management Team, and were called for when their presence was needed. One person facilitated the exercise in close collaboration with the IT security coordinator.

[Table 1 about here.]

4. Results

The three organizations carried out the preparedness exercises according to generally recommended NIST practices as referred to in Section 2.1. The plans and goals of the exercise were established in advance, and all of the groups/participants discussed the five phases of the scenario, as shown in Figure 2. While the three organizations used the same scenario and main agenda for the exercise, they all had different goals as well as numbers and types of participants. In organization A, the goal that was presented by the facilitator was aimed at exchanging knowledge and experiences in the group. In the other two organizations, the goal was to resolve the incident presented in the exercise. In organization B, the facilitators expressed to us their aim for the groups to self-manage. Further, for all organizations, the composition of the groups was such that they possessed different competencies. Organization C included a management team in their exercise, and this team was called upon when the

[4] All DSOs are required to have this role assigned to someone.

incident escalated to a level where business management-related decisions had to be made. We named the different cases based on the main characteristics concerning goals and setup:

1. Knowledge exchange and process improvement (org. A)
2. Cross-functional self-managing groups (org. B)
3. Involvement of Emergency Management Team (org. C)

[Figure 2 about here.]

Below, we present further details about the setup of the exercise in each organization along with our observations.

4.1. Knowledge exchange and process improvement

In organization A, the IT security coordinator for control systems planned and facilitated the exercise. He presented his goals for the exercise at the beginning: *knowledge exchange across organizational boundaries, obtaining a common understanding of what is technically possible in existing systems, identifying technical and organizational improvements, and ideas for future exercises.* However, the participants expected that the goal was to resolve the incident. The participants were seated around one large table. The scenario was already known to two of the participants, the fiber networks manager and the emergency preparedness coordinator, as they had participated in an identical exercise the previous week in a different context external to the organization. This was the only organization that included one participant from their control system supplier.

Throughout the entire discussion, there were a few participants, and no-one appeared to take charge of the group as the person responsible for involving all participants and achieving consensus. For the first three phases, the IT security coordinator and the fiber networks manager appeared to be quite confident regarding the correct choice of action. Still, they were open about their lack of knowledge regarding systems outside their own domain, and asked questions to other participants in order to obtain a better understanding of how certain actions would affect these systems. In the interview after the review, the facilitator stated that he had expected these two participants to dominate because of their roles, competencies, and personality. He added that in a real emergency situation, only four of the participants would be involved in the crisis management group: himself, the control systems manager, the IT security coordinator, and the fiber networks manager (the latter two being the two most dominant participants).

Based on the review, the participants were satisfied with this exercise as they considered this an important scenario for preparedness exercises, and as shortcomings were revealed, they realized the need to improve their own response capabilities. Furthermore, they approved of the initiative that would enable different parts of the organization meet for an IT security exercise. However, some participants felt that the discussion was somewhat out of control, as they were unable to focus on solving the actual problems presented in the scenario. They would have liked the facilitator to practice more control of the discussion and help them maintain this focus. They also would have liked more time for discussions. On the other hand, the facilitator was satisfied with the discussion, as he saw it as valuable knowledge exchange, which was one of his primary goals. Furthermore, some perceived the final phase of the scenario to be unrealistic and unlikely. When asked about whether their prior expectations had been fulfilled, the participants were fairly satisfied, although they lacked focus on organizational challenges and priorities during the incident-response process.

One important insight obtained during the retrospective was that in a real-life situation, they would not have been able to relate the event in the third phase to the two events that, according to the scenario, occurred three months earlier. The main priority when an incident occurs, is to return the systems to normal operating state, while there is usually less, if any, focus on understanding *why* the incident occurred. In order to strengthen the response capabilities for information security incidents affecting complex IT and control systems, a number of improvements were identified with respect to both technical and organizational perspectives.

4.2. Cross-functional self-managing groups

The exercise in organization B was prepared by a group of three managers from IT security, control systems, and the control room. The former had previously participated in a similar exercise. The goal of the exercise, as defined and presented by one of the facilitators at the beginning, was *to practice collaboration between the industrial control and IT systems departments*. The subgoals were to get to know persons, tasks, and responsibilities across the two involved departments, and to identify general improvements to existing procedures for emergency preparedness and information security. The three managers acted as observers, one for each group of participants. They were responsible for presenting the scenario, ensuring that the group made decisions for each phase of the scenario, and assisting the group in keeping the discussion going, if necessary. Each group was seated around one table in three different meeting rooms.

During the interview, the group observers reported that in general, the group discussions went well and no one person appeared to dominate. In group 3, the control room manager assumed to some extent the role of chairperson for the group; the group observer perceived this as natural based on his role in the organization. This group observer further stated that the participants appeared curious about each other's competencies and responsibilities, as they lacked this insight in order to get the big picture. The observer in group 1 expressed a desire to see more involvement from the management level in future preparedness exercises. He commented that the involvement of the HSE/Quality/Preparedness Coordinator was valuable as this coordinator challenged the groups, both in terms of the assessments and decisions. The observer in group 1 further argued that management tends to have different priorities and different views on situations, such as when would be the right time to shut down the power-automation systems, and including them in exercises enriches the discussion as they contribute with perspectives that differ from those of the other participants.

Each group was intended to be self-managing, with as little intervention from the group observers as possible. During the interview, the group observers stated that it was difficult to keep quiet as they wanted to contribute to the discussions. This was particularly challenging for the observer in group 1, as this group suffered from the absence of control systems personnel, and he was the only one having this competence. However, he chose to remain fairly passive. All group observers reported that they did not need to intervene in order for the discussions to keep going. In addition, there was no need for them to push their groups into making decisions as the group members were focused on solving the problems described in the scenario. While all groups made several decisions on what would be appropriate actions for each phase of the scenario, they did not present clear solutions for all of the sub-problems.

Overall, the participants were satisfied with the exercise, and they appreciated the opportunity to meet and get to know colleagues from other parts of the organization, and to gain insight into their areas of responsibility and knowledge. However, there was some criticism with respect to the scenario description. Some argued that the scenario was not realistic because of the ways in which their systems are integrated. One explained: *"It is stated here that we reinstalled (...), but we would never have done that because (...)"*. For some of the phases, the participants would have liked to have had more than the 20 min allocated for discussions. Furthermore, they did not have the opportunity to hear how the other groups had solved the problems presented in the scenario. Based on this feedback, we arranged a separate feedback meeting for all groups a few weeks later in order to share the results from the group discussions, and how each group solved the problems presented in the scenario. The group observers found the thorough evaluation process to be very valuable, and they considered it advantageous that it was led by an external researcher, as it contributed to the participants putting extra effort into their discussions, as opposed to what may have happened if the facilitator was internal to the organization.

4.3. Involvement of Emergency Management Team

In organization C, the exercise was planned by the IT security coordinator and a facilitator from the communications department. The goal of the exercise was *to raise awareness and practice the response to IT security incidents that occur in the control systems.* The participants were seated around one large table. Five representatives from the Emergency Management Team were present at the beginning of the exercise. After the scenario was presented, three of them left the room before the discussion began, while two chose to remain as passive observers. The entire Emergency Management Team was then to be summoned at a later phase of the scenario, when the seriousness of the incident required their involvement. This was in order to simulate a realistic situation. They were called for twice.

When the first phase of the scenario was presented, the IT operation manager quickly claimed ownership of the incident. He said that he would be the one to get the first alert, and that he would be the one to initiate analyses and report to other stakeholders in the organization. One issue that was thoroughly discussed was the reporting from IT to the control room, i.e., if and when it would be done, was it relevant to inform the control room staff, and whether this reporting line was documented. During the discussion, reporting lines and details on when to report different types of information between different departments were identified as details that were missing in the documented procedures. Nevertheless, the group still knew who to contact. Another issue that received a lot of attention in the group discussion related to the shutting down of the control systems. The IT operation manager would recommend this at the stage where the control room supplier calls and wants to install a security patch in the control systems (phase two), as he was worried about the possibility of the malware infections spreading further into the systems. On the other hand, the control system manager claimed that shutting down the control systems would have had major financial consequences for the operations, as manual operations are expensive. The Emergency Management Team decided to shut down the control systems in the fourth phase of the scenario. During the evaluation, it was agreed that such an incident would pose a great challenge for the organization. However, they still concluded that the situation was resolved satisfactorily in this exercise, and that they would be able to maintain power production and distribution, even though the control systems were shut down, by manually operating power stations. The facilitators felt that relevant assessments and decisions were made, and that the Emergency Management Team became involved at the right points in time. The Emergency Management Team contributed by providing thorough analyses and unambiguous decisions.

5. Discussion

Major technological developments related to the implementation of smart grids pose new threats to the electric power industry, and the distribution system operators in particular. Emerging threats create the need for a well-established capacity for respond- ing to unwanted incidents. Such a capacity is influenced by both organizational, human, and technological factors, and this capacity needs to be continuosly revised and improved. Preparedness exercises is one way of improving the incident-response capacity in an organization.

We have described a tabletop exercise that was performed in six groups formed at three large Norwegian electric power DSOs. While they all relied on the same scenario, their exercises were organized differently. Below, we discuss the importance of preparedness exercises, along with our results in the light of our research question: *What are the challenges associated with performing tabletop exercises for IT security incidents?* Then, we discuss how the challenges that were observed could affect a real-life incident-response process. Finally, we provide recommendations for ways in which we may realize preparedness exercises.

Our study confirmed the importance of conducting preparedness exercises. In organization A, they realized that in a real situation, they would have been unable to link the third phase to the first two, i.e., events that occur three months apart. They have not had a sufficient number of such incidents, and they reported that it would depend on whether the same personnel were on duty at both instances in time. During the exercise, they became aware that such potential links exist. Furthermore, the participants in organization B were not sufficiently aware of each other?s needs for information, and they therefore realized ways in which the information flow could be improved. The need for information sharing was demonstrated by statements from participants: *"Oh, they need this kind of alerts?"* and *"...so they actually read this information?"*.

Participants in all three organizations stated similar expectations before the exercise, such as a desire to learn about threats and challenges, understand roles and responsibilities and experience how collaboration works across different parts of their organization, and to identify the need for improvements in documentation and processes. As part of the post-exercise review, the evaluation indicated that these expectations were met fairly well in all three organizations. In two of the organizations in our study, A and B, the participants had differing views on whether or not the scenario was realistic. This difference shows a need to develop a common perception of possible threats and potential consequences, which can be partly achieved by performing exercises.

The information security incident management process was quite immature in all three organizations, as none had implemented the ISO/IEC 27035 standard (ISO/IEC, 2011) and they were not well experienced in performing preparedness exercises with the personnel required for responding to information security incidents. Their general emergency preparedness was however more mature, as they are well experienced in preparing for, and responding to, other kinds of incidents, such as bad weather conditions, fire, and other physical, and more traditional, incidents.

There is no single best practice on organizing tabletop exercises. However, we found a number of challenges that need to be understood in order to succeed with such training.

5.1. Defining goals.

For a team to achieve good performance and to effectively solve a complex problem, there needs to be a shared understanding of the team goals (Moe et al., 2010). Having several and sometimes conflicting goals for the exercise may result in individual members working towards different goals. In organization A, the team focused on solving the given problem, while the facilitator was just as focused on knowledge sharing and fruitful discussions. As a consequence, there were problems with respect to maintaining the focus during the exercise, which frustrated some of the participants.

Different goals require different exercise designs. If the goal is to solve the problem and to run the incident-response process in as realistic a manner as possible, the group of participants should resemble the core team who would actually be involved in a real-life response process. Other persons could be present as observers, and could be placed at a different table. On the other hand, if the goal is to exchange knowledge across different departments and between different groups of personnel, more participants should be included in the exercise. Getting to know people, as well as knowing who knows what, are important in order to make the organization work as efficiently as possible during an incident-response process. Both types of exercises should therefore be carried out, as they are valuable to the organization in different ways.

The main goal of the exercise should be defined and discussed by the whole team. This goal should then guide the design and execution of the exercise. Additional goals may be included as subgoals, and may be addressed during the evaluation afterwards, as was done in organization B.

Recommendation: Define only one main goal for the preparedness exercise and ensure that all participants have a common understanding of the goal.

5.2. Enabling self-management and growing team knowledge.

For a team to solve a crisis and make good decisions, it needs to be able to self-manage. Members of self-managing teams are responsible for managing and monitoring their own processes and executing tasks (Hackman, 1986). They jointly share decision authority, rather than having a centralized decision structure where one person makes all the decisions, or a decentralized decision structure where team members make independent decisions. Based on the results, organization A had problems self-managing as two persons made most of the decisions. It was later concluded that only a few of the team members would participate in a real situation. The others should have been present as observers to distinguish between persons who are part of the team and those who are not, i.e., if the goal was to run a realistic scenario rather than support knowledge exchange.

Enabling self-management further requires the group to have the necessary competence; otherwise, the group will be training to solve the problem without having the required competencies. However, because incident handling requires creativity, it may be challenging to identify in advance all of the personnel who should be present for the training. One of the teams in organization B clearly suffered from the lack of competence, and organizations B and C both lacked personnel from their external suppliers. The training outcome would have been better had the right personnel been present.

In addition to the right competence, to solve a crisis effectively, there is a need for a shared understanding of the knowledge possessed by different individuals (Lewis and Herndon, 2011). We found that in most teams, persons did not have a good overview of what the others knew; however, the team members became more aware of each other?s knowledge sets during the exercise.

In a given situation, it is possible to identify where to find the right competence by starting the exercise with just one person receiving an alert. This person needs to determine to whom the report should be made, who should get involved, and the response team will then emerge throughout the response process. To ensure that there is a realistic response to the alert, management has to inform personnel in advance that there will be an exercise.

Recommendation: Ensure the involvement of all required competencies in the team, including personnel from external suppliers. If the personnel present exceed those required, clearly differentiate between the team members and the observers. Include a facilitator to support the team in making joint decisions and conduct exercises frequently to develop a shared understanding of what information is possessed by different persons.

5.3. Availability of personnel.

Businesses require continuous operations, and may require sudden and unforeseen actions, which in turn may cause personnel to excuse themselves from the exercise. This will affect the group composition, as was the case for organization B, where last-minute changes led to the absence of one type of competence in one of the groups. Further, members of management groups tend to have little time for exercises, but their presence is needed to add realism to the exercise. Limiting the time spent on exercises would most likely make it easier for key personnel to participate. All organizations experience turnover rate. Hence, during a real-life incident, there may also be the sudden absence of a critical competence.

Recommendation: Perform preparedness exercises frequently to ensure that all personnel receive training regularly. Limit the time spent on each exercise to make it easier for key personnel to participate.

5.4. Time management.

The allocation of 20 min to discuss each phase was perceived as too short for some persons, while it was sufficient for others, depending on both the participants and the complexity of the given problems. However, it was understood that by creating a time-pressure for making quick decisions, the exercise became realistic. Still, according to FEMA (2003), it is wise to take the time to resolve problems. A facilitator needs to balance the amount of time spent on the different phases based on the progress and how well the team performs.

It is important to make the time for a thorough evaluation after the exercise in order to improve the benefits of the exercise, and this was also recommended by NIST (Grance et al., 2006). Both organizations A and B spent 60?70 min on their evaluations, and stated that a significant benefit was that of having an external facilitator perform this task, as the participants clearly put more effort into contributing than they would usually do during internal evaluations. A similar evaluation was planned for organization C, but they ran out of time and did not prioritize performing a thorough evaluation after the exercise. A short around-the-table discussion was performed instead.

If knowledge exchange is the main motivation for the exercise, the evaluation should be performed after each phase and not only at the end. The participants should be given the opportunity to discuss the decisions made, group dynamics, and information sharing before moving on to the next phase.

Recommendation: Ensure time pressure by limiting the time for problem-solving in the exercise. Allow for thorough reflections in a plenary session immediately after the exercise is completed. If there is more than one group, add time for reflection within each group as well, prior to the plenary session. If the goal is knowledge exchange, allow for evaluations after each phase.

5.5. Use of existing documentation.

During the exercise, none of the teams actively consulted written plans or procedures for IT security incident responses. Such plans were made available to the team in organization C only. Although documentation needs to be in place, situated coordination is more important because the scenarios in the exercise are unknown. When handling a crisis, an organization therefore needs to rely on the individuals and their knowledge. In organization C, the absence of reporting procedures was identified, but the participants still knew who to contact and when. It was stated that in an emergency situation, there would be no time to consult documentation. Exercises therefore contribute to the development of practical knowledge and the knowledge of who knows what, which is essential to make good decisions when handling an incident. Nevertheless, documentation would be available during a real situation, and it should therefore also be available during an exercise. One of the main goals when performing a tabletop exercise is to review plans and procedures (FEMA, 2003), and this should be performed shortly after the exercise.

Recommendation: Ensure the availability of written documentation during the preparedness exercise, and review the documentation in retrospective, if necessary. If the available documentation is not consulted, discuss the reason for this.

5.6. Involvement of business management.

It is essential to involve those with the authority to make decisions that influence business operations. IT security involves persons other than IT personnel, as an incident may have severe consequences for the organization, its customers, and society at large. In an emergency situation, the goal from a business perspective is usually to maintain normal operations as much as possible. However, there are different strategies that may be used for this: resolve the incident with as little disturbance as possible to the operations, understand why the incident occurred, and ensure that the incident will not repeat itself. These different strategies require slightly different approaches and priorities, and it is therefore crucial that the incident responders have a common understanding of the overall preferred strategy.

Organization C appeared to succeed with their model in that the team called for the Emergency Management Team when the severity of the incident required this. In organization C, the IT personnel wanted to shut down the control systems rather early because of their fear of malware infections; the control room manager wanted to wait because of the high cost of manual operations. These costs were compared to the consequences of an uncontrolled breakdown. We found that the priorities of different parts of the organization vary, which supports the need for simultaneously carrying out collaborative exercises and the practice of joint decision-making as different authority levels come into play.

Recommendation: Include all personnel who will play a role during a real-life incident, including both technical personnel and business representatives.

5.7. Remarks concerning existing guidelines.

Our study shows that different organizations have different goals for the same type of exercise, although a single exercise should have only one primary goal. This differs slightly from the recommendations made by NIST 800-84 (Grance et al., 2006), where it is stated that the objectives of an exercise should *validate the content of the IT plan and related policies and procedures, validating participants? roles and responsibilities, as documented in the plan, and validating the interdependencies documented in the plan.* Further, an additional objective could be to *meet regulatory and other such requirements that are associated with exercising plans.* FEMA (2003) states that the purpose is *usually to resolve problems or make plans as a group.* Note that there is some value of running different types of exercises with different types of goals in order to realize all of the needs of a given organization. Defining the main goal for an exercise needs to be the very first step of the planning process, as the design and setup of the exercise depend highly on this goal.

Evaluation is an important part of the exercise. Whereas NIST 800-84 (Grance et al., 2006) stresses the after-action report, we believe that the plenary session with all participants has a much higher learning value than the written report itself. However, a written report serves an important purpose of contributing to organizational knowledge and memory, which cannot be achieved by the plenary session alone. Further, we highly recommend continuous evaluation throughout the exercise when the goal is knowledge exchange.

6. Concluding remarks and future research

For industrial control organizations to withstand and/or successfully respond to attacks, personnel from different parts of the organization, e.g., IT, control systems, control room, networks/infrastructure, and business representatives, need to collaborate with each other. These groups of personnel do not usually have a tradition for collaborating with each other, as industrial control systems used to be isolated from administrative IT systems. However, a holistic view of the incident-response process is needed so that the whole organization is included in training, as it would be during a real emergency situation. A systematic approach based on the ISO/IEC 27035 standard on information security incident management would strengthen the organizations' overall response capabilities and preparedness.

There are many ways to conduct preparedness exercises. Therefore, organizations need to both optimize current exercise practices and experiment with new ones. Regardless of how the exercises are conducted, there are a number of challenges of which we should be aware of, as mentioned in our study. In addition, to improve the operational capabilities, we should perform functional exercises to supplement tabletop exercises.

We studied cases in which organizations performed inadequate IT security preparedness exercises. There is therefore a need to study the challenges that were met by organizations that are more advanced with respect to performing preparedness exercises for IT security incidents. Such a study should also investigate the good practices being performed by these organizations during their exercises. Further, challenges that are met during real-life incident-response processes should be investigated in order to make preparedness exercises even more useful.

References

Maria Bartnes, Nils Brede Moe, and Poul E. Heegaard. The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, 61, 2016.

Dennis Batchelder, Joe Blackbird, David Felstead, Paul Henry, Jeff Jones, and Aneesh Kulkarni. Microsoft Security Intelligence Report. Microsoft, 2014.

FEMA. IS 139 Exercise Design – Unit 5: The Tabletop Exercise. Federal Emergency Management Agency – Emergency Management Institute (FEMA), 2003.

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, 2006.

Lars Groth. *Future Organizational Design: The Scope for the IT-based Enterprise*. John Wiley Series in Information Systems. Wiley, 1999.

J. R. Hackman. *The psychology of self-management in organizations*. American Psychological Association, Washington, D. C., 1986.

Andrew Hale and David Borys. Working to rule, or working safely? Part 1: A state of the art review. *Safety Science*, 2012. ISSN 0925-7535. doi: 10.1016/j.ssci.2012.05.011. URL `http://www.sciencedirect.com/science/article/pii/S0925753512001312`.

Erik Hollnagel. The four cornerstones of resilience engineering. In Christopher P. Nemeth, Erik Hollnagel, and Sidney Dekker, editors, *Preparation and Restoration, Resilience Engineering Perspectives*, volume 2 of *Ashgate Studies in Resilience Engineering*, chapter 6. Ashgate Publishing, Ltd., 2009. ISBN 978-0-7546-7520-4.

Cathrine Hove, Marte Tårnes, Maria B. Line, and Karin Bernsmed. Information security incident management: Identified practice in large organizations. In *8th International Conference on IT Security Incident Management and IT Forensics (IMF)*, pages 27–46, May 2014. ISBN 978-1-4799-4330-2.

ISO/IEC. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management, 2011.

Robert E. Kraut and Lynn A. Streeter. Coordination in Software Development. *Communications of the ACM*, 38(3):69–81, March 1995. ISSN 0001-0782. doi: 10.1145/203330.203345. `http://doi.acm.org/10.1145/203330.203345`.

Kyle Lewis and Benjamin Herndon. Transactive Memory Systems: Current Issues and Future Research Directions. *Organization Science*, 22(5):1254–1265, September 2011. ISSN 1526-5455. doi: 10.1287/orsc.1110.0647. `http://dx.doi.org/10.1287/orsc.1110.0647`.

Maria B. Line. Why securing smart grids is not just a straightforward consultancy exercise. *Security and Communication Networks*, 7(1):160–174, 2013. ISSN 1939-0122. doi: 10.1002/sec.703. `http://dx.doi.org/10.1002/sec.703`.

Maria B. Line and Nils Brede Moe. Understanding Collaborative Challenges in IT Security Preparedness Exercises. In *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015*, pages 311–324. Springer Science and Business Media, 2015.

Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard A. Kemmerer. Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared? In *21st ACM Conference on Computer and Communications Security and Co-located Workshops*, pages 13–22, November 2014a. ISBN 978-1-4503-2957-6.

Maria Bartnes Line, Inger Anne Tøndel, and Martin Gilje Jaatun. Information security incident management: Planning for failure. In *8th International Conference on IT Security Incident Management and IT Forensics (IMF)*, pages 47–61, May 2014b. ISBN 978-1-4799-4330-2.

Nina Lundberg and Hilda Tellioğlu. Understanding Complex Coordination Processes in Health Care. *Scandinavian Journal of Information Systems*, 11(2):157–181, July 1999. ISSN 0905-0167. `http://dl.acm.org/citation.cfm?id=350717.350748`.

Thomas W. Malone and Kevin Crowston. The Interdisciplinary Study of Coordination. *ACM Computing Surveys*, 26(1):87–119, March 1994. ISSN 0360-0300. doi: 10.1145/174666.174668. `http://doi.acm.org/10.1145/174666.174668`.

Henry Mintzberg. *Mintzberg on Management: Inside Our Strange World of Organizations.* Free Press, 1989.

Nils Brede Moe, Torgeir Dingsøyr, and Tore Dybå. A teamwork model for understanding an agile team: A case study of a scrum project. *Information and Software Technology*, 52(5):480 – 491, 2010. ISSN 0950-5849. doi: http://dx.doi.org/10.1016/j.infsof.2009.11.004. URL `http://www.sciencedirect.com/science/article/pii/S0950584909002043`.

NVE. Øvelser: En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen (in Norwegian). Norwegian Water Resources and Energy Directorate, 2015.

Gerardo A. Okhuysen and Beth A. Bechky. Coordination in Organizations: An Integrative Perspective. *The Academy of Management Annals*, 3(1):463–502, 2009. doi: 10.1080/19416520903047533. `http://dx.doi.org/10.1080/19416520903047533`.

Colin Robson. *Real world research.* John Wiley & Sons Ltd., 3rd edition, 2011.

Lise Hellebø Rykkja. *Organisering, samfunnssikkerhet og krisehåndtering*, chapter Kap. 8: Øvelser som kriseforebygging. Universitetsforlaget, 2 edition, 2014.

Robert K. Yin. *Case Study Research - Design and Methods, 4th ed.*, volume 5 of *Applied Social Research Methods*. SAGE Publications, 2009.

List of Figures

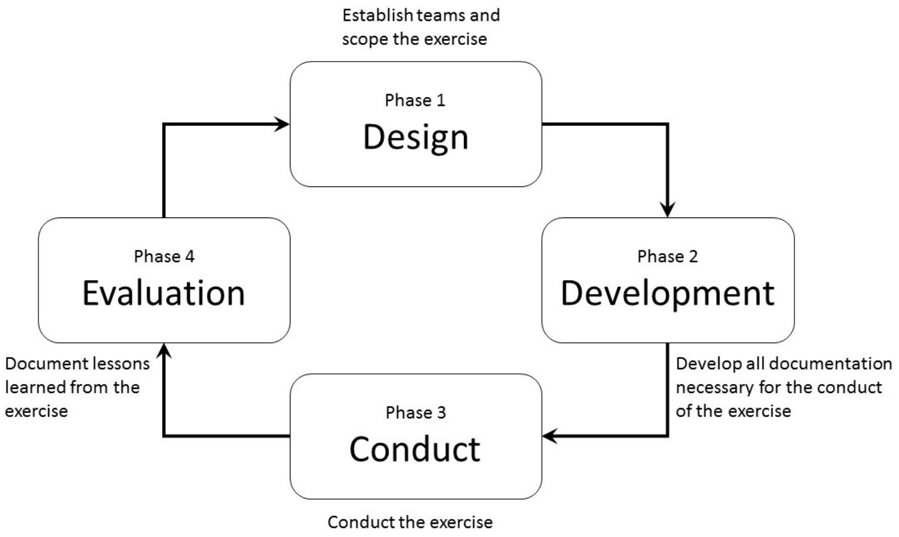
Establish teams and scope the exercise
Phase 1
Design
Phase 2
Development
Develop all documentation necessary for the conduct of the exercise
Phase 3
Conduct
Conduct the exercise
Phase 4
Evaluation
Document lessons learned from the exercise

Figure 1: NIST 800-84: Methodology for Test, Training and Exercise Programs for IT Plans and Capabilities. (Grance et al., 2006)

Figure 2: Group members engaging in the discussion on how to resolve the given incident.

List of Tables

Table 1: The teams in the three organizations - the participants' roles and years of experience

Org.	**Team**	**Role**	**Exp.**
Org. A	Group 1	IT production manager	5
		IT security coordinator	25
		Fiber networks manager	>20
		Senior engineer, fiber networks	5
		Control systems manager	20
		Special advisor, remote control units	>30
		Service engineer, supplier of control systems	>30
		Emergency preparedness coordinator	>30
		IT security coordinator for control systems (facilitator)	28
Org. B	Group 1	Control operations engineer	10
		IT infrastructures engineer	9
		IT operations engineer	1
		IT manager	4
		Control systems manager (GO)	1
	Group 2	Control operations engineer	25
		Control operations engineer	>20
		IT operations engineer	29
		IT operations engineer	8
		IT business systems manager	>20
		IT consultant	1
		Control operations manager (GO)	>10
	Group 3	Control systems engineer	6
		Control room manager	8
		IT operations engineer	>15
		IT operations engineer	8
		IT security manager (GO)	12
Org. C	Group 1 (technical personnel)	Manager, Control room DSO	5
		Deputy manager, Control room DSO	34
		Manager, Control systems	36
		Manager, Control room, Power production	7
		IT operation manager	4
		IT network security engineer	6
		Marketing, Broadband, Technical manager	8
	Group 2 (emergency management team)	Main corporation: IT manager	3
		Power production, CEO	19
		DSO Technical manager	28
		Main corporation: Deputy Chief of Communications	19
		Main corp.: Emergency preparedness coordinator	30
		DSO Manager, emergency preparedness manager	5