# Understanding Collaborative Challenges in IT Security Preparedness Exercises

Maria Line, Nils Moe



# Understanding Collaborative Challenges in IT Security Preparedness Exercises

Maria B. Line[1,2] and Nils Brede Moe[2]

[1] Norwegian University of Science and Technology (NTNU), Norway
[2] SINTEF, Norway
maria.b.line@item.ntnu.no,nils.b.moe@sintef.no

**Abstract.** IT security preparedness exercises allow for practical collaborative training, which in turn leads to improved response capabilities to information security incidents for an organization. However, such exercises are not commonly performed in the electric power industry. We have observed a tabletop exercise as performed by three organizations with the aim of understanding challenges of performing such exercises. We argue that challenges met during exercises could affect the response process during a real incident as well, and by improving the exercises the response capabilities would be strengthened accordingly. We found that the response team must be carefully selected to include the right competences and all parties that would be involved in a real incident response process, such as technical, managerial, and business responsible. Further, the main goal of the exercise needs to be well understood among the whole team and the facilitator needs to ensure a certain time pressure to increase the value of the exercise, and both the exercise and existing procedures need to be reviewed. Finally, there are many ways to conduct preparedness exercises. Therefore, organizations need to both optimize current exercise practices and experiment with new ones.

**Keywords:** Information Security, Incident Management, Preparedness Exercises, Training, Decision-making, Self-managing Teams

## 1 Introduction

Preparing 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 figure out the most appropriate response strategies; involved personnel needs to be well trained and well experienced, and hence able to make the right decisions under pressure [1]. Wrong 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 concern new technologies, higher connectivity and more integration, which increase the attack surface and the potential consequences of attacks [2]. At the same time, current threat

reports show that targeted attacks are on the rise, and critical infrastructures are attractive targets [3]. However, recent studies of the electric power industry show that preparedness exercises for IT security incidents are not commonly performed [4, 5] though guidelines exist for how to plan and perform such exercises [6, 7]. Reasons for not performing such exercises seem to relate to their perception of the probability of being attacked and their understanding of potential threats and consequences, and that more pressing tasks receive higher priority. Still, personnel from both the IT staff and the industrial control staff express confidence in their organization's incident response capabilities.

Motivated by the importance of collaborative training for responding to information security incidents, and the evident problem of adopting such training, the following research question is defined for our study:

*What are the challenges of performing tabletop exercises for IT security incidents?*

We will discuss how these challenges might affect the incident management process during a real-life incident and provide recommendations for how to reduce these challenges in the setting of an exercise, as that should positively affect a real-life incident management process as well.

The paper is structured as follows. Related work on preparedness exercises are described in Section 2. The research method and our case context are presented in Section 3, while Section 4 sums up the observations made during the case study. Challenges are discussed in Section 5 along with recommendations for preparedness exercises, and Section 6 concludes the paper.

## 2 Background

The purpose of an emergency preparedness exercise is to strengthen the response capabilities of an organization by training personnel in responding to situations that deviate from normal operations. A certain baseline of written plans and procedures should be present. However, during an emergency there is a need for a more dynamic process that requires coordination and improvisation, and where exceptions and violations are managed, and experienced incident handlers are valued. Relying on predefined documentation is what Hale and Borys refer to as Model 1 in the use of safety rules and procedures [8], while allowing for rules to be emerged from practical experience is referred to as Model 2. Exercises are a way of developing Model 2. In the following we elaborate on tabletop exercises specifically, and coordination and improvisation in the incident response process.

### 2.1 Tabletop exercises

Tabletop exercises prepare personnel for responding to an emergency situation. They allow for discussions of roles, responsibilities, procedures, coordination, and

decision-making, and are a reasonably cost-efficient way of reviewing and learning documented plans and procedures for incident response. 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; Design the event by identifying objectives and participants, Develop the scenario and guides for the facilitator and the participants, Conduct the exercise, and Evaluate by debriefing and identifying lessons learned [6]. As a training method it suffers from the weakness that it does not provide practical demonstrations of the effects of an incident or the emergency management's true response capabilities [9].

In his study of preparedness exercises initiated by the Norwegian Water and Energy Directorate (NVE), Gåsland [10] found that there is a positive attitude for participating in exercises and an understanding that collaboration is important in problem-solving processes. He still found that exercises compete with daily tasks for prioritization, and he considered it to be an obstacle to learning if exercises are not used as a means of making improvements afterwards. Further, he emphasized the importance of making exercises as realistic as possible. However, creating realistic scenarios is challenging [11], and even though a scenario is successfully responded to in an exercise, it does not give any guarantees that a real emergency situation will be successfully responded to [12].

### 2.2 Coordination in preparedness exercises

Coordination of work and making collaborative decisions are important aspects of the incident response process and hence also of preparedness exercises. Responding to an IT security incident usually implies personnel from different parts of an organization collaborating on solving complex problems. "Coordination is management of interdependencies between activities" [13] and coordination mechanisms are the organizational arrangements, which allow individuals to realize a collective performance [14]. Interdependencies include sharing of resources, synchronization of activities, and prerequisite activities. Coordination challenges in incident response are functions of the complexity, such as processes and technology.

Further, responding to an IT security incident is creative work, as there might not be one correct solution and a number of both uncertainties and interdependencies need to be taken into account. In creative work progress towards completion can be difficult to estimate [15] because interdependencies between different pieces of work may be uncertain or challenging to identify. This makes it 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 [14]. 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, storing and retrieving knowledge between members of a group [16]. TMS can be understood as a shared understanding of

who knows what and also on the degree to which individual knowledge sets are differentiated.

Coordination can be either predefined or situated [17]. Predefined coordination takes place prior to the situation being coordinated and can be understood as what Hale and Borys refer to as Model 1 [8] and an incident response scheme as described by ISO/IEC 27035 – *Information security incident management* [18]. It typically consists of establishing written or unwritten rules, routines, procedures, roles, and schedules. Situated coordination, on the other hand, occurs when a situation is unknown and/or unanticipated, such as when an IT security incident strikes, and can be understood as Model 2 [8]. Those involved in the situation do not know in advance how they should contribute. They lack knowledge of what to achieve, who does what, how the work can be divided, in what sequence sub-activities should be done, when to act, etc. Consequently, they have to improvise and coordinate their efforts ad hoc. In most collaborative efforts there is a mix of predefined and situated coordination. Involved actors may for instance already know the goal, but not who performs what, or they may know who does what but not when to do it. To compensate for lacking predefined knowledge of how the actual unfolding of activities in an exercise will be, 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; they also need to take decisions together and be responsible for managing and monitoring their own processes and executing tasks, i.e they need to be able to self-manage [19].

## 3 Method

Since the goal of this research was to explore and provide insight into challenges experienced during IT security preparedness exercises, it was important to study such exercises in practice. We designed a holistic multiple case study [20] 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]. In the following, we present the scenario used, the organizations studied, and how data collection and analysis were performed.

### 3.1 Scenario

One scenario recently recommended by the authorities[3] was used by all organizations in our study. This scenario describes an information security incident that escalates through five phases:

1. Abnormally large amounts of data is sent to external recipients.
2. Two weeks later, the SCADA supplier wants to install a patch. The contact is made in a different way than what is regulated in the service agreement.

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

3. Three months after the first event, one area suffers from power outage. The monitoring systems do not display any alarms.
4. Customers start calling as more areas suffer from power outage. The monitoring systems do still not display any alarms.
5. Mobile communications and Internet connections are down.

The participants had 20 minutes to discuss each phase before they were given information about the next. For each phase the participants had to describe how they would interpret the events and which actions they would take.

### 3.2 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. In the following, we present the organizations and how each of them set up their exercise, as well as all participants and their number of years of experience in the organization.

**Organization A.** Three groups of personnel 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 external supplier of SCADA systems, and the facilitator, cf. Table 1.

**Table 1.** Participants in organization A

| Role | Exp. |
|---|---|
| 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 |

**Organization B.** Fourteen participants represented three different areas of expertise: IT, control systems, and control room operations. They were divided into three groups for the exercise, and there was one observer in each group, cf. Table 2. "GO" indicates who was the group observer. The intention was to have all three areas of expertise represented in each group, but last minute changes due to sudden business-related events caused group 1 to not have anyone from control systems. The HSE/Quality/Preparedness Coordinator, who has more

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

than 20 years of experience, visited all three groups and is therefore not listed in the table in one specific group.

**Table 2.** Participants in organization B

| Group 1 | | Group 2 | | Group 3 | |
|---|---|---|---|---|---|
| **Role** | **Exp.** | **Role** | **Exp.** | **Role** | **Exp.** |
| Control operations eng. | 10 | Control operations eng. | 25 | Control systems engineer | 6 |
| IT infrastructures engr. | 9 | Control operations eng. | >20 | Control room manager | 8 |
| IT operations engineer | 1 | IT operations engineer | 29 | IT operations engineer | >15 |
| IT manager | 4 | IT operations engineer | 8 | IT operations engineer | 8 |
| Control sys. manager (GO) | 1 | IT business sys. manager | >20 | IT security manager (GO) | 12 |
| | | IT consultant | 1 | | |
| | | Control ops. manager (GO) | >10 | | |

**Organization C.** Twelve employees took part in the exercise, cf. Table 3. 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 3.** Participants in organization C

| Technical personnel | | Emergency Management Team | |
|---|---|---|---|
| **Role** | **Exp.** | **Role** | **Exp.** |
| Manager, Control room DSO | 5 | Main corporation, IT manager | 3 |
| Deputy manager, Control room DSO | 34 | Power production, CEO | 19 |
| Manager, Control systems | 36 | DSO Technical manager | 28 |
| IT operation manager | 4 | Emergency preparedness coordinator | 30 |
| IT network security engineer | 6 | DSO Manager, emerg. prep. manager | 5 |
| Marketing, Broadband, Tech. manager | 8 | | |

### 3.3 Data collection and analysis

The first author contributed to the planning of all the tabletop exercises. Before the scenario was presented to the participants, they were asked about their expectations for the exercise. A retrospective was facilitated after the exercise, where all participants reflected upon what worked well and what could have been done differently. Their expectations from beforehand were discussed; whether they were fulfilled and why/why not.

For the analysis, we described the tabletop exercises and evaluations from each organization to achieve an understanding of what was going on during the exercises. Then we categorized interesting expressions and observations, before we compared findings between the organizations.

## 4 Results

The three organizations carried out the preparedness exercises according to generally recommended NIST practices. Plans and goals of the exercise were established in advance, and they all discussed the five phases of the scenario. While

the three organizations used the same scenario and main agenda for the exercise, they all had diversity in goals and the number and types of participants. Our observations are hereby presented, as characterized by the following descriptions:

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

### 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 in the beginning: *knowledge exchange across organizational boundaries, obtaining a common understanding of what is technically possible in todays' systems, identifying technical and organizational improvements, and ideas for future exercises.* The participants were seated around one big 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 this exact same exercise the week before in a different context. This was the only organization that included one participant from their supplier.

A few participants dominated throughout the whole discussion and nobody seemed to take charge of the group as a chair person responsible for involving all participants and achieving consensus in the group. For the first three phases the IT security coordinator and the fiber networks manager appeared to be quite sure of what would be the right choices of action. Still, they were open about lacking knowledge of systems outside their own domain and asked questions in order to get the whole picture. The facilitator later commented that he had expected these two participants to dominate because of their roles, competences, and personality. He added that in a real emergency situation, only four of the participants would be involved in the crisis management group: the two most dominant participants, the control systems manager, and himself.

The participants were satisfied with this exercise being performed, as they see this as an important scenario for preparedness exercises and as lacks were revealed that they need to work on to improve their own response capabilities. Furthermore, they approved of the initiative of making different parts of the organization meet for an IT security exercise. However, some participants felt that the discussion was a bit out of control, as they did not manage to keep the focus on solving the actual problems presented in the scenario. They missed a person facilitating the discussion. The facilitator, on the other hand, was satisfied with the discussion, as he saw it as valuable knowledge exchange, which was one of his main goals. At the same time, some participants would have liked to have more time for discussions. Furthermore, some perceived the last phase of the scenario to be unrealistic and unlikely.

One important insight obtained was that they would not be able to relate the event in the third phase to the two events that occurred three months earlier. Their main priority is usually to get the systems back to normal operations, while

understanding *why* the incident occurred typically receives less focus, if any. A number of improvements were identified, regarding both technical and organizational aspects, in order to strengthen the response capabilities for information security incidents affecting complex IT and control systems.

### 4.2 Cross-functional self-managing groups

The exercise in organization B was prepared by a group of three managers: of IT security, control systems, and the control room. The former had participated in a similar exercise before. The goal of the exercise was to practice collaboration between the departments of industrial control and IT systems. The subgoals were to get to know persons, tasks, and responsibilities across the two involved departments and identify improvements to existing procedures for emergency preparedness and information security in general. The three managers acted as observers; one for each group of participants. They were responsible for presenting the scenario, making sure 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.

The group observers reported that in general, the group discussions were good and nobody seemed to dominate. In group 3 the control room manager took to some extent on the role as a chair person 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 on each others' competences and responsibilities as they lacked this insight in order to get the big picture. The observer in group 1 would like to see more involvement from the management level in preparedness exercises.

Each group was intended to be self-managing, with as little intervention from the group observers as possible. Reflections from the group observers indicated that it was difficult to keep quiet, as they wanted to contribute. This was particularly challenging for the observer in group 1, as this group suffered from the lack of control systems personnel, and he was the only one with this competence. He still chose to remain fairly passive. All group observers reported that they did not need to intervene in order for the discussions to keep going. They did not need to push their groups into making decisions either, as the groups were focused on solving the problems as 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 to all sub-problems.

There was some criticism to the scenario description: "It is stated here that we reinstalled (...), but we would never have done that because (...)". Some pointed out that the scenario was not realistic because of how their systems are integrated, while others found the scenario to be quite realistic.

The evaluation showed that the participants were overall satisfied with the exercise. They appreciated the opportunity to meet and get to know colleagues from other parts of the organization and to get insight into their areas of responsibilities and knowledge. The participants would have liked to have more time than 20 minutes for discussions for some of the phases. Furthermore, they

lacked the opportunity to hear how the other groups had solved the problems. A separate meeting for this was arranged a couple of weeks later. One participant suggested they use the existing preparedness plans and procedures actively during such an exercise. The group observers found the thorough evaluation process to be very valuable, and they saw it as an advantage that it was lead by an external (one researcher) as it made the participants put extra effort into contributing.

### 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 awareness raising and practice in responding to IT security incidents that occur in the control systems. The participants were seated around one big table. Five representatives from the Emergency Management Team were present during the introduction. Three of them left the room when the scenario was presented, while two chose to stay as passive observers. The intention was that the complete Emergency Management Team should be called for at a later phase of the scenario, when the seriousness of the incident required them to be involved, in order to resemble 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 reporting to other stakeholders in the organization. One issue that was thoroughly discussed, was the reporting from IT to the control room: when would that be done, if at all; is this relevant information for the control room staff; and is this reporting line documented. This was identified as a lack in the documented procedures when one participant checked these during the discussion. The group still knew who to contact. Another issue that received a lot of attention, was the question of shutting down 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 malware infections spreading further into the systems. The control system manager on the other hand claimed that shutting down the control systems has extensive 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. They still concluded that the situation was resolved satisfactorily in this exercise, and that they would be able to maintain power production and distribution by manually operating power stations. The facilitators felt that relevant assessments and decisions were made, and that the Emergency Management Team was involved at the right points in time. The Emergency Management Team contributed with thorough analyses and unambiguous decisions.

## 5 Discussion

We have described a tabletop exercise as performed in three organizations. While they all relied on the same scenario, they organized the exercise differently. In the following we discuss the importance of preparedness exercises, along with our results in the light of our research question: *What are the challenges of performing tabletop exercises for IT security incidents?* Then we discuss how observed challenges could affect a real-life incident response process. Finally, we provide recommendations for how to succeed with preparedness exercises.

Our study confirmed the importance of conducting preparedness exercises. In organization A they realized that in a real situation they would most probably not be able to link the third phase to the first two, i. e. events that occur three months apart. By training they became aware that such links exist. Further, the participants in organization B were not sufficiently aware of each others' needs for information. They realized how the information flow could be improved. In two of the organizations in our study, A and B, the participants had different views on whether the scenario was realistic or not. This difference shows a need for developing a common perception of possible threats and potential consequences, which can be partly achieved by performing exercises.

A single best practice on organizing tabletop exercises does probably not exist. However, we found a number of challenges that need to be understood in order to succeed with such training.

**Having one goal only.** For a team to have good performance and to be able to effectively solve a complex problem, they need shared understanding of the team goals [21]. Having several goals for the exercise might lead to the individual members heading 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 they had problems staying focused during the exercise. The main goal of an exercise should be to solve the problem, while additional goals may rather be aimed for during the evaluation afterwards, as was done in organization B.

*Recommendation:* Define only one main goal for the preparedness exercise.

**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 share decision authority jointly, 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. 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 who are part of the team and who are not.

Enabling self-management further requires the group to have the necessary competence; otherwise the group will be training for solving the problem without

having the necessary competence available. However, because handling incidents is creative work, it might be challenging to identify everyone that should be present in the training up front. One of the teams in organization B clearly suffered from the lack of competence, and both organizations B and C lacked personnel from their external suppliers. The training outcome would have been better with the right personnel present.

In addition to the right competence, a shared understanding of who knows what is needed to solve a crisis effectively [16]. We found that in most teams people did not have a good overview of what the others knew, however, the team members became more aware of each others' knowledge during the exercise.

*Recommendation:* Ensure the presence of all required competence in the team, including personnel from external suppliers. Make it explicit who are part of the team and who are observers. Include a facilitator to support the team in making joint decisions and conduct exercises frequently to develop a shared understanding of who knows what.

**Availability of personnel.** Business runs continuously and might require sudden and unforeseen actions, which in turn might cause personnel to cancel their presence in the exercise. This will affect the group composition as happened in organization B, where last minute changes led to the lack 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 have 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. Hence, sudden absence of critical competence might be experienced during a real-life incident as well.

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

**Time management.** Having 20 minutes for discussing each phase was perceived as too short for some, while sufficient for others, depending on both the participants and the complexity of the given problems. Creating a time-pressure for making quick decisions was understood as making the exercise more realistic. Still, according to FEMA [9] 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. Further, making time for thorough reflections after the exercise is important to improve the benefits of the exercise, as was also recommended by NIST [6]. Both organizations A and B spent 60-70 minutes on such reflections and stated that one large benefit was that of having an external facilitator for this, 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 a thorough evaluation after the exercise. A short around-the-table discussion was performed.

*Recommendation:* Ensure time pressure by limiting the time for problem-solving in the exercise. Allow for thorough reflections in a plenary session right after the exercise is completed. If there is more than one group, add time for reflection within each group as well, before the plenary session.

**Use of existing documentation.** None of the teams actively consulted written plans and procedures during the exercise. 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. An organization therefore needs to rely on the individuals and their knowledge when handling a crisis. In organization C, a lack in the reporting procedures was identified, but the participants still knew who to contact and when. It was stated that in an emergency situation there is no time for consulting documentation. Exercises contribute to develop practical knowledge and the knowledge of who knows what, which is essential to make good decisions when handling an incident. Still, documentation would be available during a real situation, therefore it should also be available during an exercise. One of the main goals with a tabletop exercise is to review plans and procedures [9], and this should be performed shortly after the exercise.

*Recommendation:* Make existing written documentation available during the preparedness exercise and review the documentation in retrospective if needed. If the available documentation is not consulted, discuss why.

**Involvement of business management.** It is essential to involve those with the authority to make decisions influencing business operations. IT security involves more than IT personnel, as an incident might have severe consequences for both 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 continuously as possible. However, there are different strategies that may be used for this: to resolve the incident with as little disturbances to the operations as possible, to understand why the incident occurred, or to make sure 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 seemed to succeed with their model where the team called for the Emergency Management Team when severity of the incident required them to. In organization C the IT personnel wanted to shut down the control systems quite early, due to their fear of malware infections; the control room manager wanted to wait, due to high costs of manual operations. These costs were compared to the consequences of an uncontrolled breakdown. We found that priorities among different parts of the organization vary, which supports the need for collaborative exercises and practicing joint decision-making, at the same time as different authority levels come into play.

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

## 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 need to collaborate: IT, control systems, control room, networks/infrastructure, and business representatives. These groups of personnel do not have a tradition for collaborating with each other, as industrial control systems used to be isolated from administrative IT systems. 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.

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 to be aware of, as identified in our study. Functional exercises should be performed as a supplement to tabletop exercises in order to improve the operational capabilities as well.

We studied organizations doing such exercises for the first time. There is therefore a need to study which challenges are met by organizations that are more mature when it comes to performing preparedness exercises for IT security incidents. Such a study should also investigate what good practices these organizations are performing in their exercises. Further, challenges met during real-life incident response processes should be investigated, in order to make preparedness exercises even more useful.

## Acknowledgments.

The authors would like to thank the three DSOs that participated in this study, and Senior Research Scientist Martin G. Jaatun, SINTEF, and Professor Poul E. Heegaard, NTNU, for providing valuable feedback. This work was funded by the Norwegian Research Council through the *DeVID* project, grant no 217528, and by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure.*

## References

1. Hollnagel, E.: The four cornerstones of resilience engineering. In Nemeth, C.P., Hollnagel, E., Dekker, S., eds.: Preparation and Restoration, Resilience Engineering Perspectives. Volume 2 of Ashgate Studies in Resilience Engineering. Ashgate Publishing, Ltd. (2009)
2. Line, M.B.: Why securing smart grids is not just a straightforward consultancy exercise. Security and Communication Networks **7**(1) (2013) 160–174
3. Batchelder, D., Blackbird, J., Felstead, D., Henry, P., Jones, J., Kulkarni, A.: Microsoft Security Intelligence Report. Microsoft (2014)
4. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Information security incident management: Planning for failure. In: 8th International Conference on IT Security Incident Management and IT Forensics (IMF). (May 2014) 47–61

5. Line, M.B., Zand, A., Stringhini, G., Kemmerer, R.A.: Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared? In: 21st ACM Conference on Computer and Communications Security and Co-located Workshops. (November 2014) 13–22
6. Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., Good, T.: NIST SP 800-84: Guide to Test, Training and Exercise Programs for IT Plans and Capabilities. National Institute of Standards and Technology (2006)
7. NVE: Øvelser: En veiledning i planlegging og gjennomføring av øvelser i NVE (in Norwegian). Norwegian Water Resources and Energy Directorate (2013)
8. Hale, A., Borys, D.: Working to rule, or working safely? Part 1: A state of the art review. Safety Science (2012)
9. FEMA: IS 139 Exercise Design – Unit 5: The Tabletop Exercise. Federal Emergency Management Agency – Emergency Management Institute (FEMA)
10. Gåsland, S.: Gjør øvelse mester? Om læringsfaktorer i beredskapsøvelser initiert av NVE (in Norw.). Technical report, University of Oslo (2014)
11. Hove, C., Tårnes, M., Line, M.B., Bernsmed, K.: Information security incident management: Identified practice in large organizations. In: 8th International Conference on IT Security Incident Management and IT Forensics (IMF). (May 2014) 27–46
12. Rykkja, L.H.: Kap. 8: Øvelser som kriseforebygging. In: Organisering, samfunnssikkerhet og krisehåndtering (in Norw.). 2 edn. Universitetsforlaget (2014)
13. Malone, T.W., Crowston, K.: The Interdisciplinary Study of Coordination. ACM Computing Surveys **26**(1) (March 1994) 87–119
14. Okhuysen, G.A., Bechky, B.A.: Coordination in Organizations: An Integrative Perspective. The Academy of Management Annals **3**(1) (2009) 463–502
15. Kraut, R.E., Streeter, L.A.: Coordination in Software Development. Communications of the ACM **38**(3) (March 1995) 69–81
16. Lewis, K., Herndon, B.: Transactive Memory Systems: Current Issues and Future Research Directions. Organization Science **22**(5) (September 2011) 1254–1265
17. Lundberg, N., Tellioğlu, H.: Understanding Complex Coordination Processes in Health Care. Scandinavian Journal of Information Systems **11**(2) (July 1999) 157–181
18. ISO/IEC: ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management (2011)
19. Hackman, J.R. In: The psychology of self-management in organizations. American Psychological Association, Washington, D. C. (1986)
20. Yin, R.K.: Case Study Research - Design and Methods, 4th ed. Volume 5 of Applied Social Research Methods. SAGE Publications (2009)
21. Moe, N.B., Dingsøyr, T., Dybå, T.: A teamwork model for understanding an agile team: A case study of a scrum project. Information and Software Technology **52**(5) (2010) 480 – 491