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

Maria Bartnes[a,b,1,2,*], Nils Brede Moe[b], Poul E. Heegaard[a]

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

Abstract

Recent attacks and threat reports indicate that industrial control organizations are attractive targets for attacks. Emerging threats create the need for a well-established capacity for responding to unwanted incidents. Such a capacity is influenced by organizational, human, and technological factors. We have conducted extensive fieldwork for 2.5 years in Norwegian electric power companies with the aim of identifying challenges for improving information security incident management practices. Semi-structured interviews, document analysis, a survey and participant observations have been performed as part of this case study.

We describe how training for responding to information security incidents is given low priority and that different types of personnel, such as business managers and technical personnel, have different perspectives and priorities in regard to information security. Moreover, there is a gap in how IT staff and control system staff understand information security. Furthermore, *cross-functional teams* need to be created to ensure a holistic view during the incident response process.

To improve the capacity for responding to incidents, organizations need regular training sessions and systematic evaluations after such sessions. There is also the potential for improvement in evaluating minor incidents. A transition from an ad hoc approach to a systematic approach in training and learning requires a reorientation not only by the electric power companies but also by management. We found that *learning to learn* will enable the organizations to improve their incident response practices.

[*] Corresponding author
Email addresses: `maria.bartnes@item.ntnu.no` (Maria Bartnes), `nils.b.moe@sintef.no` (Nils Brede Moe), `poul.heegaard@item.ntnu.no` (Poul E. Heegaard)
[1] Tel.: +47-45218102, Fax: +47-73593350

[2] This work has mainly been funded 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 grants no 217528 (DeVID).

Keywords: Information security, Incident management, Incident response, Cross-functional teams, Learning to learn

1. Motivation and Objectives

Emerging information security threats create the need for a structured capacity for responding to unwanted incidents. Such a capacity is influenced by organizational, human, and technological factors. Benefits from a structured approach to information security incident management include an overall improvement in information security, reduced impact of incidents, improved focus and better prioritization of security activities, and better and more updated information security risk assessment efforts (ISO/IEC, 2011; Cusick and Ma, 2010).

Basic structures are needed, such as well-documented procedures and clear definitions of roles and responsibilities. However, during an incident there is a need for a more dynamic process that requires coordination and improvisation, where exceptions and violations are managed and experienced incident handlers are valued. Therefore, personnel who will be involved in responding to incidents that may compromise business operations require training.

Industrial control systems will undergo major technological changes in the near future (ERCIM, 2015). There is a lack of research and experiences related to incident response in such environments (NIST, 2010), hence there is a need for investigations in this area. A study of current practice and challenges is needed to identify potential improvements. This work was guided by the following research question:

[Table 1 about here.]

We have conducted an empirical study of current practices for information security incident management in Norwegian electric power organizations. The level of cyber situation awareness was surveyed to analyze their level of preparedness for targeted attacks. Furthermore, we investigated which challenges were met during preparedness exercises for information security incidents.

This paper is structured as follows: Section 2 presents background and related work. Research methods and the industrial case context are introduced in Section 3. Section 4 describes our findings, while Section 5 discusses these findings in light of the research questions and proposes implications of the results for both practice and research. Finally, Section 6 provides the study's concluding remarks.

2. Background

The purpose of information security incident management training is to strengthen the capabilities of an organization in responding to incidents that may compromise business operations (ISO/IEC, 2011). Involved personnel need to be familiar with the overall information security incident management process.

Training involves cooperation, coordination, and technical expertise. Human factors in incident management are described below as principles from the area of resilience engineering, and the relation between the incident management process and resilience engineering is discussed. Furthermore, specific attention is given to cyber situation awareness and preparedness exercises as means of enhancing the incident management process, as well as the importance of coordination in incident response teams, including the issues of making decisions and sharing knowledge. In the following, we will introduce the concepts of information security management and preparedness exercises, resilience engineering, cyber situation awareness, and coordination in incident response.

2.1. Information security preparedness tabletop exercises

Tabletop exercises are discussion-based exercises. They are usually performed in a classroom setting without the use of any specific equipment, and a facilitator presents a scenario and initiates the discussion (Grance et al., 2006). Tabletop exercises 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 (Grance et al., 2006). Functional exercises, alternately, involve practical simulations of incidents with the use of physical equipment and the execution of procedures, such as alerting and reporting. Both tabletop exercises and functional exercises prepare personnel for responding to an incident (Grance et al., 2006). Exercises provide a means for personnel to train for making the right decisions under pressure (Hollnagel, 2009). Wrong decisions may cause the incident to escalate and lead to severe consequences. According to National Institute of Standards and Technology (NIST) (Grance et al., 2006), both types of exercises should consist of the following four phases:

- *Phase I: Design* the event by identifying objectives and participants,
- *Phase II: Develop* the scenario and guides for the facilitator and the participants,
- *Phase III: Conduct* the exercise, and
- *Phase IV: Evaluate* by debriefing and identifying lessons learned.

Tabletop exercises and functional exercises supplement each other: tabletop exercises do not provide practical demonstrations of the effects of an incident or the emergency management's true response capabilities (FEMA, 2003), while this is exactly what is supported by functional exercises.

Creating realistic scenarios for training (Hove et al., 2014) and making sure that the right people perceive the exercise as relevant are challenging, and even though an exercise is based on a realistic scenario, there are no guarantees that a real incident will be successfully responded to (Rykkja, 2014).

2.2. Information security incident management

A number of standards and recommendations describe the information security incident management process: ISO/IEC (2011), NIST (Grance et al., 2008), ITIL (Brewster et al., 2012)[3], and ENISA (2010)[4]. They provide a useful baseline for organizations about to implement their own scheme or looking for inspiration for improvements. ISO/IEC 27035 should be regarded as the most comprehensive and internationally recognized documentation of what is currently the recommended practice in this field, as it is consensus-based and developed by independent non-governmental and non-profit organizations (ISO[5] and IEC[6]). The standard is therefore used as a basis for the interview studies performed in our work. It describes the incident management process in five phases, as illustrated in Figure 1:

- *Plan and prepare* includes activities such as establishing a dedicated response team, defining roles and responsibilities, and documenting procedures, as well as training of personnel and awareness raising activities regarding incident management throughout the organization.
- *Detection and reporting* is the first operational phase of incident management and involves detection of what might be an incident and reporting into an incident tracking system.
- The *assessment and decision* phase decides what type of response is needed to cope with the registered event.
- The *responses* phase describes the actions taken to cope with the incident and prevent further consequences, restore systems, collect electronic evidence, and possibly escalate to crisis handling.
- In the *lessons learned* phase, the team analyzes whether the incident management scheme worked satisfactorily and considers whether any improvements are needed on any level: the scheme, policies, procedures, security mechanisms, or similar aspects. The improvements are then implemented as part of the continuously running phase of *plan and prepare.*

[Figure 1 about here.]

A few studies have identified practices and challenges related to the one or more phases of the incident management process. An efficient and effective approach for incident management is achieved through a successful combination of various reporting capabilities, automatic analysis and response, and process-oriented intervention (Metzger et al., 2011). Findings by Ahmad et al. (2012)

[3] ITIL: Information Technology Infrastructure Library

[4] ENISA: European Union Agency for Network and Information Security

[5] ISO: The International Organization for Standardization

[6] IEC: International Engineering Consortium

indicated that the incident management process tends to have a narrow technical focus, where maintaining continuous operation was the main goal, while strategic security concerns tended to be neglected. Furthermore, according to the same study, post-incident review processes tended to focus more on incidents with high impact than so-called “high learning” incidents, i.e., incidents that have the potential to be more useful from a learning perspective rather than having major consequences. Scholl and Mangold (2011) claimed that a “well-developed incident response process should be a driver for continuous improvement of enterprise security” and that attending to small security events and early warnings can prevent major security disasters.

Incident responders need a set of skills comprising pattern recognition, hypothesis generation, and cooperation (Werlinger and Botta, 2007). Moreover, incident response is a highly collaborative activity, and the diagnostic work is complicated by the practitioners’ need to rely on tacit knowledge, as well as usability issues with security tools (Werlinger et al., 2010).

2.3. Resilience engineering

Resilience engineering concerns an organization’s ability to succeed under varying conditions, which includes efficient response to both information security incidents and other unexpected disturbances. It is usually explained by four principles (Hollnagel, 2009), as illustrated in Figure 2:

- *Actual:* The ability to address the *actual* is knowing what to *do* and being able to respond to changes and disturbances in an effective and flexible matter.
- *Factual:* The ability to address the *factual* is knowing what has *happened* and being able to learn from past events and understand correctly what happened and why.
- *Critical:* The ability to address the *critical* is knowing what to *look for* and being able to monitor what can be a threat or cause disturbances in the near future.
- *Potential:* The ability to address the *potential* is knowing what to *expect* and being able to anticipate developments, threats or opportunities in the future and imagine how they can affect the organization through changes or disruptions.

[Figure 2 about here.]

Figure 2 illustrates how the basic abilities of resilience relate to the information security incident management process. Knowing what to expect (anticipation: the potential) is a result of the plan and prepare phase, where the situation awareness (Section 2.4) is developed through preparedness exercises (Section 2.1). In the detection and reporting phase it is important to know what to look for (monitoring: critical) as an input to the responding phase (defining what to do, which responses to take), combined with the results of the learning phase (where coordination is essential; see Section 2.5).

The degree to which an organization is resilient is determined by how well these four abilities are established and managed. A resilient organization is prepared to deal with the unexpected and able to adapt to the occurring situations. Resilience is an immanent property that must be developed over time.

In spite of the need for individual planning for each organization, training is a common key factor in regard to improving resilience. The more experienced each worker is in anticipating and responding to incidents, the better prepared they will be for recognizing and responding to unexpected events. In fact, Pariès (Hollnagel et al., 2011) states that it takes "a subtle balance between experience and opportunism, self confidence and awareness of limitations" to succeed in extreme situations.

2.4. Cyber situation awareness

The concept of cyber situation awareness relates to the field of resilience engineering as both regard the ability to understand the current situation, potential changes, and consequences thereof. When technology fails, the human factor is of great importance. Human system operators must be able to interpret alerts, put pieces of information together, know about possible attacks and understand their consequences. This ability is referred to as Cyber Situation Awareness (CSA) and can, to some degree, be supported by automatic tools. According to Barford et al. (2010) situation awareness can generally be described as a three-phase process: situation recognition, situation comprehension, and situation projection. Tadda (2008) provides an overview of metrics developed for measuring the performance of cyber situation awareness systems. He specifically points out the need for research on measuring the level of situation awareness achieved by human operators, which he indicates as being significantly different from measuring the performance of a computer system. Cyber situational awareness for industrial control systems, and the power grid in particular, has received attention lately (Franke and Brynielsson, 2014). Research areas include frameworks that comprise collection and analysis of network traffic data, simulation systems, and intrusion detection systems. One example is Klump and Kwiatkowski (2010), who proposed an architecture for sharing information about incidents in the power system.

2.5. Coordination in incident response

Coordination of work and making collaborative decisions are important aspects of the incident response process and hence also of preparedness exercises. Responding to an information security incident usually implies the collaboration of personnel from different parts of an organization collaborating to solve complex problems. "Coordination is management of interdependencies between activities" (Malone and Crowston, 1994) and coordination mechanisms are the organizational arrangements that allow individuals to realize a collective performance (Okhuysen and Bechky, 2009). Interdependencies include sharing of resources, synchronization of activities, and prerequisite activities. Coordination challenges in incident response are functions of the complexity of the processes and technology.

Furthermore, responding to an information security incident is creative work, as there might not be one correct solution, and a number of uncertainties and interdependencies need to be taken into account. In creative work, progress towards completion can be difficult to estimate because interdependencies between different pieces of work may be uncertain or challenging to identify (Kraut and Streeter, 1995). 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 (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, 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. The successfulness of a TMS depends on the degree to which a team's knowledge is differentiated. Differentiated group knowledge is thought to be useful because it provides the group with diverse, specialized knowledge that can be applied to the group's task.

Coordination can be either predefined or situated (Lundberg and Tellioğlu, 1999):

- *Predefined coordination* takes place prior to the task being coordinated. It typically consists of establishing written or unwritten rules, routines, procedures, roles, and schedules; thus, it resembles an incident response scheme as described by ISO/IEC 27035 (ISO/IEC, 2011).

- *Situated coordination* occurs when a task is unknown and/or unanticipated, such as when an information security incident strikes. Those involved in the task 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 conducted, 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 mix of predefined and situated coordination. Involved actors may, for instance, already know the goal but not who does what or they may know who does what, but not when to do it. To compensate for the lack of predefined knowledge of how the activities in an exercise will actually unfold, the participants must update themselves on the status of the task.

When preparing to handle an incident, not only does a response team need to understand how to coordinate their work, they also need to understand how to make decisions together, and how to manage and monitor their own processes and execution of tasks; they need to be able to self-manage (Hackman, 1986). Training is essential for developing mutual understanding and a shared mental model (Floodeen et al., 2013), which will increase the performance during an incident handling process because the team will be better prepared to cooperate with limited and efficient communication.

3. Research Method

In our case study (Yin, 2009), we applied exploratory research with a flexible design (Robson, 2011). We used an *inductive research approach* as we wanted to derive patterns from our observations rather than evaluating existing hypotheses. The study combined qualitative, semi-structured interviews (Myers and Newman, 2007; Cassell and Symon, 2004; Robson, 2011), with document analysis (Yin, 2009) and participant observation (Robson, 2011). In the following, we introduce the context of our case study before we describe the data collection and analysis process further.

3.1. Industrial case context

The electric power industry is currently implementing smarter distribution grids. This implies a closer integration with IT systems and results in what can be referred to as *cyber physical systems-of-systems* (CPSoS) (ERCIM, 2015). In CPSoSs, there are strong interdependencies with high autonomy and complexity in the technical ”system-of-systems” itself, in the interactions between them, and in the global operation of them. New functionalities, such as monitoring, automatic failure detection, and remote control, will be implemented into electric power distribution grids, supporting more efficient operation and partially autonomous management. The technological changes introduce threats and vulnerabilities that make the systems more susceptible to both accidental and deliberate information security incidents (Line et al., 2011), as well as new dependability challenges and networked risks (Helbing, 2013). The electric power grid is considered a critical infrastructure in Norway, as a large part of the power consumption is based on electricity. As industrial control systems are used for controlling crucial parts of this critical infrastructure, incidents may have catastrophic consequences on our physical environment in addition to major costs for the organizations that are being hit (Anderson et al., 2012).

Well-known attacks, such as Stuxnet/Duqu/Flame (Albright et al., 2010, 2011; Falliere et al., 2011; Perlroth, 2012), NightDragon (McAfee, 2011), and the cyber espionage campaign by Dragonfly (Symantec, 2014), as well as statistics presented by ICS-CERT (2013), demonstrate that industrial control organizations are attractive targets for attacks. According to these statistics, 59% of the incidents reported to the Department of Homeland Security in 2013 occurred in the energy industry. ICS-CERT (2013) expresses an explicit concern for vulnerable control systems being accessible from the Internet and for unprotected control devices. Hence, technological changes in industrial control systems pose new challenges to the industry. It is, however, worth noting that the reported incidents do not only occur in the control systems. Other parts of the organizations are also susceptible to attacks, e.g., for exfiltration of sensitive information. Research on information security incident management in environments with co-functioning IT systems and industrial control systems is currently limited (Tøndel et al., 2014). Therefore, there is a knowledge and understanding gap for both current practices and related challenges for incident management in such environments, as well as compliance to standards and/or the need for changes in standards. We will particularly investigate issues related to knowledge and understanding and communication and collaboration between IT staff and control system staff in the participating organizations.

Our case study was carried out in four steps, as shown in Table 2. In total, seven large and three small Distribution System Operators (DSOs) participated. The large DSOs are among the top 15 largest DSOs in Norway with respect to the number of energy customers, and they all serve close to 100,000 customers or more. The small DSOs serve less than 10,000 customers each. There are approximately 150 DSOs in Norway in total, and the majority of them have a few thousand customers.

Four of the large DSOs have outsourced the operation of IT systems and networks to an external supplier, while the remaining two operate these inhouse. The three small DSOs rely on an external supplier as well. All the DSOs have dedicated personnel for maintaining their control systems. In addition, they all have a service agreement with their supplier for the control systems, which includes assistance in case of failures, annual reviews of the systems, and critical patches whenever necessary.

[Table 2 about here.]

3.2. Data collection and analysis

For the investigation of the *current practice* for information security incident handling, semi-structured interviews were conducted in combination with a review of the documentation for existing plans and procedures and evaluation reports from past incidents. Our interview guide was based on ISO/IEC (2011). We interviewed personnel with the following roles in each organization: IT manager, IT security manager and control room manager. In the small DSOs, the IT manager was also responsible for information security. In total, 19 interviews in six large and three small DSOs were conducted. The data analysis followed an integrated approach (Bogdan and Biklen, 1982; Lofland, 1971). The list of categories for metadata encoding was based on the five phases of ISO/IEC 27035, cf. Figure 1. The results from this step of our case study were published by Line et al. (2014b) and Line et al. (2015).

Semi-structured interviews were conducted in our investigation of *information security awareness* for industrial control systems as well. This interview guide was based on a categorization of elements comprising cyber situation awareness (CSA). One fellow researcher and one expert from a control system vendor assisted in evaluating the questions. The interview guide was distributed to the interviewees in advance. This was to ensure that we interviewed the right persons and to give them the possibility to prepare for the interview (discuss with colleagues, consult documentation, and collect information) in advance to improve the quality of our data material. IT security managers for the control systems were asked to participate. Both group and individual interviews were conducted; six interviews in total, in the large DSOs that participated in the first phase of the case study as well. For the data analysis, the first author, who performed the interviews, wrote a summary of each interview. Fellow researchers participated in discussing the results, and said results were published in Line et al. (2014a).

The interviews in our case study were carried out before the Dragonfly attack in 2014 (Symantec, 2014), which targeted Norwegian electric power operators. We therefore conducted an additional mini-survey, consisting of three questions sent by e-mail to each of the DSOs participating in the interview studies. The purpose was to investigate how this attack affected information security efforts in the companies, independent of whether they were hit by this attack or not. Six out of nine DSOs responded.

A holistic multiple case study (Yin, 2009) was performed for our investigation of *tabletop exercises*. We contributed to planning of the tabletop exercises in each of the organizations and acted as a participant observer (Robson, 2011) studying leadership, decision-making, and involvement. Furthermore, we facilitated a plenary evaluation after the exercise for reflections among the participants as shown in Figure 3. This evaluation was organized as a brainstorming session where all participants reflected upon what worked well and what could have been done differently. Three DSOs were studied, and they all used the same scenario as a basis for their exercise, although they organized the exercise slightly differently from one another. The participants did not receive any information about the exercise in advance other than that the topic of the tabletop exercises would be an information security incident. For the data analysis, we described the tabletop exercises and evaluations to achieve an understanding of what was going on during the exercises. Interesting expressions and observations were categorized, and findings from the different organizations were compared. This analysis was performed and published by the first and second authors (Line and Moe, 2015).

[Figure 3 about here.]

Results from each of the four steps of this case study have been presented in research papers before, as referred to above. However, the former papers were primarily focused on surveying current practices for incident management and preparedness exercises, while this paper takes on a different approach in synthesizing the data material based on a new research question that regards challenges for improving current practices. Hence, the discussion results from analyzing findings in light of this research question and has previously not been published.

3.3. Privacy and confidentiality issues

The case study was registered at the Data Protection Official for Research[7]. All interviews were voice recorded and transcribed, and the NVivo tool was used for coding and analysis of the data material.

[7] Personvernombudet for forskning, www.nsd.uib.no/personvern/en/index.html. Equivalent to the US Institutional Review Board (IRB)

Confidentiality issues prevented three DSOs from sharing documentation, and non-disclosure agreements and encrypted electronic transfer were not sufficient instruments to overcome these issues.

4. Findings

In this section, we present the main findings from our studies. The lack of major incidents experienced by the participating organizations (at the time of our study) resulted in little focus or priority being given to training and exercises. Hence, coordination is not improved, and different views and understandings of threats and vulnerabilities are maintained. Further, insufficient attention is given to post-evaluations of minor incidents, which implies that no systematic procedures are defined or exercised for either minor or major incidents. Figure 4 highlights the relationships between the identified challenges for improving incident management practices.

[Figure 4 about here.]

4.1. The absence of major incidents limits preparatory activities

The level of preparedness and the priority assigned to incident management planning and preparatory activities among DSOs were limited, particularly compared to the recommendations by ISO/IEC 27035 [P6, P7]. The feedback from the DSOs was that no major information security incidents had been observed that had disturbed their business operations. In general, they did not feel the need to realize major improvements to their incident management practices.

The DSOs have experienced few incidents so far. One malware infection in one part of the control systems and a number of minor malware incidents in administrative systems were reported in the interviews, but they have been manageable (Line et al., 2014b). Although the respondents had a realistic view of potential attackers and possible threats (Line et al., 2014a), one of the large DSOs stated:

> *"As long as there has been no major attacks against the power industry in Norway, we consider the probability of an attack to be low. As soon as something happens, we will consider the probability to be increased."*
>
> *– Control manager in a large DSO*
> *(before the Dragonfly attack)*

The above statement indicates that systematic approaches to several incident management activities will remain lacking as long as things go well.

After the Dragonfly attack in 2014 (Symantec, 2014), top managers were more concerned about information security incidents and preparedness exercises in particular. All respondents in the mini-survey answered that they would be able to respond appropriately to such an attack, although it would depend on the complexity of the attack and how quickly the attack was detected. After this attack, preparedness exercises for information security incidents were given higher priority, reviews of documentation were performed, and the understanding of threats and of the importance of monitoring and analysis of incidents was improved.

4.2. Training for information security incidents is not prioritized

Training for information security incidents is considered less important than a number of other everyday tasks, even though tacit knowledge and experience are more relied on than documented plans during an incident (Line et al., 2014b). Training involves a certain cost, time, and workload, which are perceived as hindrances. Moreover, protecting the physical grid and the production process from fire and other physical damages is viewed as more important than protecting the IT systems. Finally, real incidents rarely occur, which adds to the perception of training not being prioritized, even though information security policies require regular tests of emergency preparedness plans, including IT/infrastructure issues (Line et al., 2014b).

> *"There are too many other tasks, so we haven't had the time for it. Maybe that's wrong, not to prioritize it."*
>
> *— Control system manager in a large DSO*

Minor incidents occur regularly in the administrative systems, which ensures some training and, to a certain degree, keeps personnel alert. One IT security manager in a large DSO stated that "fumbling and hubbub" constituted the most useful training (Line et al., 2014b). There are, however, few incidents in the control systems, which implies that control staff does not receive this practical training through everyday work. Four out of the six control room managers in large DSOs felt that training efforts are not satisfactory (Line et al., 2014b,a)

> *"The personnel operating the control systems would benefit from training on scenarios like 'what do we do if the control systems break down?'"*
>
> *— Control system manager in a large DSO*

4.3. Deficient documentation of plans for incident management

The existence of plans for incident management varied among the DSOs. Some of the large DSOs were working on documenting such plans. They found it difficult to run preparedness exercises without having written plans as a baseline (Line et al., 2014b). In two of the three large DSOs, existing documentation of plans and procedures was not made available during the exercise. Some participants commented on this afterwards and wanted to have documentation available in the next exercise. An IT security manager in a large DSO said that they lack practice and established procedures with regard to being well prepared to respond to a worst-case scenario. He still felt confident that they would be able to improvise (Line et al., 2014b).

4.4. IT and control personnel understand information security differently

Control systems and IT systems have traditionally been operated separately, in both the electric power industry and similar industries. They have served different purposes and therefore have been subject to different security objectives. Further, while IT systems have already have been exposed to typical Internet threats for a long time, such as malware infections and deliberate hacker attacks, control systems have been run in closed networks without these types of threats (Line, 2013).

There is a knowledge and understanding gap for information security between IT and control personnel. IT and IT security managers share the understanding of what an information security incident is and were able to provide examples of such. The control room managers, in contrast, were not able to provide a clear definition, although they did mention relevant examples. All had a similar understanding of the worst-case scenarios, but control room personnel's ability to recognize an incident is questionable as they have limited understanding of and experience with technical mechanisms for incident detection and handling (Line et al., 2014b,a).

One of the first questions asked of all interviewees concerned their organization's dependency on IT. Control room managers understood this primarily as a matter of availability and reflected upon their ability to operate the power grid without the control systems functioning. The properties of integrity and confidentiality were not mentioned in relation to the control systems. IT and IT security managers considered all three properties for the administrative systems: availability for invoicing systems to ensure cash flow, integrity for backups, and confidentiality for customer databases (Line et al., 2014b).

> *"The greatest challenge is that they don't understand how IT intensive their new world will be."*
>
> *— IT manager in a large DSO*
> *(on control room operators and*
> *the future with Smart Grids)*

4.5. Post-incident evaluations are not performed

Even though all respondents stated a need for thorough evaluations, such evaluations of both preparedness exercises and real incidents are given low priority by DSOs. Several DSOs said that they perform evaluations after other types of incidents and believed they would do this after information security incidents as well. As they have not experienced major information security incidents, this assumption remains to be confirmed. However, none of the DSOs reported on using near misses and minor mishaps for learning, which Hollnagel et al. (2011) reported as being just as important as learning from failures.

> *"We are not good in post-evaluating real incidents and consider them as training exercises, we are too solution-oriented."*
>
> *— Corporate IT manager in a large DSO*

The practices for registration of information security incidents varied, although all DSOs reported to have some type of reporting of exceptions and mishaps. However, none reported having a systematic approach to information security metrics. Reports and registration could form a useful basis for evaluations, particularly in the absence of major incidents to learn from. Collaborative exercises make employees realize the need for improvements. An understanding of why the existing deficiencies have emerged, however, was not aimed for (Line and Moe, 2015). We observed that evaluation was given higher priority, and more time was assigned to this because we requested and facilitated it. In two of the DSOs, the participants put more effort into contributing than they typically would in internal evaluations, according to the internal facilitators.

4.6. Managers and technical personnel have different perspectives and priorities

When an incident occurs, the goal from a business perspective is usually to maintain business operations as continuously as possible. However, we observed that there are different strategies to be used for this: to resolve the incident with as little disturbance 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 important that the incident responders have a common understanding of the overall preferred strategy (Line and Moe, 2015).

One of the large DSOs that we observed included their Emergency Management Team in the exercise, a team consisting of business managers. Their participation revealed the difference in priorities between business managers and technical personnel. IT personnel wanted to shut down the control systems quite early in the exercise due to their fear of malware infections, while the Emergency Management Team decided to let the systems run due to the high costs of manual operations. They compared these costs to the consequences of an uncontrolled breakdown.

5. Discussion

Our findings are now discussed in light of the research question: *What are the challenges for improving information security incident management practices?* Next, the implications for both research and practice are stated before limitations are described. The findings show that there are currently two key challenges for improvement of information security incident management practices: *learning to learn* and *forming cross-functional teams.*

Different types of personnel have different understandings and views on how to assess and react to information security incidents. Business managers and technical personnel have different perspectives and priorities, and IT staff and control system staff understand information security differently. It is important to have the different perspectives present in an incident response team. Good incident response teams are formed by composing collaborative and complementary teams with team members that serve different functions in the organization, i.e., *cross-functional teams* (Pinto et al., 1993) are needed. Furthermore, an incident response team needs to be autonomous and self-managing, where the team members have the responsibility not only to execute the task but also to monitor, manage, and improve their own performance (Hackman, 1986). They need to learn how to improve their incident management activities.

However, training for responding to information security incidents is currently given low priority, and evaluations after training sessions and minor incidents are seldom performed. Because of the little focus on learning and reflection, there was little focus on improving how to reflect and learn together. In other words, they did not *learn to learn*, which would make organizations able to take advantage of training sessions and evaluations and thereby improve their incident response practices.

Figure 5 illustrates how these two key challenges relate to our main findings, which were presented in Section 4.

[Figure 5 about here.]

5.1. Creating cross-functional teams

Incident response is a highly collaborative activity (Werlinger et al., 2010) and requires cooperation of individuals drawn from various functional areas, with different perspectives, to make the best possible decisions. To create good cross-functional response teams, it is important to acknowledge that the team members might have conflicting goals. Different functional areas within an organization should possess complementary goals that are derived from a set of general organization-wide goals. Consequently, for one functional area to achieve its goals, another functional area may be required to sacrifice, or at least compromise, its primary goals. Therefore, the cross-functional team need superordinate goals for their incident response process. Superordinate goals will have a positive and significant direct effect on cross-functional cooperation (Pinto et al., 1993). The team further needs to be able to update its initial superordinate goals if the initial conditions change during the incident response process, as stated by Bergström et al. (Hollnagel et al., 2011).

The difference in understanding of information security goals that we found between IT staff and control system staff is in agreement with Jaatun et al. (2009), who studied incident response practices in the oil and gas industry. However, we did not identify any signs of mistrust between IT staff and control system staff, as Jaatun et al. (2009) found. Rather than feeling mistrust, both IT staff and control system staff admitted the need for exchanging information and learning from each other to become better at both detecting and responding to incidents.

Not only does the cross-functional team need participants from various functional areas within the organization, it also needs participation from, or communication with, suppliers. The DSOs assumed collaboration with suppliers to be well functioning but acknowledged that this should be given more attention, as common plans were rare and collaborative exercises were not performed. Collaboration on information security incident response tends to be challenging in outsourcing scenarios (Hove et al., 2014).

If a DSO is not able to establish a cross-functional team when performing a preparedness exercise, the group will be training to solve the task without having the necessary competence available. One challenge of establishing cross-functional teams for exercises is that handling incidents is creative work. Therefore, it might be challenging to identify everyone that should be present in the training up front. In addition to a cross-functional team having the right competence, the team members need a shared understanding of who knows what is needed to solve a task, such as a information security incident, effectively (Lewis and Herndon, 2011). Exercises provide a means for growing shared understanding of the team knowledge.

One challenge in having a good cross-functional team for handling incidents is that you do not always know who is available and who should be part of the team. Thus, for training, an organization needs to set up different configurations of this cross-functional team depending on the training scenario.

5.2. Learning to learn

Learning from previous incidents as well as preparedness exercises is important for improving practices for responding to incidents. Learning improves the ability to anticipate future trends and events by producing relevant understandings of what can happen in the future (Line and Albrechtsen, 2016). Motivations for learning activities include keeping security practitioners updated on current threats, getting new ideas on how to resolve challenging incidents, discussing possible improvements of incident response activities, performing trend analysis, identifying direct causes, identifying new security measures needed, and updating risk assessments (Tøndel et al., 2014). Learning from incidents should include systematic analysis, use of lessons learnt to make changes, and storing and sharing information (Line and Albrechtsen, 2016). Scholl and Mangold (2011) claimed that attending to small security events and early warnings can prevent major security disasters.

The organization needs to establish an incident learning system, which can be described as "the collection of organizational capabilities that enable the organization to extract useful information from incidents of all types and to use this information to improve organizational performance over time." Key enablers for learning from incidents are the extent of management commitment and the willingness to commit resources to facilitate learning. For management to be committed to learning, they need to have a realistic perception of actual threats and possible consequences. In our research, we found that training for incident responses and post-incident evaluations were not prioritized. One explanation is that the risk perception among the organizations in our study was found to be lower than it should be from the level of current threats. This is in agreement with the research of Rhee et al. (2012), who showed that management tends to be optimistically biased in that they underestimate their organization's vulnerability and overestimate their ability to control security threats. Our mini-survey showed that the Dragonfly attack implied increased risk perception among top managers and increased focus on preparedness exercises and learning.

A lack of post-incident evaluations could further be explained by the lack of major incidents, as organizations tend to not bother learning from low-impact incidents (Ahmad et al., 2012). A problem with focusing on learning from high-impact incidents only is that they make up just a small portion of the total number of incidents. There is a large number of incidents that have limited or no unfortunate outcomes but still could be used as learning material (Scholl and Mangold, 2011; Hollnagel, 2009; Kjellén, 2000). Systematic registration of such would provide a certain basis for evaluation and learning. False alarms should also be included in the learning process to improve incident detection accuracy. Thus, as the organizations in our study claimed not to experience major incidents, they should look more into minor incidents that occur.

> *"The ability to deal with a crisis situation is largely dependent on the structures that have been developed before chaos arrives. The event can in some ways be considered as an abrupt and brutal audit: at a moment's notice, everything that was left unprepared becomes a complex problem, and every weakness comes rushing to the forefront."*
>
> — *Pat Lagadec (1993)*

In general, there are two main obstacles to organizational learning: embarrassing and threatening issues (Argyris and Schön, 1978). Information security incidents may be embarrassing, such as malware infections caused by unauthorized or unintended use of IT systems, and threatening in the sense that the incidents are considered to be confidential. Hiding embarrassing issues or ignoring threatening issues can be viewed as *impression management*, which Morgan (2006) describes as giving the impression of being better than one actually is. These characteristics create individual and organizational behavior that is counterproductive in regard to learning from unwanted incidents.

When incidents become increasingly complex and ill-structured, the need for learning increases, but so does the difficulty in carrying out effective learning as well (Argyris, 1976). The organization needs to learn how to carry out single- and double-loop learning (Argyris and Schön, 1996). Single-loop learning is changing practices as problems arise to avoid the same problem in the future, i.e., learning how to handle one specific incident. Double-loop learning is using the problems being experienced to understand their underlying causes and then taking some action to remedy these causes. One example is understanding whatever caused the incident to occur. Single-loop learning then implies learning to improve performance at an increasing rate: *Are we doing things right when solving the incident?* Double-loop learning, in contrast, implies learning to conduct the reflection on and inquiry into the governing variables, values, and norms underlying organizational action: *Are we doing the right things when solving the incident?* According to Ahmad et al. (2012), post-incident evaluations, when performed, tend to adopt a technical focus rather than a strategic focus, which indicates single-loop learning. A structured accident analysis methodology can help identify the immediate and underlying causes, e.g., as described by Kjellén (2000), and should cover organizational and technical issues, as well as human factors.

A facilitator can promote team effectiveness by helping team members learn how to work interdependently in the specific team. The role of the facilitator is not to dictate to group members the one best way to proceed with their collaborative work; it is about helping members learn how to minimize process loss that happens in groups and how to consider how they might work together to generate synergistic process gains. The facilitators in our study had the tasks of leading their teams through the different steps of the exercise and making sure that the discussions were going well. They were also writing down ideas for future improvements with respect to both procedures or technical measures. It appears that the facilitators in our study focussed on keeping the time schedule and that their teams finished the problem solving, rather than making the team function well. This differs from the description by Hackman et al. (2000), which states that a facilitator can help the members with coordination and motivation and make the group work as a team and not as separate individuals to achieve a common performance goal, utilizing the creativity and ideas of the individuals.

5.3. Limitations

Construct validity. The interviewees' conscious or unconscious desire to make their organization and themselves look good from the outside could cause a certain bias, particularly as the topic of the interviews was information security, which tends to concern confidential business information. Our impression is that the interviewees were being honest as several of the interviewees reported weaknesses and deficiencies in a number of areas rather than a perfect situation. Some even expressed their gratitude to us for performing these studies, as it gave them an opportunity to discuss these issues internally. Being able to refer to external independent researchers strengthened their message. Technical personnel, who perform a large part of the daily tasks concerning incident management, could have provided a slightly different perspective than managers and perhaps with more details, at least on some of the questions. Further, suppliers have not been included in our studies. Their attitudes, awareness, and level of preparedness play an important role in incident response. As an alternative approach, we could have studied one or two organizations more in depth and interviewed a larger number of employees from each organization, including representatives from suppliers.

Data triangulation. Interviews, documentation, and observations were intended to provide three different views on incident management. The interviewees would describe their practice as they know it, documentation could show the planned procedures, and observations would show how they perform exercises in practice. The documentation received, however, was sparse with regard to information about incident response. Moreover, confidentiality issues prevented three DSOs from sharing documentation. As information security researchers, we appreciate such caution regarding the sharing of confidential documents, although it poses limitations to the data triangulation. Kotulic and Clark (2004) noted this challenge in obtaining sensitive data as limiting to research on information security management in general and recommended focusing on a few selected companies, which would ease the building of trust. All interviewees in our studies, and the facilitators of the exercises, were provided with a draft of the reports and hence given the opportunity to comment on the results.

External validity. Our studies are restricted to DSOs in the electric power industry in Norway. Both the DSOs and the participating interviewees were described in Section 3.

5.4. Implications for practice and research

The results from our case study have led to a number of recommendations for practice and potential directions for future research. The following recommendations for practice are proposed:

- *Preparedness exercises:* More scenarios for preparedness exercises should be developed. The newly established KraftCERT[8] in Norway (a dedicated incident response team for the electric power industry), the authorities, and individual organizations are possible creators of such scenarios. Furthermore, organizations need to create cross-functional and self-managed teams for incident response and perform exercises frequently to ensure that all possible members of this team receive training.

- *Learning:* A change of focus is needed, from learning from high-impact incidents only, which rarely occur, to improved evaluations of preparedness exercises and attention to minor incidents and near misses. More openness is needed to overcome the challenges of embarrassing and threatening issues. Double-loop learning, in addition to single-loop learning, must be targeted, as it allows the organization to understand the underlying causes of problems and initiate actions to solve them, hence ensuring a long-lasting improvement.

- *Communities of practice:* We would encourage representatives from both small and large organizations to create communities of practice for information security and for incident response in particular. KraftCERT and similar establishments in other industries have the potential to trigger such communities of practice, although both the creation and operation must be carried out by self-selected members. Sharing of knowledge and experience is valuable. For small organizations with limited in-house resources, CoPs across companies would be useful, while CoPs within single companies would strengthen internal collaborations.

- *Technical security mechanisms:* Detection and monitoring mechanisms for industrial control systems need to be improved to match the level of current and emerging threats. Technical improvements alone, however, are

[8] www.kraftcert.no

not beneficial without the strengthening of capabilities for following-up on logs and alerts as well, which requires both human capacities and automated tools. Improved detection capabilities would yield a more correct impression of what is going on in the technical systems and increase the probability of detecting attacks.

As for research, there is a need for longitudinal studies in individual organizations to investigate actual incident management practices in more depth. Our case study was based on interviews and preparedness exercises in several organizations and gave insight into general practices. Explicit observations of how personnel from different functional areas define incident management, cooperate in practice, and how they respond to minor incidents and near misses, would increase the understanding of the critical factors that affect the current practice and cause challenges for improvement.

Furthermore, there is a need to investigate in more detail how communication and collaboration related to incident response are performed with third parties, such as suppliers and authorities. They were not studied in particular in this case study, but they are part of the cross-functional teams responding to information security incidents when they occur.

Finally, more empirical studies on preparedness exercises and organizational learning should be carried out. How general preparedness exercises are performed and how they could be adapted for information security training should be investigated. Moreover, it should be investigated how the facilitator's role could be strengthened in order to increase the benefit of the exercise. Furthermore, a better understanding is needed of how to utilize minor incidents and near misses as a basis for learning.

6. Concluding Remarks

The main objective of this case study was to *understand challenges for improvements of information security incident management practices in Norwegian electric power companies* and thereby recommend a future direction for preparedness exercises and training.

Challenges for improving information security incident management practices concern the creation of cross-functional teams and learning to learn. Incident response teams should be cross-functional and self-managing; they should include individuals drawn from various functional areas, and the members should be able to monitor, manage, and improve their own performance in addition to executing a given task. Organizations need to learn how to carry out both single-loop and double-loop learning to take advantage of training sessions and evaluations and thereby improve their incident response practices.

Well-functioning incident response capabilities are an important component of the overall information security management system in an organization. Creation of cross-functional and self-managed teams, combined with the ability to learn, will ensure effective and efficient incident response in a world where information security threats are ever-changing and it is impossible to prevent all possible incidents.

References

Atif Ahmad, Justin Hadgkiss, and Anthonie B. Ruighaver. Incident Response Teams - Challenges in Supporting the Organisational Security Function. *Computers & Security*, 31(5):643–652, 2012.

David Albright, Paul Brannan, and Christina Walrond. Did Stuxnet take out 1000 centrifuges at the Natanz enrichment plant? Technical report, Institute for Science and International Security (ISIS), 2010.

David Albright, Paul Brannan, and Christina Walrond. Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report. Technical report, Institute for Science and International Security (ISIS), 2011.

R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the Cost of Cybercrime. In *11th Workshop on the Economics of Information Security (WEIS'12)*, 2012.

Chris Argyris. *Increasing Leadership Effectiveness*. John Wiley, 1976.

Chris Argyris and Donald A. Schön. *Organizational learning: A theory of action perspective*. Addison-Wesley, 1978.

Chris Argyris and Donald A. Schön. *Organizational Learning II: Theory, Method and Practice*. FT Press, 1996.

Paul Barford, Marc Dacier, Thomas G. Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, Xinming Ou, Dawn Song, Laura Strater, Vipin Swarup, George Tadda, Cliff Wang, and John Yen. Cyber SA: Situational Awareness for Cyber Defense. In Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang, editors, *Cyber Situational Awareness*, volume 46 of *Advances in Information Security*, pages 3–13. Springer US, 2010. ISBN 978-1-4419-0139-2.

R. Bogdan and S. K. Biklen. *Qualitative research for education: an introduction to theory and methods*. Allyn and Bacon, 1982. ISBN 9780205076956. `http://books.google.no/books?id=wIOcAAAAMAAJ`.

Ernest Brewster, Richard Griffiths, Aidan Lawes, and John Sansbury. *IT Service Management: A Guide for ITIL Foundation Exam Candidates*. BCS, The Chartered Institute for IT, 2nd edition, 2012.

Catherine Cassell and Gillian Symon. *Essential Guide to Gualitative Methods in Organizational Research*. Sage Publications Limited, 2004.

J. J. Cusick and G. Ma. Creating an ITIL inspired Incident Management approach: Roots, response, and results. In *2010 IEEE/IFIP Network Operations and Management Symposium Workshops (NOMS Wksps)*, pages 142–148, 2010. doi: 10.1109/NOMSW.2010.5486589.

ENISA. Good practice guide for incident management. European Network and Information Security Agency, 2010.

ERCIM. ERCIM News no 102 – Special Theme: Trustworthy Systems of Systems. The European Research Consortium for Informatics and Mathematics, June 2015. http://ercim-news.ercim.eu/en102.

Nicolas Falliere, Liam O. Murchu, and Eric Chien. W32.Stuxnet Dossier. Technical report, Symantec, February 2011.

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

Robert Floodeen, John Haller, and Brett Tjaden. Identifying a Shared Mental Model Among Incident Responders. In *7th International Conference on IT Security Incident Management and IT Forensics 2013*, pages 15–25, Los Alamitos, CA, USA, 2013. IEEE Computer Society.

Ulrik Franke and Joel Brynielsson. Cyber situational awareness - A systematic review of the literature. *Computers & Security*, 46:18 – 31, 2014. ISSN 0167-4048. doi: http://dx.doi.org/10.1016/j.cose.2014.06.008. http://www.sciencedirect.com/science/article/pii/S0167404814001011.

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.

Tim Grance, Karen Kent, and Brian Kim. NIST SP 800-61: Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2008.

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

J. R. Hackman, R. Wageman, T. M. Ruddy, and C. R. Ray. *Team effectiveness in theory and practice*. Blackwell, Oxford, UK, 2000.

Dirk Helbing. Globally networked risks and how to respond. *Nature*, 497(7447):51–59, 05 2013.

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.

Erik Hollnagel, Jean Pariès, David D. Woods, and John Wreathall, editors. *Resilience Engineering in Practice - a Guidebook*. Ashgate Publishing Ltd., 2011.

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.

ICS-CERT. ICS-CERT Monitor, Oct/Nov/Dec 2013. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.

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

Martin Gilje Jaatun, Eirik Albrechtsen, Maria B. Line, Inger Anne Tøndel, and Odd Helge Longva. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2:26–37, 2009.

Urban Kjellén. *Prevention of Accidents Through Experience Feedback*. Taylor and Francis, 2000.

R. Klump and M. Kwiatkowski. Distributed IP watchlist generation for intrusion detection in the electrical smart grid. *IFIP Advances in Information and Communication Technology*, 342:113–126, 2010.

Andrew G. Kotulic and Jan Guynes Clark. Why there aren't more information security research studies. *Information & Management*, 41(5):597 – 607, 2004. ISSN 0378-7206. doi: http://dx.doi.org/10.1016/j.im.2003.08.001. http://www.sciencedirect.com/science/article/pii/S0378720603000995.

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.

Patrick Lagadec. *Preventing Chaos in a Crisis: Strategies for Prevention, Control and Damage Limitation*. Mc Graw-Hill, 1993.

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 Eirik Albrechtsen. Examining the suitability of industrial safety management approaches for information security incident management. *International Journal of Information and Computer Security*, 24, 2016.

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. Cyber security challenges in Smart Grids. In *2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, Dec. 2011. doi: 10.1109/ISGTEurope.2011.6162695.

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.

Maria Bartnes Line, Inger Anne Tøndel, and Martin Gilje Jaatun. Current practices and challenges in industrial control organizations regarding information security incident management Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection*, 2015. ISSN 1874-5482. doi: http://dx.doi.org/10.1016/j.ijcip.2015.12.003.

J. Lofland. *Analysing social settings*. Wadsworth Pub, 1971. ISBN 9780534907211. http://books.google.no/books?id=fIOjKQAACAAJ.

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.

McAfee. Global Energy Cyberattacks: "Night Dragon". McAfee (R) Foundstone (R) Professional Services and McAfee Labs (TM), 2011.

S. Metzger, W. Hommel, and H. Reiser. Integrated Security Incident Management – Concepts and Real-World Experiences. In *Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*, pages 107–121, 2011.

Gareth Morgan. *Images of Organization*. SAGE Publications, 2006.

Michael D. Myers and Michael Newman. The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1):2–26, January 2007. ISSN 1471-7727. doi: 10.1016/j.infoandorg.2006.11.001. http://dx.doi.org/10.1016/j.infoandorg.2006.11.001.

NIST. NIST 7628-3: Guidelines for Smart Grid Cyber Security, 2010.

NVivo. NVivo. http://www.qsrinternational.com/.

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.

Nicole Perlroth. Researchers find clues in malware, 2012. http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

Mary Beth Pinto, Jeffrey K. Pinto, and John E. Prescott. Antecedents and Consequences of Project Team Cross-Functional Cooperation. *Management Science*, 39(10):1281–1297, October 1993.

Hyeun-Suk Rhee, Young U. Ryu, and Cheong-Tag Kim. Unrealistic optimism on information security management. *Computers & Security*, 31(2):221–232, 2012.

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.

F. Scholl and M. Mangold. Proactive Incident Response. *The Information Systems Security Association Journal*, 9, 2011.

Symantec. Dragonfly: Cyberespionage Attacks Against Energy Suppliers. Symantec Security Response, 2014.

George P. Tadda. Measuring performance of Cyber situation awareness systems. In *11th International Conference on Information Fusion*, pages 1–8, June 2008. ISBN 978-3-8007-3092-6.

Inger Anne Tøndel, Maria B. Line, and Martin G. Jaatun. Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45:42–57, 2014. ISSN 0167-4048. doi: 10.1016/j.cose.2014.05.003.

Rodrigo Werlinger and David Botta. Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis. *Workshop on Usable IT Security Management (USM '07)*, Jul 2007.

Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 2010.

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

List of Figures

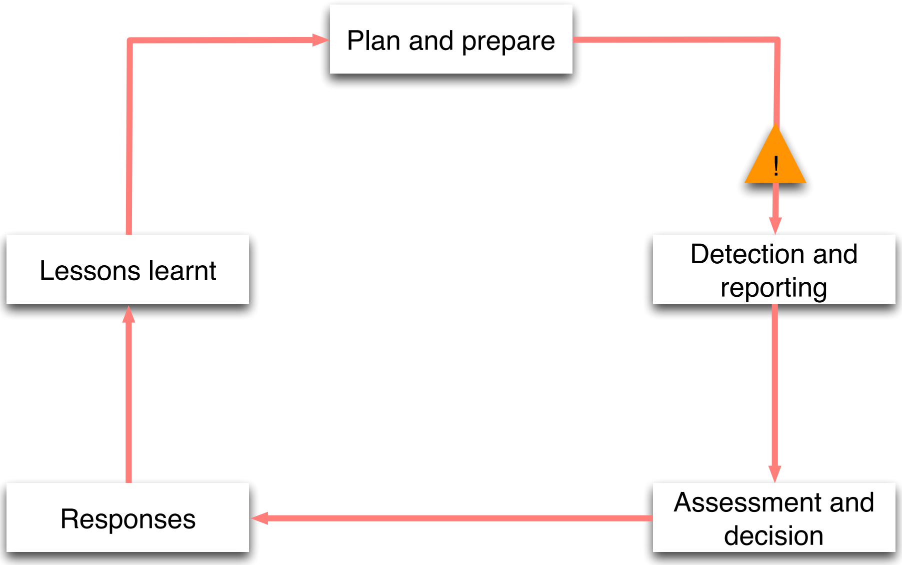

Figure 1: The information security incident management process (ISO/IEC, 2011).

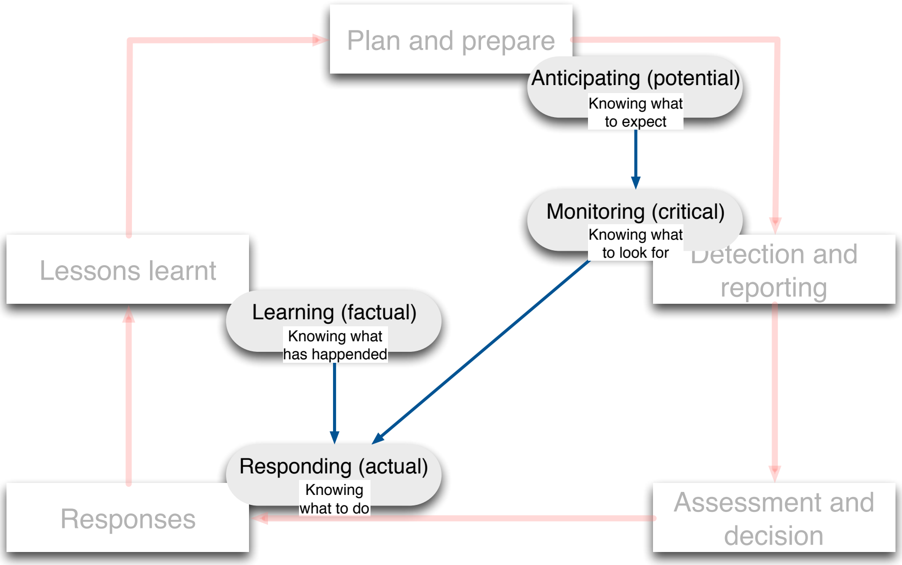

Figure 2: The four basic abilities of resilience (Hollnagel, 2009) combined with the information security incident management process (ISO/IEC, 2011).

Figure 3: Evaluating a tabletop exercise

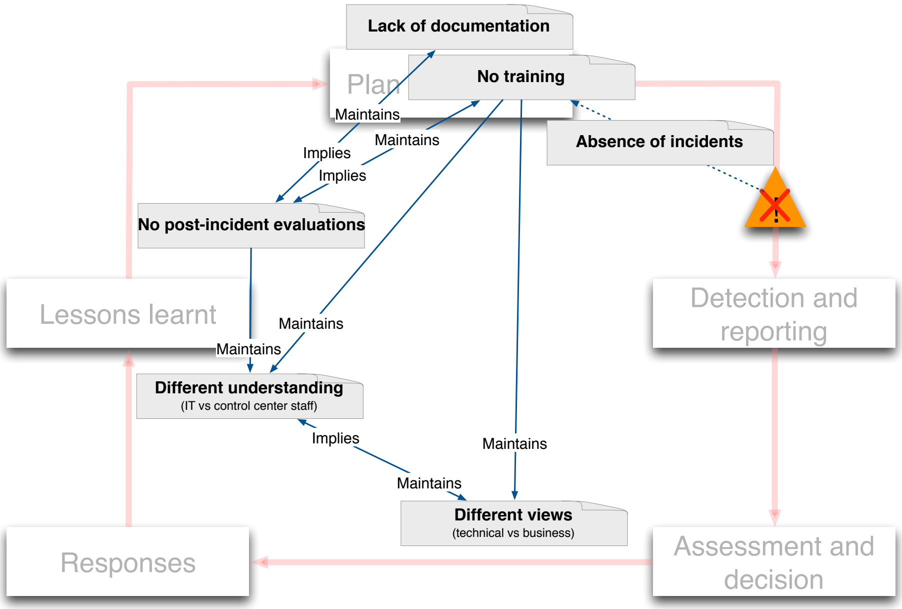

Figure 4: Challenges for improving incident management practices

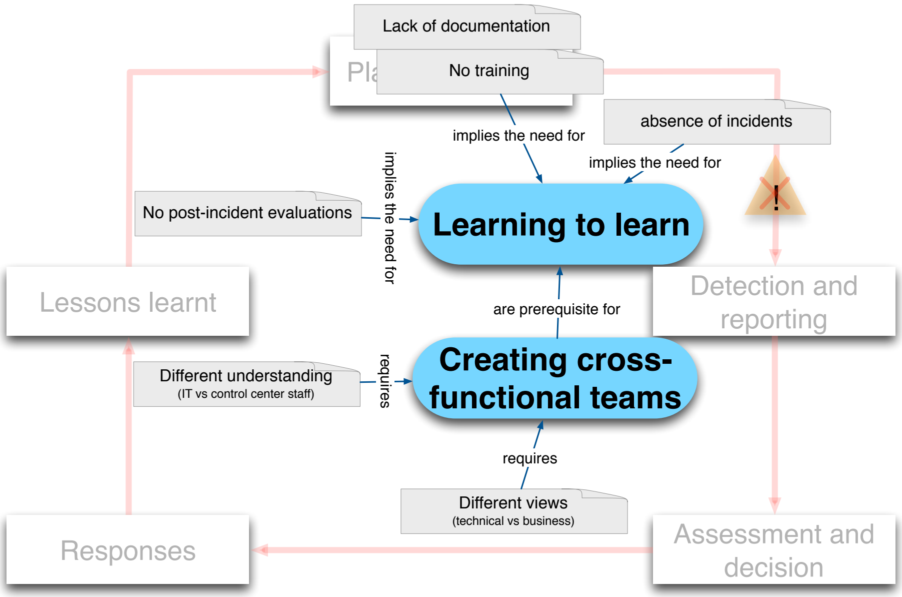

Figure 5: Relations between findings in Section 4 (in grey) and the key challenges (in blue) for improving incident management practices

List of Tables

What are the challenges for improving information security incident management practices?

Table 1: The research question for our case study

Step	When	Purpose	Data sources
1	June-Dec 2012	Current practice for both IT and industrial control	19 interviews in six large and three small distribution system operators (DSOs): IT managers, IT security managers, control room managers. Written documentation – plans and procedures.
2	Apr-May 2014	Cyber situation awareness related to industrial control systems	Six interviews (both group and individual) in the same six large DSOs as in Step 1: control room managers and/or IT security managers for control systems.
3	Nov 2014	Investigate how the Dragonfly attack affected information security efforts	Mini-survey: three questions sent by e-mail to one respondent in each of the large and small DSOs, nine in total. Six responded.
4	Oct-Nov 2014	Challenges experienced during information security preparednes exercises	Participant observation of preparedness exercises in three large DSOs; two from Step 2 and one additional large DSO.

Table 2: The four steps of our case study.