Does size matter?
Information security incident management in large and small industrial control organizations

Maria B. Line[a,b,*], Inger Anne Tøndel[b], Martin G. Jaatun[b]

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

Abstract

Through an interview study, we have surveyed current practice regarding information security incident management among large and small distribution system operators (DSOs) in the electric power industry in Norway. Our findings indicate that current risk perception and preparedness is low, in particular for small DSOs. Further, small DSOs rely heavily on their supplier should an incident occur. At the same time, small DSOs in particular are confident that they will be able to handle also worst case scenarios in their systems. This paper documents these current perceptions and discusses to what extent they are likely to hold given the transition towards smarter grids. Based on the findings and this discussion, a set of recommendations are provided. Small DSOs should strengthen the collaboration with their IT supplier and other small DSOs. DSOs in general should establish written documentation of procedures, perform preparedness exercises, and improve detection capabilities in the control systems.

Keywords: Incident management, Incident response, Industrial control organizations, Information security

1. Introduction

Industrial control organizations are currently going through a major modernization, as exemplified by the Integrated Operations in the oil and gas industry, and Smart Grids in the power industry. Functionalities such as monitoring, automatic failure detection, and remote control are being implemented in the industrial control systems, supporting more efficient operation and management. This modernization requires introduction of new technologies and leads to increased connectivity and complexity. 'Regular' IT components – hardware, firmware, software – replace proprietary solutions. These technological changes introduce threats and vulnerabilities that make the systems more susceptible to both accidental and deliberate information security incidents [1, 2]. As industrial control systems are used for controlling crucial parts of a society's

[*]Corresponding author. Tel.: +47-45218102, Fax: +47-73596973.

Email addresses: `maria.b.line@item.ntnu.no` (Maria B. Line), `inger.a.tondel@sintef.no` (Inger Anne Tøndel), `martin.g.jaatun@sintef.no` (Martin G. Jaatun)

critical infrastructure, incidents may have catastrophic consequences to our physical environment in addition to major costs for the organizations that are being hit [3].

Well-known attacks like Stuxnet [4, 5, 6] and NightDragon [7], and statistics presented by ICS-CERT [8] 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 [8] expresses an explicit concern for vulnerable control systems being accessible from the Internet and for unprotected control devices. 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, i.e., for exfiltration of sensitive information. Hence, the technological changes in the industrial control systems pose new challenges for the whole organization. These emerging threats are creating the need for a well established capacity for responding to unwanted incidents. This capacity is influenced by organizational, human, and technological factors. Benefits from a structured approach to information security incident management include an overall improvement of information security, reduced impact of incidents, improved focus and better prioritization of security activities, and better and more updated information security risk assessment efforts [9].

We have studied current practice for information security incident management among electric power distribution system operators (DSOs). They are in the middle of the modernization process due to their current effort on implementing smart meters, which is the first step toward the goal of a smart grid. Besides, they represent the class of industrial control organizations that is the most attractive target for attacks according to the statistics from ICS CERT. The perspectives of both industrial control systems and corporate IT systems were investigated in order to cover the organizations' response capabilities as a whole. Furthermore, we aimed at including middle-level managers rather than operators in our study, as they were assumed to have a more thorough overview of the complete incident management process. Our study is thus mainly concerned with management aspects of information security incident management.

In Norway, there are about 150 DSOs. About two thirds of these are categorized as small, serving fewer than 10.000 power consumers. In our study we have included both small and large DSOs to get insights into the current state of preparedness and incident response practices in the sector. In the analysis and presentation of the findings from the study, the size of the DSO is taken into account. Results from this study on planning and preparatory activities among large DSOs were presented by Line et al. [10]. In this paper we present related findings among small DSOs as well, and identify similarities and differences between small and large DSOs. Furthermore, we provide prioritized recommendations to DSOs on how they could improve their response capabilities for the new and emerging threats that they will be, or already are, exposed to. Understanding the differences between small and large DSOs is a prerequisite for the tailoring of these recommendations.

This paper is structured as follows. Related work is summarized in Section 2 together with the most acknowledged standards and guidelines. Section 3 describes the research method used in our study. Findings from our interview and documentation study are presented in Section 4, while Section 5 discusses the findings and compares the practices in large and small DSOs. Section 6 offers concluding remarks and identifies further work.

2. Background

A number of standards and guidelines provide recommendations regarding the general information security incident management process, including ISO/IEC 27035 [9], NIST 800-61 [11],

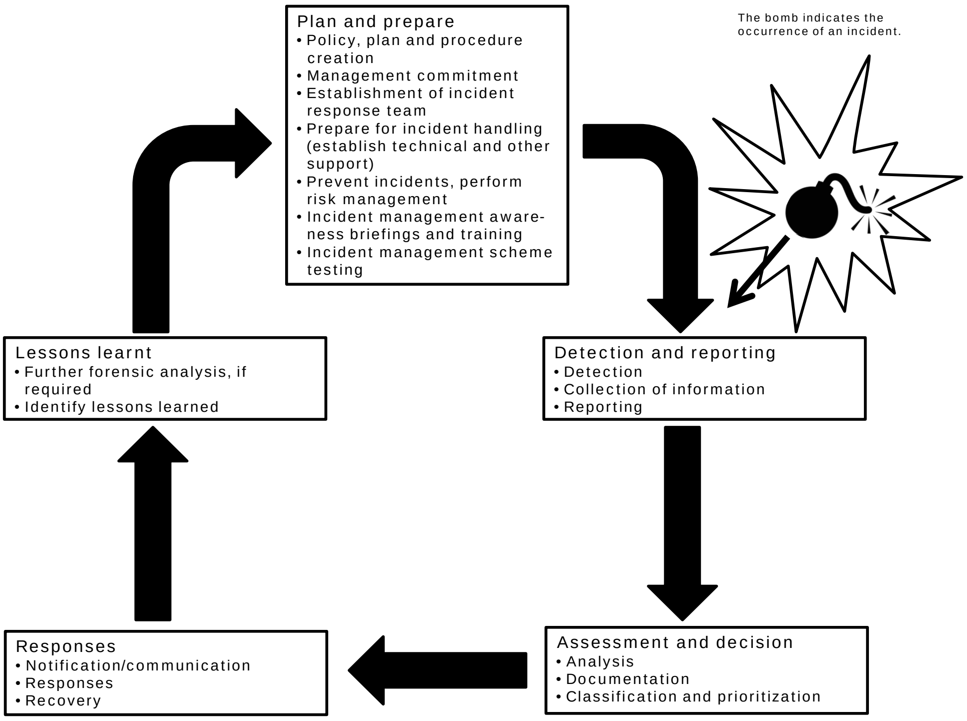
Plan and prepare
• Policy, plan and procedure creation
• Management commitment
• Establishment of incident response team
• Prepare for incident handling (establish technical and other support)
• Prevent incidents, perform risk management
• Incident management awareness briefings and training
• Incident management scheme testing
The bomb indicates the occurrence of an incident.
Lessons learnt
• Further forensic analysis, if required
• Identify lessons learned
Detection and reporting
• Detection
• Collection of information
• Reporting
Responses
• Notification/communication
• Responses
• Recovery
Assessment and decision
• Analysis
• Documentation
• Classification and prioritization

Figure 1: The complete incident management process (ISO/IEC 27035).

ITIL [12], and ENISA [13, 14]. The process is commonly described as a set of phases: planning and preparatory activities, detection, analysis, response, and post-incident evaluations. However, none of these documents concern industrial control systems in general. Figure 1 illustrates the five phases as described by ISO/IEC, including the main activities related to each phase.

In part 3 of their Guidelines for Smart Grid Security (NISTIR 7628) [15], NIST points out the need for research on cross-domain incident response for IT and power systems. More specifically, the issues of response and containment, intrusion detection and prevention, and event and impact prediction are emphasized.

Tøndel et al. [16] performed a systematic review of published experiences and practices related to information security incident management. In total 11 studies and 4 experience reports were included in the review, and they cover several sectors, including finance, acedemia, energy and national CERTs. Only two of the studies, Jaatun et al. [17] and Line [18], considered organizations with industrial systems, the latter of these being a publication of preliminary results from the study presented in this paper. Available documentation of experiences from information security incident management in control systems is thus limited in academic literature. Experiences from other sectors can however be of use for industrial contexts as well. The previous studies, as well as the inspirational examples and prominent challenges identified in the review, serve as important input for understanding and improving incident management in DSOs. Especially relevant for this study, as it focuses on the management aspects, are the benefits but also challenges of creating a simple plan, and establishing efficient practices for learning from incidents and sharing lessons learnt throughout the organization. DSOs are also likely to experience challenges related to senior management commitment, collaboration among teams and disciplines, and practicing incident management in outsourcing scenarios [16].

Based on the systematic review, activities on awareness, training and incident management scheme testing seem less elaborated in the existing literature, although the need for such activities is clearly pointed out [16]. Flodeen et al. [19] studied how a shared mental model for decision making in a group of incident responders could be created. A shared mental model has the potential to increase the performance during an incident handling process because the team manages to cooperate with limited and efficient communication. The actors involved will know where the others are in the process, the next steps, and the information required to complete the incident handling without wasting time on frequent recapture. Incident response is a highly collaborative activity and the diagnosis work is complicated by the practitioners' need to rely on tacit knowledge, as well as usability issues with security tools [20]. Hove et al. [21] found that plans and procedures are needed as a basic structure, but experienced incident handlers are much more valuable in an emergency situation. This finding aligns with theory within resilience engineering [22]. Challenges of training for incident management, such as ensuring realistic training scenarios and that the training actually provides value in real situations, were discussed by Hove et al. [21].

The future of smart grids, with the integration of IT and industrial control systems raises the need for DSOs to be prepared for the accompanying, emerging information security threats. Knowledge and understanding of current practices and related challenges for incident management in DSOs today are needed in order to provide valuable contributions to the DSOs in this process. Findings from other industries, as presented above, are useful, but there is a need to explore whether there are specific challenges in industrial control organizations and how these should best be met.

3. Research method

Our study was guided by the following research question: *How is information security incident management different in small DSOs compared to large DSOs?* We conducted interviews and collected documentation in nine distribution system operators (DSOs) in the electric power industry [23, 24].

3.1. Data collection

Semi-structured interviews are based on an interview guide and allow for unplanned questions [24]. Our interview guide was inspired by the ISO/IEC 27035 [9]. The interview guide used for large DSOs can be found as an appendix in Line et al. [10]. We revised this interview guide from the study of large DSOs before interviewing the small DSOs: some questions were added (6, 17, 30, 31, 33, and 34) and one was removed, which was too vague and was interpretede very differently by interviewees in the large DSOs. The added questions mainly aim at capturing the interviewee's reflections on own practices; whether they have practices that work particularly well, which challenges are worth emphasizing, and how the fact that they are a small DSOs affects the area of incident management.

The large DSOs were interviewed in June-December 2012, and the small DSOs were interviewed in December 2013; at their respective premises. All interviews were voice recorded and transcribed. The study was registered at the Data Protection Official for Research [25]. One test interview was carried out in DSO B.

We asked each of the DSOs for the following types of documents:

- Information security policy
- Information security instructions
- Plans for continuity and preparedness
- Plans for information security incident management
- Periodical reports on information security incidents
- Other related documents they may have

Five of the DSOs provided us with some documentation (c.f. Table 1). Confidentiality issues prevented three of the other DSOs from sharing documentation, and one DSO never replied to our request. Non-disclosure agreements and encrypted electronic transfer were not sufficient instruments for overcoming the confidentiality issues.

3.2. Data analysis

The analysis followed an integrated approach, which combines the inductive development of codes with a start list of categories in which the codes can be inductively developed [26, 27]. This was performed by one researcher due to confidentiality restrictions posed by four of the participating DSOs (D, E, F, Z). Two fellow researchers were involved in discussing coding categories and findings, and writing up this report. They had access to the transcriptions from the interviews conducted in the other DSOs (A, B, C, X, Y, c.f. Table 1) and reviewed the codes that emerged during the analysis. The software tool NVivo [25] was used for the data analysis.

3.3. Industrial case context

Nine DSOs were included in the study. The DSOs A-F are considered to be large in a Norwegian context as they serve more than 50.000 power consumers, and they were selected for being partners in the national research project DeVID. They constituted the first phase of the study, as presented by Line et al. [10]. The second phase included three small DSOs (X-Z), each which serve less than 10.000 consumers. An overview of the participating organizations is presented in Table 1, while roles and responsibilities of all the interviewees are shown in Table 2.

We asked to interview three different roles from each of the large DSOs: IT manager, IT security manager, and manager of control systems. The IT manager in DSO F was unable to participate, and we interviewed the manager for quality and risk instead, as was suggested and arranged for by that DSO. In DSO A we also interviewed one member of the technical IT staff in addition to the IT manager on their request, as the IT manager was fairly new to his role. In the small DSOs we interviewed two roles: the IT and IT security manager, as these roles were assigned to one person, and the one responsible for control systems operation. In DSO Y we also interviewed the finance manager, as he was responsible for the contract with their external IT supplier. In the small DSOs, it was common for one person to have several roles. In total, 26 interviews were carried out: 19 in large DSOs and 7 in small DSOs.

DSO	Number of interviewees	Documentation received	Size	Adm. IT outsourced	Req. NDA
A	4	Information security instructions, Plans for preparedness in IT systems	large	yes	yes
B	3	no	large	no	no
C	3	no	large	yes	no
D	3	no	large	yes	yes
E	3	Information security instructions, Plans for preparedness in control systems	large	no	yes
F	3	Information security policy, Information security events (quarterly report Q2-2012)	large	yes	yes
X	2	Security mechanisms in data centre	small	yes	no
Y	3	no	small	yes	no
Z	2	Information security policy, Information security instructions, Form for reporting incidents internally, Form for reporting incidents to authorities, NDA form, Agreements with IT supplier: NDA and security instructions	small	yes	yes

Table 1: The distribution system operators (DSOs) included in our study

DSO	Interviewee			
	1	2	3	4
A	Manager of IT supplier.	Owner of control systems, member of branch company management staff.	IT manager and IT security manager in branch company.	Employed by IT supplier, responsible for network infrastructure for both IT and control systems.
B	Corporate IT manager. Responsible for all IT systems and network infrastructure, and IT security.	Control room operations, operating the power distribution grid.	IT security manager for all IT systems, but in practice not for control systems.	–

C	IT manager in branch company.	Manager of the group that is responsible for daily operations of control systems and all network infrastructure for corporation.	Corporate IT manager.	–
D	Daily responsible for information security in corporation, approval of changes, point of contact for IT supplier,	Responsible for daily operations of, and information security for, control systems.	IT security manager in branch company.	–
E	IT manager, responsible for administrative IT systems in corporation. Overall responsible for IT security as well.	Responsible for daily operations of, and information security for, control systems.	Corporate IT security advisor.	–
F	Quality & risk manager, reviews both administrative and control systems.	Control room operations, operating the power distribution grid.	Corporate IT security advisor. Employed by IT supplier.	–
X	IT manager, finance manager, responsible for IT security, energy salesperson.	Manager of control systems.	–	–
Y	IT manager and IT security manager, but in practice: internal IT support.	Manager of control systems.	Finance manager, responsible for contracts with external IT supplier.	–
Z	IT manager, IT security manager, and manager of energy sales, including AMI and invoicing.	Manager of control systems.	–	–

Table 2: Roles and responsibilities of all the interviewees

3.4. Confidentiality issues in information security research

It must however be noted that just the day after our request for documentation from the large DSOs, the authorities sent an e-mail to all units that are part of the national emergency preparedness organization for power supply, which all the DSOs in this study are part of, encouraging them to be critical to all requests for sensitive information. The authorities stated that information sharing is not prohibited, but should be carefully considered in each case. As information security researchers we should appreciate such caution regarding sharing of confidential documents, although it poses limitations on the data triangulation. Kotulic and Clark [28] point out this challenge of obtaining sensitive data as limiting to research on information security management in general and recommend focusing on a few selected companies. This opens for building trust between the company and the researcher, which will ease the collection of sensitive data. Also, the companies in focus can be more involved in discussing and approving the results.

4. Findings

This section provides an overview of current incident management practices as reported by the interviewees from both small and large DSOs. The findings are presented according to the structure of ISO/IEC 27035, as shown in Figure 1. For the *Plan and prepare* phase, the section emphasizes findings from small DSOs, as planning and preparatory activities in large DSOs were presented previously by Line et al. [10]. Table 3 shows a summary of all incident management activities as they are performed in large and small DSOs respectively, and the main differences are emphasized in italics.

For the small DSOs, the term *IT manager* denotes the interviewees representing the perspectives of administrative systems in the small DSOs, although they are responsible for both IT and IT security.

4.1. Plan and prepare

Planning and preparing for information security incidents include understanding what incidents may happen, creating plans, and performing tabletop and functional exercises. The findings for the plan and prepare phase are structured similarly to the presentation of findings from large DSOs [10]: We describe the DSOs' perceived dependency on IT, their understanding of what an information security incident is and what they consider to be a worst case scenario, documented plans and procedures, their perceived preparedness for a worst case scenario, and their practices when it comes to preparedness exercises.

4.1.1. Dependency on IT

Both large and small DSOs state that they are more dependent on the administrative systems than the control systems. *Small DSOs seem however to be less dependent on control systems than large DSOs.* Small DSOs serve limited geographical areas, the distances between the critical nodes in their network are short, and, according to DSO Z, the operators know quite well where these nodes are. The distribution grid can be operated manually, and recovering from failures is manageable. However, without functioning control systems the automatic failure detection will not work, and they will depend more on customers contacting them about failures.

In both large and small DSOs, the administrative systems are important for cash flow. Further, they contain detailed maps of the grid. Hence, all DSOs report the dependency on these systems to be high. The control room manager in DSO X said that if the administrative systems are down for more than 48 hours, they will need more personnel for manually finding paper-based information. This will represent a considerable cost compared to having functioning systems.

4.1.2. Definition of an incident

Among the small DSOs, none of the interviewees provided a clear definition of an IT security incident. The terms confidentiality, integrity, and availability (CIA) were not mentioned specifically by any of the interviewees from the small DSOs. These terms were however used in the received information security policy and instructions from DSO Z. Despite the lack of a clear definition, all interviewees provided relevant examples of incidents. This is in line with the responses from the large DSOs.

4.1.3. Worst case scenario

Both large and small DSOs considered unauthorized control of power switches to be the worst case scenario. However, their view on this scenario is quite different: *Small DSOs do not consider themselves attractive targets. Furthermore, they consider the consequences to be quite limited compared to large DSOs.* The control manager in DSO X explained that the substation is not far away from their main office, so they would be able to get there quite fast, disconnect the remote control system, regain control of the switches, and turn the power back on. The control manager in DSO Y did not see that anyone would be interested in causing such harm to their power grid. He believed that a larger DSO, covering larger areas and more significant industries, would be a much more attractive target for hacker attacks. Those who could be interested in causing harm to the small DSOs, would not be able to do it due to lack of knowledge of their particular systems, he claimed. This view was also supported by the control room manager in DSO Z. DSO Y does not have remote control systems, which greatly limits the technical possibilities of performing a hacker attack.

Just like the large DSOs, the small DSOs also identified worst case scenarios for the administrative systems. Hacking of the customer database with the purpose of selling personal information was mentioned as a more realistic scenario than a power outage attack. Other threats perceived as realistic included virus attacks and physical failures. Further, two IT managers (DSOs Y, Z) added that the issue of having a non-functioning backup would make this scenario even worse. It would be quite costly to restore systems without an up-to-date backup.

4.1.4. Documentation of plans and procedures

The interviews with the large DSOs revealed that responsibilities and plans regarding information security incidents were not widely established. This was particularly the case when IT operations were outsourced. The small DSOs showed the same tendencies. None of the documentation that we received from the small DSOs contained any information about procedures for incident management. However, all the small DSOs explained that they have some plans regarding the handling of information security incidents. The control manager in DSO X stated that they have a collaborative plan with their IT supplier for incident management.

Though the small DSOs stated that they have some documentation to support them if an incident should occur, the awareness of the existence of this documentation seems to be limited. In addition, the knowledge of the content of the documentation seems to be lacking. The IT manager in DSO X stated that he did not know whether procedures for IT security incident management were described in the emergency preparedness plan. The control manager of DSO X admitted that the emergency preparedness plan was probably not well-known among the employees, partly due to new hirings, but they were about to have a meeting on this quite soon. In

DSO Y, the IT manager had not learnt about the incident management documentation from their IT supplier. They have a different supplier for their control systems, and the control manager claimed that they have not seen the need for documenting any procedures for incident management so far. If they experience any problems, they would just call their supplier. This applies to the administrative IT systems as well, as stated by the finance manager. In DSO Z, the control manager did not know about the plans and procedures referred to by the IT manager, but he also stated that there has never been a need for such. This was supported by the IT manager. Documented or improved plans and procedures were suggested by both large and small DSOs as possible improvements in their own organization.

4.1.5. Preparedness for worst case scenarios

All interviewees from the small DSOs claimed that their organization would be able to respond appropriately to a worst case scenario. Thus, *small DSOs appear to be more confident in their own preparedness than large DSOs*, who were more diverse in their responses. The control room managers of the small DSOs, who viewed hacking into the control systems as the worst scenario they could imagine, all stated that they would be able to disconnect the remote control system and manually operate the power grid for quite a long time if such a scenario should occur. The control room manager in DSO Z pointed out that the critical time period would be from the beginning of the attack until they managed to disconnect their systems.

Though all the DSOs are in general confident in their own ability to handle also worst case incidents, the IT manager in DSO Y said he did not know how much time they would need to achieve a complete recovery. The IT manager in DSO X expressed the importance of having a professional, large, and competent IT supplier on which they can rely in such situations. Some of the large DSOs were concerned about few preparedness training drills and the limited scope of the performed drills.

4.1.6. Preparedness exercises

The responses from small DSOs indicate that training receives an even lower priority than among large DSOs. Reasons for the lack of training were similar; it has not been on the agenda, other tasks receive higher priority, and training has a certain cost. In addition, the small DSOs assigned a low probability for IT attacks to occur, and they claimed to be able to operate the power grid manually for a long period of time. Where some of the large DSOs see the need to improve their training activities, small DSOs thus do not see the need to perform training for this in the near future.

All DSOs performed general emergency preparedness exercises regularly, but they were usually based on bad weather, fire, sabotage, and similar incidents. In small DSOs, IT-based scenarios were never used for such exercises, except for one tabletop exercise in the control room for DSO Y. The IT manager in DSO Z stated that protecting the physical grid and the production process from fire and similar incidents are viewed as more important than protecting the IT systems in order to ensure continuous power supply. The IT manager in DSO X emphasized the importance of having a competent supplier to assist during actual incidents. Still, he had never considered the need for performing a collaborative preparedness exercise on IT-based scenarios with this supplier. None of the other interviewees had discussed the possibility of performing such collaborative exercises with their suppliers either. The IT manager in DSO Z saw it as reasonable to include the supplier in such an exercise, but he had not given this any thought before the interview.

4.2. Detection and reporting

The seven DSOs that have outsourced their IT operations (A, C, D, F, X, Y, Z), rely on their supplier to detect incidents and notify them if something occurs. The other two DSOs (B, E) claimed to have monitoring and detection mechanisms in place. All respondents, except from DSOs X and Y, pointed out that employees are an important part of the sensor network for detecting irregularities. There are large variations between the DSOs regarding monitoring and detection systems for the control systems, but the size of the DSO seems to be irrelevant. DSOs B and E reported that the power automation network is fully monitored and failures will trigger alarms. The other DSOs said that incidents would be discovered accidentally by an operator noticing that something is not working satisfactorily, as there are limited, if any, detection mechanisms in place for the control systems.

Any irregularities in either the control or administrative IT systems are reported through the official channels: control room manager and control system manager or IT and IT security manager, supplier, corporate manager, authorities; the severity of the incident determines how far the reports go. The authorities are to be notified only if there are potential consequences for the electric power supply.

4.3. Assessment and decision, and Responses

None of the DSOs reported on having experienced any serious information security incidents. For administrative systems, the IT and IT security managers in large DSOs reported on experiencing the well-known: vulnerabilities in software requiring patches, malware infections, breaches of procedures like users not locking their PC when leaving their office, and unintentional mishaps. None of the DSOs had experienced any deliberate information security incidents in the control systems. Technical failures occur occasionally, but they never cause any disruptions for the power supply. One virus infection was mentioned, and this happened to a control system for power production in DSO B. They did not know the cause of this virus infection, but there was no antivirus running in these systems, and no patching regime was in place either. The incident caused control system computers to run slowly and required an extensive effort for clean-up, but it did not cause any damage. The small DSOs reported that they had never detected any information security incidents at all in their control systems. Furthermore, among the small DSOs the IT manager in DSO Z was the only one to report an information security incident in the administrative systems, as they experienced an extensive malware infection two-three years ago that caused the need for reinstalling all their computers. The IT managers in DSOs X and Y attributed their lack of incidents to the excellence of their IT supplier.

As none of the DSOs had experienced any major incidents in their ICT systems, their experiences regarding response was also limited. The need for collaboration during response was however discussed in the interviews. Several parties were mentioned to be included in this work: operators, managers on different levels, one or more suppliers, consultants. Several of the interviewees reported that this works well and that both the DSO and the supplier(s) benefit from successful and smooth collaborations. *The small DSOs stated that because they are small, several persons are assigned more than one role, and the same persons tend to meet and cooperate on many different tasks. The distances between key personnel are short.* However, large DSOs have also established close connections that are useful during response. The IT security manager in DSO A explained that they have close collaborations between the different departments, as the organization is fairly small, despite being among the largest with respect to the number of power consumers. Still, some collaborative challenges were pointed out: gaps in competence and understanding of information security (DSOs A, C), and central IT operations department not familiar with local implementations (DSO B). As one IT manager put it, referring to the IT staff on one hand and the control room operators on the other hand:

> *"There is a large gap in maturity when it comes to information security."*
>
> *— IT manager (C, branch)*

A lack of formally defined responsibilities was reported by the IT manager in DSO B, but despite of that, they have not experienced any specific problems. The interviewee suggested that the reason might be that they have not experienced any worst case scenarios yet.

In general, the large DSOs would like to improve the collaboration between IT and control system staff. Furthermore, DSO Z would like to improve the flow of information with their supplier of administrative IT systems, and the IT manager in DSO D would like their supplier to be more in front in making decisions, as they are the ones to hold the most competence on information security. These challenges were however related to everyday tasks rather than incident management in particular.

4.4. Lessons learnt

All respondents stated the need for thorough evaluations after an incident: identifying the root causes, extracting lessons learnt, and identifying improvements to risk assessments, organizational procedures, and technical systems. The type and severity of the incident determine who should participate in such an evaluation. Some DSOs stated that they have never evaluated any information security incidents, as they have never experienced them. They still considered learning activities to be an obvious part of the aftermath. DSOs do this for other types of incidents and saw no reason why information security incidents should be treated differently.

All DSOs reported that they have some kind of general discrepancy reporting. At the same time, none of the DSOs had a systematic approach to measurements related to information security incidents. The IT security manager in DSO E clearly expressed that this would be quite useful for communication with the top management:

> *"Maybe it would be easier to argue for solutions that we find necessary."*
>
> *— IT security manager (E)*

Some interviewees stated that they are able to estimate costs from some incidents, as their employees register work hours assigned to a dedicated project when they are not able to perform their regular work due to unforeseen downtime. Furthermore, some DSOs register the duration of unforeseen downtime per month as well. Such records might indicate a trend upwards or downwards and allow for the DSO to initiate actions if necessary. The control manager in DSO Y stated that the cost for one incident could be estimated based on records of work hours, invoice from supplier, loss of production, and not-delivered power. The need for regular reporting of incidents and procedures for this and increased awareness among management were expressed by large DSOs.

	Large DSOs	**Small DSOs**
Dependency on IT	100% dependent on both adm. IT and control systems. Can endure for some days without adm. IT, until cashflow stops. Can operate power grid manually without control room for a limited period.	100% dependent on adm. IT systems, can endure for some days, until cashflow stops. *Do not consider availability of the control systems as critical.*
Definition of incident	No common definition among control staff. Some IT/IT sec. staff used the terms confidentiality, integrity, availability.	No common definition, but relevant examples were provided. One security policy used the terms confidentiality, integrity, availability.
Worst case scenario	Malicious hacker attacks in control systems resulting in outages. Compromised/deleted databases with customer information and/or information on the physical power grid.	Compromised and sold customer database. Malware attack or failure in adm. IT sys. *Malicious hacker attacks in control systems resulting in outages was viewed as possible, but very unlikely.*
Documented plans	Established in one DSO only, in progress in some DSOs, non-existing in others. Reliance on suppliers, but no collaborations on plans.	One DSO has collaborative plans with their IT supplier. Otherwise some plans documented, but not well established and known.
Preparedness for worst case	Various perceptions: Trust their well-organized and planned general emergency preparedness, and/or ability to improvise. Some reported doubt on own preparedness due to lack of training.	*Confident with own and/or supplier's response capabilities.*
Training	Regular general emergency preparedness exercises, but they are rarely based on IT security incidents.	Regular general emergency preparedness exercises, but they are rarely based on IT security incidents. *Receives lower priority than in the large DSOs due to the perception that attacks are unlikely.*
Detection of incidents	Mainly rely on suppliers of IT and/or own employees. Monitoring of control systems implemented by some DSOs.	*Rely heavily on suppliers* of both IT and control systems, unless incidents are easily detected by internal employees.
Initial reporting	Official channels: middle and top managers, suppliers, authorities. Depends on severity of incident.	Official channels, but *shorter distances between key personnel* than in large DSOs. Same personnel involved in all kinds of incidents.

Common incidents and consequences	Adm. IT: malware, unintentional breaches of procedure, etc. Control systems: few incidents (only one virus infection mentioned).	Adm. IT: *no major incidents*, explained with well-functioning monitoring. Control systems: *no information security incidents.*
Collaborative challenges during responses	Competence gaps, lack of formalized responsibilities. Still, works fairly well in practice. Successful collaborations with suppliers.	*No challenges related to responses mentioned*, but would like to improve communication with supplier in general.
Post-incident evaluations	Would identify lessons learnt and necessary improvements. Management and suppliers would participate. DSOs do this for other types of incidents.	Would include key personnel, top management, and possibly supplier, depending on type of incident.
Registration and metrics	All have quality systems, but IT matters are not registered by all. No systematic approach to metrics for information security incidents in particular.	Some have their own quality system, other leave this to supplier. No systematic approach to metrics for information security incidents in particular.

Table 3: Established practices for incident management activities in large and small DSOs.

5. Discussion

Our findings from the interviews and the documentation study show a number of differences between large and small DSOs:

1. Small DSOs do not see themselves as possible targets for targeted attacks. They believe that the large DSOs are more attractive targets. Preparedness exercises based on IT security incidents therefore receive even lower priority in the small DSOs than in the large DSOs. The large DSOs are more aware of their own position as possible targets for worst case scenarios.

2. The small DSOs depend little on the control systems. A shutdown of the control room will not cause nearly the same inconvenience to the small DSOs as compared to the large DSOs. Consequently, small DSOs consider the consequences of malicious hacker attacks against the control systems to be rather limited.

3. Despite the fact that small DSOs give preparedness exercises based on IT security incidents a low priority, they are confident in their ability to respond to the worst case scenarios. Large DSOs realize the need for better preparations.

4. The distances between key personnel are short in small DSOs, which simplifies communication and collaboration during a crisis. Large DSOs are more likely to suffer from organizational dividing lines, a lack of dynamic collaborations across these lines, and unclear responsibilities in some areas.

5. Small DSOs depend heavily on their IT supplier. They rely on the supplier to have the necessary plans, procedures, exercises, competence, equipment and the ability to respond appropriately to incidents. Large DSOs show the same tendency, but to a much lesser degree, and they have more IT and IT security competence in-house.

In the following, the differences between large and small DSOs and their implications on the incident management process are discussed in more detail. Further, a set of recommendations are provided, both for small DSOs specifically and for DSOs of all sizes. Finally, we discuss threats to validity for our study.

5.1. Risk perception

An individual's risk perception is influenced by technical/formal risk assessments and her own personal risk assessments, combined with perceptual factors such as fear [29]. Hence, there might be a gap between risk perceptions and the actual level of risk. As individual risk perceptions affect risk behavior, they might also influence the risk perception in an organization [30]. For exercises and other preparatory activities to be performed, the top management needs to show commitment. Senior management commitment is key to successful information security, but is perceived as quite challenging to achieve, as reported by Tøndel et al. [16]. Rhee et al. [31] showed that management tends to be optimistically biased in that they underestimate their organization's vulnerability and overestimate their ability to control the security threats. This indicates that the effort towards the management should be less on general security awareness and more on the actual threats and possible consequences to the specific organization.

The small DSOs believed that malicious attackers who want to cause power outages, would rather target larger DSOs. Furthermore, they considered the consequences of attacks to the control systems as limited, as these systems are not of crucial importance in the process of maintaining continuous power supply to the customers. The information security risk was perceived to be lower among the small DSOs than among the large DSOs. In the following, we discuss whether or not the small DSOs' perception that they are not a target, is likely to be true. In addition, we discuss whether or not their perception of low dependency on control systems is likely to still hold given the development towards smarter grids.

5.1.1. Attractiveness as a target

It is reasonable to believe that attackers would look for larger areas where major organizations within finance, energy, media, and public authorities operate, in order for an attack to have a certain impact and/or receive a certain amount of attention. However, certain cornerstone enterprises and several military installations are located in smaller towns where the power grid is operated by a small DSO. A small DSO may not be the target by itself, but it might serve customers that are attractive targets for attacks. The small DSOs in our study had not considered this before the interviews. Besides, one small DSO might not be attractive alone, but striking several small DSOs at the same time might be easier than attacking one large DSO. Attackers who would want to harm the country as a whole might consider this as a strategy. The consequences of a power outage attack should be considered beyond the effects for one single DSO.

In addition to power outages, industrial espionage is a possible motivation for attacks against the power industry – obtaining access to confidential corporate information. It is reasonable to assume that striking larger organizations would be more rewarding, as their contracts typically involve more money. A third main motivation for attacks these days is collection of personal information [32]. This was mentioned as a possible worst case scenario by both large and small

DSOs. The probability of such a compromise depends on the level of protection of data and ease of accomplishment rather than the size of the organization.

5.1.2. Dependency on the control systems

The degree to which a DSO is dependent on the control systems seems to be determined by the DSO's ability to maintain continuous power supply to their customers without the control systems. The geographical area served by a small DSO is typically limited. The operators know the area well, and there are short distances between the main office and the substations. The grid contains fewer substations and fewer components than the grids operated by larger DSOs, and this limits the attack surface as well. Small DSOs are responsible for the local distribution grid only, while some of the larger DSOs operate regional or transmission grids in addition. These were reasons provided by the small DSOs for why they could operate successfully with unavailable control systems. However, there is a large difference between unavailable control systems and minor, undetected errors in the information provided by the control systems. We are concerned that only the property of availability was considered by the DSOs when asked about dependency. None of the interviewees mentioned breaches of integrity or confidentiality. We believe that an integrity breach in the control systems could potentially have severe consequences, as erroneous information could make operators perform unfortunate actions and cause overload in the grid, possibly with physical damages as a result. Such minor errors can be invisible to the human eye and only be detected by automatic monitoring systems, which are not yet widely used for control systems, at least not among small DSOs.

The emergency preparedness regulations require DSOs of all sizes to be able to manually operate the power grid [33]. The large DSOs however stated that manual operation would not be possible for a long period of time. The number and severity of occurring failures determine how long they can manage, due to the need for having a sufficient amount of personnel. With the smart grids being implemented in the future, it is reasonable to believe that the complexity of the IT and control systems will increase and that the DSOs, including the small DSOs, will depend more heavily on these systems for efficient operation.

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

5.2. Collaborations during incident response

Employees in small DSOs know each other well and their offices are in the same corridor, which enables close collaborations, as opposed to in a large DSO that is divided into departments, and responsibilities are clearly defined for each department. Communication between personnel in different departments tends to be more limited. This difference affects information sharing, adhoc collaborations, and lines for alerting and reporting. During a crisis situation it is important to have an overview, see connections, and make the right decisions. The IT manager in DSO X claimed this to be much easier in a small organization. Sharing, rather than finding, information was stated as challenging by Ahmad et al. [34], but this seems to be less of a challenge in small DSOs. On the other hand, as personnel in the small DSOs have more than one role, some tasks may be given low priorities due to other, more pressing tasks. This puts the onus on the top manager to communicate the appropriate prioritizations.

We would expect the IT staff to be able to share expertise, as hacker attacks towards administrative IT systems have been around for several years. That being said, knowing how to prepare for, and appropriately respond to, such attacks is not straigthforward, but a combination of general knowledge of attackers' strategies and detailed knowledge of the control systems should be a reasonable starting point. There are some distinct differences between administrative IT and control systems, such as availability requirements and consequences from an attack [35]. Response strategies are therefore not directly transferrable. Still, there should be synergy effects from collaborations between IT and control system operators.

All the DSOs rely on their suppliers of control systems, and in most cases also their suppliers for IT systems, for support in case an incident occurs. Small DSOs expect the suppliers to have appropriate security measures in place, in addition to plans and response capabilities. The existence of plans or having a response team in place seem to have a significant effect on the feeling of preparedness according to Witchalls and Chambers [36].

Documented experiences on incident management from other sectors show that efficient and successful incident management requires collaboration between several parties [16]. This is also the case for DSOs. However, DSOs seem relatively confident that collaboration will be smooth in case an incident occurs, while the literature shows that collaboration tends to be challenging, particularly in outsourcing scenarios [16]. Hove et al. [21] specifically identified the challenge of determining who *owns* an incident, an issue that could not be exactly documented in written procedures. Hesitations and delays in the early stages of the response phase could make the cost of the incident much higher than necessary.

All the three small DSOs have outsourced their IT operations, and outsourcing relieves the DSO of several practical tasks, which are more efficiently solved by large-scale professional supply organizations. Still, the DSOs need to be knowledgable about threats to be able to formulate appropriate requirements to their supplier. This is in fact also stated in national requirements: all organizations licensed according to Energiloven (Energy Act) must have in-house expertise for all tasks covered by the license. A small DSO is, however, just one out of several customers for the IT supplier, and might feel that they are not in the position of making demands. Therefore, they tend to accept what the supplier has to offer and assume that this is sufficient. The security level of the administrative IT systems is then in the hands of the suppliers. One of the large DSOs actually pointed out their concern about the supplier of control systems being attacked and the consequences this could pose to the DSO. The supplier has several employees with extensive competence and knowledge about their systems and remote access into the core of the control systems.

In addition to formulating requirements, the DSOs should make sure that all collaborations are well documented, including plans and procedures for incident management. The existence of such plans was limited among both large and small DSOs, and particularly among those who had outsourced their IT operations. The lack of such documentation does not imply unsuccessful incident management by the supplier, as they might have their own well-functioning procedures without the DSO being aware of this. However, documentation is the first step on the way to successful collaboration as it forms a basis for further clarifications and exercises. DSO X had collaborative plans with their supplier, a practice that we would like to recommend to all the other DSOs as well.

Small DSOs have the same duties and obligations as large DSOs, but not the same amount of financial resources and personnel. Collaborations with other small DSOs are valuable, according to DSO X. Sharing knowledge and competence compensates for not having the same capabilities as the larger ones.

5.3. Awareness and training

It was stated by both large and small DSOs that a malicious attack could easily be stopped by disconnecting the control room from the network. The IT operator from DSO A's IT supplier was the only one who pointed out the challenge of investigating an incident and its consequences if just pulling the plug was the response strategy. Our major concern regarding this strategy and the fact that this was the number one strategy suggested by everyone, is that it requires the attack to be detected. Targeted attacks tend to be designed with the aim of not being easily detected and might be in progress for a long time before the consequences become evident. A power outage is indeed a notable consequence, but an attacker might just as well perform slight modifications for a longer period of time. This might cause serious damage one day in the future, but do not necessarily result in sudden consequences, as was the case with Stuxnet [4, 5, 6].

The responses showed that no targeted attacks have been detected so far and that the number of IT security incidents in the control systems in general is rather low. This means that the operators get very little practical experience in recognizing and responding to such incidents, which indeed are likely to occur at some point, as indicated by current threat statistics [8]. The smart grid future is likely to involve higher connectivity and integrations between IT and control systems, also for the small DSOs. This demonstrates the importance of performing preparedness exercises, as they should expect IT security incidents to occur at some point. The need for training is supported by the fact that experienced incident responders are considered to be of higher value than documented plans and procedures when an emergency situation occurs [21].

General emergency preparedness exercises are well-known and regularly performed by all the DSOs, but the scenarios are usually related to physical damage. Deliberate hacker attacks in the control systems or other IT security incidents are rarely part of drills. Such exercises are given an even lower priority among the small DSOs than among the large DSOs. Two main reasons were stated for general preparedness exercises being performed regularly: the national regulations require this, and interruptions in the power supply have considerable costs for a DSO. Norwegian authorities have already realized the need for requiring IT security incidents to be trained for, as they included IT security incidents among recommended training scenarios in the national regulations in July 2013. The interviews with large DSOs were performed before this date. It remains to be seen how long it will take them to adopt the recent recommendations.

The fact that a large number of IT services, particularly administrative IT systems, are outsourced, calls for the need for collaborative preparedness exercises with suppliers. The practical response activities will typically be performed by them, and there are a number of factors that determine whether an incident is responded to in the best possible manner. Collaborative exercises could reveal unclear responsibilities and other grey areas.

5.4. Recommendations

We hereby provide a set of prioritized recommendations to DSOs with the intention of improving preparedness for information security incidents. For small DSOs we specifically recommend the following:

1. Improve the collaboration with the IT supplier. Discuss risk perceptions, security mechanisms, reporting and response procedures, and exercises. Ensure that requirements are written in accordance with performed risk assessments.

2. Initiate/maintain a dialogue with other small DSOs. Exchange experiences and concerns related to information security incidents and incident management practices. Existing initiatives for information sharing and analysis could be used as inspiration, such as FS-ISAC [37].

Additionally, we recommend the following to both small and large DSOs:

1. Document plans and procedures for incident management. Include both IT and control systems suppliers in this process, use ISO/IEC 27035 as a checklist, make sure that key personnel are aware of their roles and responsibilities.

2. Perform preparedness exercises on information security incidents in the control systems, including targeted attacks and the worst case scenarios. Perform collaborative exercises: with suppliers, other DSOs, the largest customers.

3. Implement automatic monitoring and detection mechanisms in the control systems.

4. Establish and/or improve collaboration between control system operators and IT staff. Educate control room operators in information security and strengthen their ability of detecting malicious activity in the networks. Educate IT staff in control system properties and differences from IT systems.

5.5. Threats to validity

Construct validity: Interviewees may be biased [38], and they might have a conscious or unconscious desire of giving a good impression of themselves and their organization. We perceived the interviewees to be honest in their responses as they reported shortcomings in a number of areas rather than a perfect situation. Some even expressed their gratitude for us performing this study, as it gave them an opportunity to discuss these issues internally, they gained new insights during our interviews, and they appreciated that their area receives additional attention.

> *"The way you presented the questions... it made me learn something, too."*
>
> *— Control manager (Z)*

We limited our study to include interviewees from the management level in the organizations. This also limited the level of detail we were able to bring to light regarding the practical tasks of detecting, interpreting, and responding to incidents, as these tasks are performed by employees on lower levels and/or by supplier organizations. It would have strengthened this study to include such operational personnel, but our limitation was due to time and resource constraints.

Data triangulation: The quality of data increases when a phenomenon is studied from different perspectives [23]. We used interviews and documentation as information sources, as they provide two different views on incident management. The interviewees would describe their practice as they know it, while documentation would show the planned procedures.

All interviewees were provided with a draft of this paper, and hence given the opportunity to comment on the results. This is referred to as member checking [24], and is a strategy for reducing researcher bias. In our study where one researcher did most of the analysis, this was especially important. It also shows our informants that we value their contributions.

External validity refers to the degree to which the findings from one study can be generalized to other settings [24]. Our study is restricted to DSOs, and both the DSOs and the participating interviewees were thoroughly described in Section 3. This description of the industrial case context is of great importance when considering whether our results are transferrable to a given setting. There is a lack of similar studies (with the exception of the related work of Jaatun et al. [17]) on incident management in industrial control organizations. We believe that more empirical studies like ours should be carried out within a broader spectrum of such organizations. Generalizability will be strengthened by increasing the number of studies.

After the completion of the planned interviews in the large DSOs, saturation was reached [39]. For the perspectives of IT managers and IT security managers, saturation was actually reached before all the planned interviews were completed, as their responses were fairly well aligned. The need for information about the control systems still called for completing the interviews in all the six large DSOs. The small DSOs were included in the study for the purpose of investigating how, if at all, current practice differs between them and the large DSOs. It could be argued that more than three small DSOs should be explored, but we still felt that saturation was achieved after completion of the seven interviews conducted in the small DSOs. The responses reflected similar practices and hence constituted a sufficient amount of empirical data for us to compare with the practices in the large DSOs.

6. Concluding remarks and further work

Our study shows that there are a number of differences between large and small DSOs in their information security incident management practices. The risk perception tends to be lower among small DSOs, and their feeling of preparedness is accordingly higher than in the larger DSOs. Both large and small DSOs have weaknesses in their practices that need to be addressed in order for the industry to meet the emerging threats.

None of the DSOs had ever experienced any targeted attacks to their IT systems nor their control systems before our study. After we completed this study, the power industry in Norway was hit by a hacker attack [40]. We followed up by sending three questions by email to each DSO, asking about how this attack affected their approaches to information security, independent of whether they were hit by the attack or not. Six DSOs responded. The responses indicate that the top managers are now more concerned about information security incidents and preparedness exercises in particular. All the DSOs claim 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, the trend seems to be that preparedness exercises for information security incidents are given higher priority, reviews of documentation are performed, and the understanding of threats and of the importance of monitoring and analysis of incidents has been improved.

The power industry, and DSOs in particular, are implementing smart grids, and they will be experiencing large technological changes in the near future. Even though everything seems to go well so far, the DSOs foresee the possibilities of malicious attacks being performed, also in the control systems as of today. The worst case scenarios are considered real, although not very likely. These scenarios have not been included in training and drills. Based on our findings, we claim that there has been a mismatch between anticipation and preparation. The recent major attack clearly served as a wakeup call for a number of organizations, and top management in particular. Such attacks typically increase awareness, but this effect is usually short-lived. Continuous preparations and improvements to the information security incident management process is required in order for the power industry to be prepared for the future.

Research efforts should be put into preparedness exercises for IT security incidents: design and evaluations of collaborative exercises, both tabletop and more functional exercises, where participants represent both IT and control systems, DSO and suppliers. Both low-impact and high-impact incidents should form scenarios to be trained for.

Acknowledgments

The authors would like to thank the distribution system operators and specifically all of the respondents that contributed to this study. This work was funded by the Norwegian Research Council, grants no 217528 (the *DeVID* project) and no 234644/F11, and by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*.

References

[1] M. B. Line, I. A. Tøndel, M. G. Jaatun, Cyber security challenges in Smart Grids, *Proceedings of the Second IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)* (dx.doi.org/10.1109/ISGTEurope.2011.6162695), 2011.

[2] M. Rashid, S. Yussof, Y. Yusoff, R. Ismail, A review of security attacks on IEC61850 substation automation system network, *Proceedings of International Conference on Information Technology and Multimedia (ICIMU)*, pp. 5–10 (dx.doi.org/10.1109/ICIMU.2014.7066594), 2014.

[3] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. v. Eeten, M. Levi, T. Moore, S. Savage, Measuring the Cost of Cybercrime, *Proceedings of Eleventh Workshop on the Economics of Information Security (WEIS'12)*, 2012.

[4] D. Albright, P. Brannan, C. Walrond, Did Stuxnet take out 1000 centrifuges at the Natanz enrichment plant?, Institute for Science and International Security (ISIS), Washington, DC, USA (http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/), 2010.

[5] D. Albright, P. Brannan, C. Walrond, Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, Institute for Science and International Security (ISIS), Washington, DC, USA (isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8), 2011.

[6] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Version 1.4, Symantec, Mountain View, California, USA (www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf), 2011.

[7] McAfee, Global Energy Cyberattacks: "Night Dragon", McAfee Foundstone Professional Services and McAfee Labs, Santa Clara, CA, USA, 2011.

[8] Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Monitor Newsletter, ICS-MM201312 Washington, DC, USA (ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf), 2013.

[9] International Standards Organisation / International Electrotechnical Commission, Information technology - Security techniques - Information security incident management, ISO/IEC Standard 27035:2011, Geneva, Switzerland, 2011.

[10] M. B. Line, I. A. Tøndel, M. G. Jaatun, Information security incident management: Planning for failure, *Eighth International Conference on IT Security Incident Management and IT Forensics (IMF)*, pp. 47–61, 2014.

[11] T. Grance, K. Kent, B. Kim, Computer Security Incident Handling Guide, NIST SP 800-61, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2008.

[12] E. Brewster, R. Griffiths, A. Lawes, J. Sansbury, IT Service Management: A Guide for ITIL Foundation Exam Candidates, 2nd Edition, BCS, The Chartered Institute for IT, Swindon, UK, 2012.

[13] H. Bronk, M. Thorbruegge, M. Hakkaja, A basic collection of good practices for running a CSIRT, European Network and Information Security Agency, Heraklion, Greece, 2007.

[14] ENISA, Good practice guide for incident management, European Network and Information Security Agency, Heraklion, Greece, 2010.

[15] The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References, NISTIR 7628-3, National Institute for Standards and Technology, Gaithersburg, MD, USA, 2010.

[16] I. A. Tøndel, M. B. Line, M. G. Jaatun, Information security incident management: Current practice as reported in the literature, *Computers & Security*, vol. 45, pp. 42–57 (`dx.doi.org/10.1016/j.cose.2014.05.003`), 2014.

[17] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, O. H. Longva, A framework for incident response management in the petroleum industry, *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 26–37, 2009.

[18] M. B. Line, A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry, *Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, pp. 26–32, 2013.

[19] R. Floodeen, J. Haller, B. Tjaden, Identifying a Shared Mental Model Among Incident Responders, *Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, pp. 15–25, 2013.

[20] R. Werlinger, K. Muldner, K. Hawkey, K. Beznosov, Preparation, detection, and analysis: the diagnostic work of IT security incident response, *Information Management & Computer Security*, vol 18(1), pp. 26–42, 2010.

[21] C. Hove, M. Tårnes, M. B. Line, K. Bernsmed, Information security incident management: Identified practice in large organizations, *Eighth International Conference on IT Security Incident Management and IT Forensics (IMF)*, pp. 27–46, 2014.

[22] E. Hollnagel, J. Pariès, D. D. Woods, J. Wreathall (Eds.), *Resilience Engineering in Practice - a Guidebook*, Ashgate Publishing Ltd., Farnham, Surrey, UK, 2011.

[23] R. K. Yin, *Case Study Research - Design and Methods*, 4th ed., Vol. 5 of *Applied Social Research Methods*, SAGE Publications, London, UK, 2009.

[24] C. Robson, *Real world research*, 3rd Edition, John Wiley & Sons Ltd., Chichester, West Sussex, UK, 2011.

[25] The Data Protection Official for Research, http://www.nsd.uib.no/personvern/en/index.html.

[26] R. Bogdan, S. K. Biklen, *Qualitative research for education: an introduction to theory and methods*, Allyn and Bacon, Boston, MA, USA, 1982.

[27] J. Lofland, *Analysing social settings*, Wadsworth Publications, Belmont, CA, USA, 1971.

[28] A. G. Kotulic, J. G. Clark, Why there aren't more information security research studies, *Information & Management* vol. 41(5), pp. 597–607 (`dx.doi.org/10.1016/j.im.2003.08.001`), 2004.

[29] T. Aven, O. Renn, *Risk Management and Governance: Concepts, Guidelines and Applications*, vol. 16 of *Risk, Governance and Society*, Springer, Heidelberg, Germany, 2010.

[30] T. Rundmo, Associations between risk perception and safety, *Safety Science*, vol. 24(3), pp. 197–209 (`dx.doi.org/10.1016/S0925-7535(97)00038-6`), 1996.

[31] H.-S. Rhee, Y. U. Ryu, C.-T. Kim, Unrealistic optimism on information security management, *Computers & Security*, vol. 31(2), pp. 221–232, 2012.

[32] A. Sood, R. Enbody, Targeted Cyberattacks: A Superset of Advanced Persistent Threats, *IEEE Security & Privacy*, vol. 11(1), pp. 54–61 (`dx.doi.org/10.1109/MSP.2012.90`), 2013.

[33] NVE, Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (Beredskapsforskriften) (in Norwegian), Ministry of Petroleum and Energy, Norwegian Water Resources and Energy Directorate, (`www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20121207-1157.html`), December 11, 2012.

[34] A. Ahmad, J. Hadgkiss, A. B. Ruighaver, Incident Response Teams - Challenges in Supporting the Organisational Security Function, *Computers & Security*, vol. 31(5), pp. 643–652, 2012.

[35] M. B. Line, Why securing smart grids is not just a straightforward consultancy exercise, *Security and Communication Networks*, vol. 7(1), pp. 160–174 (`dx.doi.org/10.1002/sec.703`), 2013.

[36] C. Witchall, J. Chambers, Cyber incident response: Are business leaders ready?, The Economist Intelligence Unit (EIU), London, UK, 2014.

[37] Financial Services - Information Sharing and Analysis Center, (`www.fsisac.com`), 2015.

[38] T. Diefenbach, Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structured interviews, *Quality & Quantity*, vol. 43(6), pp. 875–894 (`dx.doi.org/10.1007/s11135-008-9164-0`), 2009.

[39] G. Guest, A. Bunce, L. Johnson, How many interviews are enough? an experiment with data saturation and variability, *Field Methods*, vol. 18(1), pp. 59–82 (`dx.doi.org/10.1177/1525822X05279903`), 2006.

[40] L. Munson, Massive cyber attack on oil and energy industry in Norway, *Sophos – naked security*, (`nakedsecurity.sophos.com/2014/08/28/massive-cyber-attack-on-oil-and-energy-industry-in-norway/`), August 28, 2014.