Maria Bartnes Line

UNDERSTANDING INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICES

A case study in the electric power industry

Thesis for the degree of Philosophiae Doctor

Trondheim, April 2015

Norwegian University of Science and Technology
Faculty of Information Technology,
Mathematics and Electrical Engineering
Department of Telematics

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Telematics

© Maria Bartnes Line

ISBN 978-82-326-1138-6 (printed ver.)
ISBN 978-82-326-1139-3 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2015:241

Printed by NTNU Grafisk senter

*“The real voyage of discovery
consists not in seeing new landscapes,
but in having new eyes.”*

— *Marcel Proust*

Abstract

With the implementation of smarter electric power distribution grids follows new technologies, which lead to increased connectivity and complexity. Traditional IT components – hardware, firmware, software – replace proprietary solutions for industrial control systems. These technological changes introduce threats and vulnerabilities that make the systems more susceptible to both accidental and deliberate information security incidents. As industrial control systems are used for controlling crucial parts of the society's critical infrastructure, incidents may have catastrophic consequences for our physical environment in addition to major costs for the organizations that are hit. Recent attacks and threat reports show 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 both organizational, human, and technological factors. The main objective of this doctoral project has been to explore information security incident management practices in electric power companies and understand challenges for improvements. Both literature studies and empirical studies have been conducted, with the participation of ten Distribution System Operators (DSOs) in the electric power industry in Norway.

Our findings show that detection mechanisms currently in use are not sufficient in light of current threats. As long as no major incidents are experienced, the perceived risk will most likely not increase significantly, and following, the detection mechanisms might not be improved. The risk perception is further affected by the size of the organization and whether IT operations are outsourced. Outsourcing of IT services limits the efforts put into planning and preparatory activities due to a strong confidence in suppliers. Finally, small organizations have a lower risk perception than large ones. They do not perceive themselves as being attractive targets for attacks, and they are able to operate the power grid without the control systems being available. These findings concern risk perception, organizational structure, and resources, which are factors that affect current practices for incident management.

Furthermore, different types of personnel, such as business managers and technical personnel, have different perspectives and priorities when it comes to information security. Besides, there is a gap in how IT staff and control system staff understand information security. Cross-functional teams need to be created in order to ensure a holistic view during the incident response process. Training for responding to information security incidents is currently given low priority. Evaluations after training sessions and minor incidents are not performed. Learning to learn would make the organizations able to take advantage of training sessions and evaluations and thereby improve their incident response practices.

The main contributions of this thesis are knowledge on factors that affect current information security incident management practices and challenges for improvement, and application of organizational theory on information security incident management. Finally, this thesis contributes to an increased body of empirical knowledge of information security in industrial control organizations.

Preface

This thesis was submitted in partial fulfillment of the requirements for the degree of philosophiae doctor (PhD) at the Norwegian University of Science and Technology (NTNU). The doctoral work has been performed at the Department of Telematics and supervised by Professor Poul E. Heegaard, Professor Svein J. Knapskog (2011-2013), and Professor Danilo Gligoroski (2013-2015).

The 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), no 234644/F11 (support for research visit at UCSB), and no 201557 (IMMER); the Telenor-SINTEF research agreement Smart Grid initiative; the Office of Naval Research (ONR) under Grant N000140911042; the Army Research Office (ARO) under grant W911NF0910553; and Secure Business Austria.

I would like to thank my supervisors: Poul E. Heegaard, Svein J. Knapskog, and Danilo Gligoroski. Thank you, Poul, for being a great colleague and friend. I owe a special thanks to Professor Richard A. Kemmerer at the University of California, Santa Barbara, for hosting my research visit at UCSB in 2014. Santa Barbara is my paradise on earth – the opportunity to stay there for seven months was invaluable, both for myself, my doctoral project, and my family.

I could not have completed this project without the support and collaboration with a few of my colleagues at SINTEF. Martin Gilje Jaatun and Inger Anne Tøndel; for all my questions you always have the time and helpful answers, and it is always a pleasure working with you. Nils Brede Moe, thank you for all your guidance in writing up this thesis, and for at least 425 coffee breaks with challenging and fun discussions about goals, opportunities, and everything; *Don't underestimate the coffee machine.* I would also like to thank Eldfrid Ø. Øvstedal for supporting me in pursuing my PhD degree and letting me combine that with my research position at SINTEF.

My fellow PhD students and office mates; Jonas Wäfler, Bjørn J. Villa, Katrien De Moor, Joakim Klemets, and Mauritz Panggabean; thanks for all the talks about the many questions in life, both professional and personal, major and not so major.

Finally, life is so much more than work. I am forever thankful for my children; Guro, Eirin, and Jonas; you make me learn something new every day. Friends and family, thanks for all the encouragement and inspiration. I would like to thank three of you in particular: Grete Bartnes, Inge Nordbø, and Marianne Gullvåg. You are amazing.

April 30, 2015
Maria Bartnes Line

Contents

List of Papers

P1. Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun. *Cyber Security Challenges in Smart Grids,* IEEE PES Innovative Smart Grid Technologies 2011, Manchester, UK.

P2. Maria B. Line. *Why securing smart grids is not just a straightforward consultancy exercise,* Security and Communication Networks, 2014.

P3. Inger Anne Tøndel, Maria B. Line, and Martin G. Jaatun. *Information security incident management: Current practice as reported in the literature,* Computers & Security, 2014.

P4. Maria B. Line and Eirik Albrechtsen. *Examining the suitability of industrial safety management approaches for information security incident management,* forthcoming in International Journal of Information and Computer Security.

P5. Maria B. Line. *A Study of Resilience within Information Security in the Power Industry,* IEEE Africon 2013, Mauritius.

P6. Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun. *Information security incident management: Planning for failure,* 8th International Conference on IT Security Incident Management and IT Forensics (IMF) 2014, Münster, Germany.

P7. Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun. *Does size matter? Information security incident management in large and small industrial control organizations,* submitted to International Journal of Critical Infrastructure Protection.

P8. Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard A. Kemmerer. *Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?* 2nd Smart Energy Grid Security Workshop (SEGS) 2014, Phoenix (AZ), US.

P9. Maria B. Line and Nils Brede Moe. *Understanding Collaborative Challenges in IT Security Preparedness Exercises,* International Conference on ICT Systems Security and Privacy Protection (IFIP SEC) 2015, Hamburg, Germany.

Other Publications

Maria B. Line, Inger Anne Tøndel, and Erlend Andreas Gjære. *A Risk-Based Evaluation of Group Access Control Approaches in a Healthcare Setting,* Multidisciplinary Research and Practice for Business, Enterprise, and Health Information Systems Workshop (MURPBES) 2011, Wien, Austria.

Erlend A. Gjære, Inger Anne Tøndel, Maria B. Line, Herbjørn Andresen, and Pieter J. Toussaint. *Personal Health Information on Display: Balancing Needs, Usability and Legislative Requirements,* Studies in Health Technology and Informatics, 2011.

Maria B. Line and Inger Anne Tøndel. *Information and Communication Technology (ICT) – Enabling and Challenging Critical Infrastructure,* In: Risk and Interdependencies in Critical Infrastructures. A Guideline for Analysis. Springer, London, 2012.

Maria B. Line, Gorm I. Johansen, and Hanne Sæle. *Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS,* SINTEF Technical Report, 2012.

Maria B. Line. *Sårbare strømmålere,* Feature article in Adresseavisen, 2012.

Jan Onarheim, Kjell Sand, Jens Auset, Eilert Henriksen, and Maria B. Line. *Smart strøm,* Information film by NTNU/Department of Electric Power Engineering and The Norwegian Smartgrid Centre Trondheim, 2012.

Inger Anne Tøndel, Martin Gilje Jaatun, and Maria B. Line. *Threat modeling of AMI,* 7th International Workshop on Critical Information Infrastructures Security (CRITIS) 2012, Lillehammer, Norway.

Maria B. Line. *Preparing for the Smart Grids: Improving Information Security Management in the Power Industry,* Feature article in ERCIM News, 2013.

Maria B. Line. *A Case Study: Preparing for the Smart Grids – Identifying Current Practice for Information Security Incident Management in the Power Industry,* 7th International Conference on IT Security Incident Management and IT Forensics (IMF) 2013, Nürnberg, Germany.

Inger Anne Tøndel, Maria B. Line, Gorm I. Johansen, and Martin Gilje Jaatun. *Risikoanalyse av AMS knyttet til informasjonssikkerhet og personvern,* NEF Teknisk rapport, 2014.

Maria B. Line. *Eksersis mot strømhackere,* Feature article in Teknisk Ukeblad, 2014.

Cathrine Hove, Marte Tårnes, Maria B. Line, and Karin Bernsmed. *Information security incident management: Identified practice in large organizations,* 8th International Conference on IT Security Incident Management and IT Forensics (IMF) 2014, Münster, Germany.

Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard A. Kemmerer. *Vær IT-beredt,* Feature article in Energiteknikk, 2014.

Maria B. Line and Bjørn J. Villa. *Offentlige WiFi-nett er en større sikkerhetsrisiko enn falske basestasjoner,* Feature article in Aftenposten, 2014.

Inger Anne Tøndel, Maria B. Line, and Gorm I. Johansen. *Assessing information security risks of AMI: What makes it so difficult?* 1st International Conference on Information Systems Security and Privacy 2015, Angers, France.

Maria B. Line and Nils Brede Moe. *Hvorfor øves det så lite på IT-kriser?* Feature article in Teknisk Ukeblad, 2015.

List of Figures

List of Tables

Part I

SUMMARY OF STUDIES

1. Motivation and objectives

The electric power industry is currently implementing smarter distribution grids. Increasing numbers of electric cars, higher peaks of power consumption during the day, a need for storage of energy, zero buildings, and the demand for local power production are the main reasons for the need for modernization. Besides, the European Commission has stated its 20-20-20 climate and energy targets for 2020: 20% reduction in greenhouse gas emissions, 20% improvement in energy efficiency, and 20% increased use of renewable resources [3]. Further, Norwegian authorities have stated the requirement of complete roll-out of smart meters by 2019 [4], which concerns all Distribution System Operators (DSOs) responsible for the electric power distribution grid and their customers. These requirements imply functionalities such as monitoring, automatic failure detection, and remote control being implemented into the power grid, supporting more efficient operation and partly autonomous management. Introduction of new technologies leads to increased connectivity and complexity, and "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 [5]. As industrial control systems are used for controlling crucial parts of the society's critical infrastructure, incidents may have catastrophic consequences for our physical environment in addition to major costs for the organizations that are hit [6].

Well-known attacks like Stuxnet/Duqu/Flame [7–10], NightDragon [11], and the cyberespionage campaign by Dragonfly [12], as well as statistics presented by ICS-CERT [13], 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 [13] expresses an explicit concern for vulnerable control systems being accessible from the Internet and for unprotected control devices. Hence, the technological changes in the 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.

Different kinds of information security mechanisms are of crucial importance in order to prevent the great variety of incidents. Still, it is impossible, and also economically infeasible, to prevent all incidents. Furthermore, new threats may occur in the near future that are impossible to foresee. These 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. Information security incident management is the process of detecting and responding to incidents, including supplementary work as learning from the incidents, using lessons learnt as input in the overall risk assessments, and identifying improvements to the implemented incident

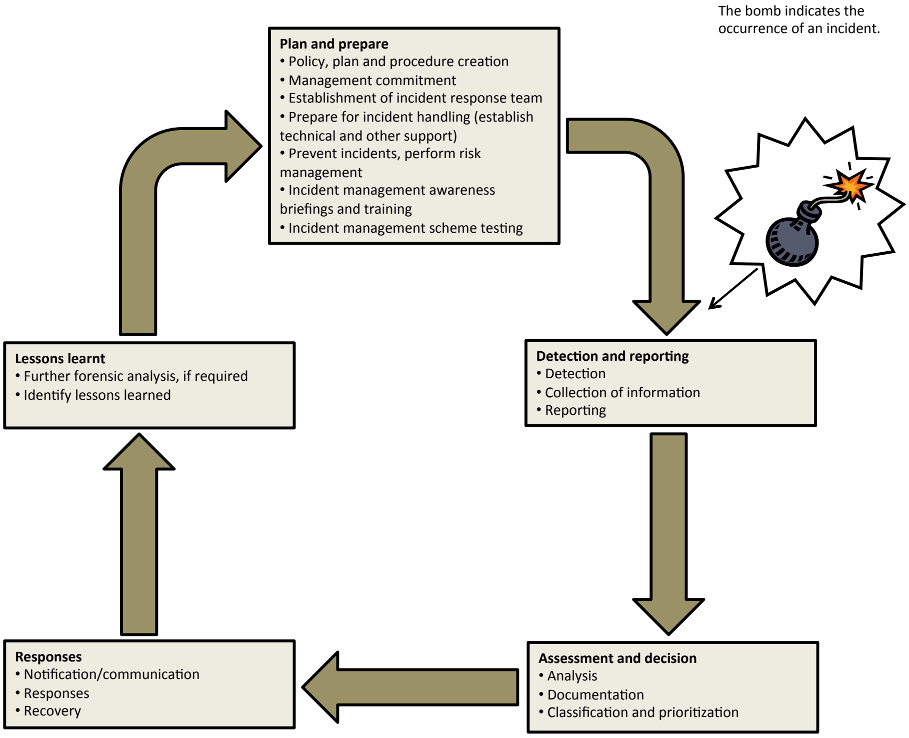

The bomb indicates the occurrence of an incident.
Plan and prepare
• Policy, plan and procedure creation
• Management commitment
• Establishment of incident response team
• Prepare for incident handling (establish technical and other support)
• Prevent incidents, perform risk management
• Incident management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

Figure 1: The information security incident management process (ISO/IEC 27035 [1]).

management scheme. Further, preparatory activities such as establishing a response team, defining roles and responsibilities, documenting procedures, and training are also included in the incident management process [1]. The complete process is described by *ISO/IEC 27035 – Information security incident management* [1] and illustrated in Figure 1. 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 [1, 14].

The National Institute of Standards and Technology (NIST) pointed out a lack of research and experience related to incident response in operating environments where IT and control systems are closely integrated, as current recommendations contain high-level requirements regarding governance, risk, and compliance only [15], and ISO/IEC 27035 addresses corporate systems in general and does not contain any considerations related more specifically to industrial control systems.

1.1 Research questions and design

Due to the major technological changes to industrial control systems in the near future and the lack of research and experiences related to incident response in such environments, there is a need for investigations in this area. A study of current practice and challenges is needed in order to identify potential improvements. The main objective of this doctoral project was to explore information security incident management practices in electric power companies and understand challenges for improvements. The work was guided by the following research questions:

RQ 1. Which factors affect information security incident management practices?

RQ 2. What are the challenges for improving information security incident management practices?

Three literature studies and three empirical studies have been conducted, and a total of ten Distribution System Operators (DSOs) in the electric power industry in Norway have participated. The studies are summarized in Table 1. The research method, the studies, and the industrial case context are further elaborated in Chapter 3.

Table 1: Studies performed and the resulting papers.

Study	**Purpose**	**Paper**
Literature studies	To survey information security challenges in smart grids, to identify empirically documented incident management practices and challenges, and to explore adaptive management strategies for adoption to information security incident management.	P1, P2, P3, P4
Study 1	To survey **current practice** for information security incident management. IT managers, IT security managers, and control room managers in six large and three small DSOs were interviewed.	P5, P6, P7
Study 2	To survey the level of **cyber situation awareness** in order to analyze the level of preparedness in DSOs for targeted attacks. The six large DSOs from Study 1 participated.	P8
Study 3	To understand challenges met during **preparedness exercises** for information security incidents in order to provide recommendations for future exercises. Observations were performed in three large DSOs.	P9

1.2 Included papers

P1-P4 resulted from the literature studies performed in the early phase of this doctoral project. P5-P7, P8, and P9 present results from Study 1, 2, and 3, respectively. Each paper is given a short introduction in the following.

P1: Maria B. Line, Inger Anne Tøndel, and Martin Gilje Jaatun: *Cyber Security Challenges in Smart Grids*, IEEE PES Innovative Smart Grid Technologies 2011, ISSN 2165-4816, Manchester, UK.
Information security challenges for the smart grids are presented: increased connectivity, new trust models, security management on several levels, software vulnerabilities, consumer's privacy, and human factors. The amalgamation of power grids and information technology systems is discussed, and a parallel from the oil and gas industry is drawn, where the same kind of evolution has been going on with the so-called integrated operations. Moreover, differences and similarities between traditional safety and information security are pointed out, as they represent two different cultures that need to cooperate closely as a result of the implementation of smart grids. Finally, a roadmap for smart grids is presented, which describes good practices to be applied and research tasks ahead, and incident response is among these tasks.
Contributes to key findings: 1, 6.

P2: Maria B. Line: *Why securing smart grids is not just a straightforward consultancy exercise*, Security and Communication Networks, ISSN 193-0114, vol. 7, no. 1, p. 160-174, January 2014.
Concerns are presented that need to be addressed in order for the implementation of smart grids to succeed from an information security point of view. These concerns include the need for a unified terminology, a cross-cultural understanding, and a cross-disciplinary cooperation both in academia and industry. Risk assessments, privacy, security architecture, and incident management are quite detailed elaborated as challenges that may stand in the way of a successful implementation of smart grids.
Contributes to key findings: 2, 6.

P3: Inger Anne Tøndel, Maria B. Line, and Martin G. Jaatun: *Information security incident management: Current practice as reported in the literature*, Computers & Security, ISSN 0167-4048, vol. 45, p. 42-57, September 2014.
A systematic literature review on current practice and experiences with incident management is presented, covering a variety of organizations. Experience reports and empirical studies were included in the review. Identified practices are summarized according to the incident management process as described in ISO/IEC 27035. Our findings show that current practices seem to be in line with the standard. There are however some recommendations that are challenging to follow in practice. Some inspirational examples are identified that should be useful for organizations looking to improve their practices. Besides, suggestions are provided for how challenges could be addressed, and research needs within information security incident management are identified.
Contributes to key findings: 1, 3, 7.

P4: Maria B. Line and Eirik Albrechtsen: *Examining the suitability of industrial safety management approaches for information security incident management*, forthcoming in International Journal of Information and Computer Security, ISSN 2056-4961.
This paper addresses some of the challenges identified in P3 by applying principles and theories from adaptive management strategies such as resilience engineering to the field of information security incident management. Three areas are discussed in particular: plans, compliance, and situational adaptation; training; and learning from incidents. Although there are several similarities between them, these two fields have been the subjects of quite different research approaches and solutions, a phenomenon that might be explained by four interlinked reasons: maturity, individual awareness, national regulations, and traditions.
Contributes to key findings: 5, 7.

P5: Maria B. Line: *A Study of Resilience within Information Security in the Power Industry*, IEEE Africon 2013, ISSN 2153-0025, Mauritius.
The main principles of resilience engineering and high-reliability organizations (HRO) are presented in relation to each of the five phases of the incident management process as described by ISO/IEC 27035. Preliminary results from the interviews with large DSOs are discussed with respect to how well current practices in large DSOs align with the principles of resilience and HRO. The analysis indicates that there are lacks in current practices when it comes to plans, training, learning from minor incidents and things that go right, and systematic approaches to information security metrics. An increased focus on these activities, which are key areas in the literature on resilience and HRO, would improve resilience for information security incidents.
Contributes to key findings: 5, 7.

P6: Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun: *Information security incident management: Planning for failure*, 8th International Conference on IT Security Incident Management and IT Forensics (IMF) 2014, Münster, Germany, ISBN 978-1-4799-4330-2.
Findings from the first round of interviews are presented: current practice regarding planning and preparatory activities for incident management in six large DSOs. Similarities and differences between the two traditions of conventional IT systems and industrial control systems (ICS) are identified. The findings show that there are differences between the IT and ICS disciplines in how they perceive an information security incident and how they plan and prepare for responding to such. The completeness of documented plans and procedures for incident management varies. Even if documentation exists, it is not well-established throughout the organization. Preparedness exercises with specific focus on information security are rarely performed. There is a need to create a more unified approach to information security incident management

in order for the electric power industry to be sufficiently prepared to meet the challenges following the implementation of smart grids in the near future.
Contributes to key findings: 1, 2, 3, 5, 6.

P7: Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun: *Does size matter? Information security incident management in large and small industrial control organizations*, submitted to International Journal of Critical Infrastructure Protection, ISSN 1874-5482.
Planning and preparatory activities in small DSOs are presented and compared to the practices in large DSOs, as described in P6. Further, activities in both large and small DSOs from the remaining phases of the incident management process beyond planning and preparations are presented and compared: detection, assessment, responses, and lessons learnt. Significant differences are emphasized. Activities where the practices do not seem to be affected by the size of the DSOs are summarized, before recommendations to all DSOs are provided. The recommendations are intended to improve preparedness for information security incidents.
Contributes to key findings: 1, 2, 3, 4, 5, 6, 7.

P8: Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard A. Kemmerer: *Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?* 2nd Smart Energy Grid Security Workshop (SEGS) 2014, ISBN 978-1-4503-3154-8, Phoenix (AZ), US.
A new taxonomy for targeted attacks is presented and used for providing insight into the importance of different aspects of cyber situation awareness for defending against such targeted attacks. Further, a systematic assessment of cyber situation awareness in large DSOs is presented. Our findings indicate that the electric power industry is very well prepared for traditional threats, such as physical attacks. However, cyber attacks, and especially sophisticated targeted attacks, where social engineering is one of the strategies used, have not been appropriately addressed so far. By understanding previous attacks and learning from them, our aim is to aid the industry in improving their detection mechanisms and response capabilities. A list of prioritized suggestions for theses DSOs is provided, which is intended to increase their cyber situation awareness.
Contributes to key findings: 1, 2, 5.

P9: Maria B. Line and Nils Brede Moe: *Understanding Collaborative Challenges in IT Security Preparedness Exercises*, International Conference on ICT Systems Security and Privacy Protection (IFIP SEC), ISSN 1868-4238, Hamburg, Germany, 2015.
Previous interview studies (P5-P8) have shown that information security preparedness exercises are not prioritized by DSOs for a number of reasons. Such exercises allow for reviews of written plans and procedures and practical

training of personnel, which in turn lead to improved response capabilities for an organization. We encouraged DSOs to conduct such exercises and observed one tabletop exercise as performed by three different DSOs. We argue that challenges met during exercises could affect the response process during a real-life incident as well, and by improving the exercises the response capabilities would be strengthened accordingly. We found that the response team must be carefully selected to include the right competences and all parties that would be involved in a real incident response process. Furthermore, the main goal needs to be well understood among the whole team and a certain time pressure during the exercise adds realism to it. Both the exercise itself and existing procedures need to be reviewed afterwards. Finally, organizations need to both optimize current exercise practices and experiment with new ones, as there are many ways to conduct preparedness exercises.
Contributes to key findings: 3, 5, 7, 8.

1.3 Contributions

We have investigated current practices for information security incident management in ten organizations in the Norwegian electric power industry and identified challenges for improvement of these practices. The main contributions of this thesis are:

- *Knowledge on factors affecting current incident management practices.* The level of risk perception, organizational structure, and the amount of available financial and human resources have been identified as factors affecting current incident management practices. An understanding of these factors is a prerequisite for enabling improvements with the goal of ensuring effective and efficient incident response.
- *Knowledge on challenges for improving current incident management practices.* The importance of creating cross-functional and self-managing teams for both training and real emergency situations has been demonstrated. Further, the need for establishing a learning system has been identified, as learning from neither training nor real incidents is currently sufficiently performed. Challenges for improvements need to be understood in order to achieve effective and efficient incident response.
- *Application of organizational theory to information security incident management.* Information security has traditionally been occupied mainly by a focus on technical security mechanisms and compliance. This thesis demonstrates application of organizational theory, including adaptive management strategies, to information security incident management. Organizational theory is needed to understand obstacles for implementing practices and developing new practices.
- *Empirical knowledge on information security in industrial control organizations.* Major technological changes are currently being implemented

in industrial control systems, leading to increased connectivity and complexity, which require appropriate and sufficient information security measures. This can only be achieved by a thorough understanding of both technological and organizational matters. The amount of empirical information security research studies in industrial control organizations is currently rather limited. This thesis contributes to the body of knowledge on information security practices and challenges in industrial control organizations, and to increased awareness and knowledge of information security in the organizations participating in our research and the Norwegian electric power industry as a whole.

1.4 Outline

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

Appendices are included in Part II, while Part III presents the scientific papers that resulted from this PhD project.

2. Background

Information security comprises the three attributes of confidentiality, integrity, and availability, as defined by ISO/IEC 27000 [16]:

- *Confidentiality:* the property that information is not made available or disclosed to unauthorized individuals, entities, or processes,
- *Integrity:* the property of safeguarding the accuracy and completeness of assets, and
- *Availability:* the property of being accessible and usable upon demand by an authorized entity.

Data security, cyber security, and computer security are similar terms that can be observed in different contexts. However, throughout this thesis the term *information security* will be used, as this is the most recognized and correct term as defined by ISO/IEC 27000.

Information security incidents and the incident management process are presented in the following. Further, information security in the context of industrial control systems is introduced. Then, the concept of cyber situation awareness and the principles of resilience engineering are described as concerning human factors in incident management. Preparedness exercises are introduced as a means of improving the incident management process, and finally, coordination in incident response is described, including the issues of self-management, team knowledge, and joint decision-making.

2.1 Information security incidents

An information security event is defined to be “an identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant” [16]. An information security incident is then defined as “a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security” [16]. In this thesis, we use the definition provided by ISO/IEC 27000 and include both intentional and unintentional incidents, as both types might have major consequences for the information security properties of both IT and control systems.

2.2 Information security incident management

The information security incident management process and the ISO/IEC 27035 [1] that describes it, were briefly introduced in Chapter 1. The process comprises five phases:

1. *Plan and prepare*,
2. *Detection and reporting*,
3. *Assessment and decision*,
4. *Responses*, and
5. *Lessons learnt.*

The first phase runs continuously, as opposed to the next four, which are triggered by the occurrence of an incident. *Plan and prepare* includes activities such as establishing a dedicated response team, defining roles and responsibilities, documenting procedures, and 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. Deciding what kind of response is needed to cope with the registered event belongs to the *Assessment and decision* phase. The *Responses* phase then describes the actions taken to cope with the incident and prevent further consequences, restore systems, collect electronic evidence, and possibly escalate to crisis handling. The final phase, *Lessons learned*, is when 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. The improvements are then implemented as part of the continuously running phase of *Plan and prepare*. Similar recommendations are described by NIST [17], ITIL [18], and ENISA [19] as well. Existing standards and recommendations in the area of incident management provide a useful baseline for organizations about to implement their own scheme or looking for inspiration for improvements, and ISO/IEC 27035 should be regarded as the most comprehensive and internationally recognized documentation of what is currently the recommended practice in this field. The standard is used as a basis for the interview studies performed in this project.

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 [20]. Findings by Ahmad et al. [21] indicated 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 a potential for being more useful from a learning perspective rather than having major consequences. Scholl and Mangold [22] 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 comprised by pattern recognition, hypothesis generation, and cooperation [23]. Besides, incident response is a highly collaborative activity, and the diagnosis work is complicated by the practitioners' need to rely on tacit knowledge and usability issues with security tools [24]. Both technical, human, and organzational issues will be investigated as part of our studies in identifying factors affecting current practices and challenges for improvements.

2.3 Information security and industrial control systems

Industrial control systems have traditionally been based on proprietary technologies operating in closed networks. They have been designed to fulfill specific purposes and have by many not been recognized as IT, even though they are a combination of hard-, firm-, and software. The security objectives have been limited, as availability has been the prioritized property. Confidentiality and integrity have not received the same attention, due to the nature of the systems [25]. Traditional IT systems, on the other hand, consist of commercial-off-the-shelf technologies operating on TCP/IP/Ethernet networks, and they are usually designed to fulfill multiple purposes. Incidents affecting power systems may have severe consequences, both for business operations and the society at large, including life, health, and the physical environment. Such incidents tend to be more associated with safety than information security, and hence the industrial control systems have been designed to meet safety requirements. This is also what characterizes the mindset of the staff operating these systems [26].

The electric power industry is currently modernizing the power grids in order to achieve the goal of smart grids. These changes concern new technologies, such as introducing IT into control systems, higher connectivity, and more integration, which increase the attack surface and the potential consequences of attacks [27]. At the same time, current threat reports show that targeted attacks are on the rise, and critical infrastructures are attractive targets [28]. This calls for increased knowledge and understanding of information security in the setting of co-functioning IT and industrial control systems: technical security measures and organizational aspects, knowledge exchange and cooperation between different types of personnel, detecting and responding to incidents, and understanding of threats and potential consequences of incidents. NIST has provided several recommendations for securing industrial control systems, including a comprehensive overview of vulnerabilities [29]. There is however a lack of standards and recommendations for incident response in settings where corporate IT systems and industrial control systems co-function and where incidents might have cascading consequences, as mentioned in Chapter 1.

In their study on incident management in the oil and gas industry, Jaatun et al. [26] found that although integrated operations in the North Sea were highly dependent on IT, there was still a great deal of mistrust between traditional process control engineers and IT staff. Further, there was a low level of awareness among upper management of the importance of doing cyber security training exercises due to both a low number of cyber security incidents and limited systematic reporting of these. Some control system engineers even refused to acknowledge that their systems contained vital IT components. Finally, they found that existing reporting tools used for Health, Safety, and Environment (HSE) incidents were poorly suited for reporting of cyber security incidents.

Research on information security incident management in environments with co-functioning IT systems and industrial control systems is currently limited. There is a gap of knowledge and understanding of both current practices and related challenges for incident management, and compliance to standards and/or 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.

2.4 The human factor: cyber situation awareness and resilience engineering

When technology fails, the human factor is of great importance. However, as computer systems are ever-changing and new threats emerge continuously, it is quite a challenge to educate all users to be well functioning perimeter controls for an organization. Still, human system operators need to be able to interpret alerts, put pieces of information together, and 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. [30] situation awareness can in general be described as a three-phase process: situation recognition, situation comprehension, and situation projection. Tadda [31] provides an overview of metrics developed for measuring the performance of CSA systems. He specifically points out the need for research in measuring the level of situation awareness achieved by human operators, and he indicates that it would require quite different means than measuring the performance of a computer system. Cyber situational awareness for industrial control systems, and the power grid in particular, has received attention lately [32]. Research areas include frameworks that comprise collection and analysis of network traffic data, simulation systems, intrusion detection systems. One example is Klump and Kwiatkowski [33], who proposed an architecture for sharing information about incidents in the power system.

The concept of CSA relates to the field of resilience engineering as both regard abilities of understanding the current situation, potential changes, and consequences thereof. Resilience engineering is a fairly recent development within industrial safety and concerns an organization's ability to succeed under varying conditions. It is usually explained by four principles [2], as illustrated in Figure 2:

- *Actual:* The ability to address the *actual* is knowing what to *do*, 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*, 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*, 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*, being able to anticipate developments, threats or opportunities into the future and imagine how they can affect the organization through changes or disruptions.

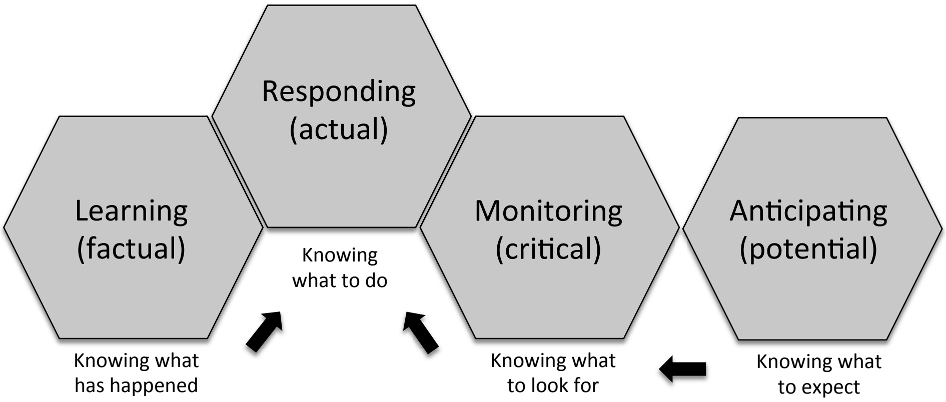


Figure 2: The four basic abilities of resilience [2].

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 for dealing with the unexpected and able to adapt to the occurring situations. Resilience is not a product that can be implemented in a day or a week. It is an immanent property that can be developed over time, piece by piece, and it touches upon individuals, teams, culture, and priorities.

In spite of the need for individual planning for each organization, training is a common key factor when it comes to improving resilience. The more experienced each worker is in anticipating and responding to incidents, the better prepared will they be for recognizing and responding to unexpected events. In fact, Pariès, in Hollnagel et al. [34], states that it takes "a subtle balance between experience and opportunism, self confidence and awareness of limitations" to succeed in extreme situations.

2.5 Information security preparedness exercises

The purpose of an emergency preparedness exercise is to strengthen the response capabilities of an organization by training personnel in responding to situations that deviate from normal operations. Basic structures such as well documented procedures and clear definitions of roles and responsibilities need to be in place, but during an incident, there is a need for a more dynamic process that requires coordination and improvisation, and where exceptions and violations are managed, and experienced incident handlers are valued. Relying on predefined documentation is what Hale and Borys refer to as Model 1 in the use of safety rules and procedures [35], while allowing for rules to emerge from practical experience is referred to as Model 2. Exercises are a way of developing Model 2. Further, exercises provide a means for personnel to train for making the right decisions under pressure [2]. Wrong decisions may cause the incident to escalate and lead to severe consequences.

Both tabletop exercises and functional exercises prepare personnel for responding to an emergency situation [36]. 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. Tabletop exercises are usually performed in a classroom without the use of any specific equipment, and a facilitator presents a scenario and initiates the discussion. Functional exercises, on the other hand, involve practical simulations of incidents with the use of physical equipment and execution of procedures, such as alerting and reporting. According to NIST, both types of exercises should consist of the following four phases:

1. *Design* the event by identifying objectives and participants,
2. *Develop* the scenario and guides for the facilitator and the participants,
3. *Conduct* the exercise, and
4. *Evaluate* by debriefing and identifying lessons learned [36].

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 [37], while this is exactly what is supported by functional exercises.

In his study of preparedness exercises initiated by the Norwegian Water and Energy Directorate (NVE)[1], Gåsland [38] found that there is a positive attitude for participating in exercises and an understanding that collaboration is important in problem-solving processes. He still found that exercises compete

[1] http://www.nve.no

with daily tasks for prioritization, and he considered it to be an obstacle to learning if exercises are not used as a means of making improvements afterwards. Further, he emphasized the importance of making exercises as realistic as possible. However, creating realistic scenarios is challenging [39], and even though a scenario is successfully responded to in an exercise, it does not give any guarantees that a real emergency situation will be successfully responded to [40].

2.6 Coordination in incident response

Coordination of work and making collaborative decisions are important aspects of the incident response process and hence of preparedness exercises as well. Responding to an information security incident usually implies personnel from different parts of an organization collaborating on solving complex problems. “Coordination is management of interdependencies between activities” [41] and coordination mechanisms are the organizational arrangements that allow individuals to realize a collective performance [42]. Interdependencies include sharing of resources, synchronization of activities, and prerequisite activities. Coordination challenges in incident response are functions of the complexity of i.e. 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 [43]. 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 [42]. 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 [44]. 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 [45]:

- *Predefined coordination* takes place prior to the situation being coordinated and can be understood as what Hale and Borys refer to as Model 1 [35]. 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 [1].
- *Situated coordination* occurs when a situation is unknown and/or unanticipated, such as when an information security incident strikes, and can

> be understood as Model 2 [35]. Those involved in the situation do not know in advance how they should contribute. They lack knowledge of what to achieve, who does what, how the work can be divided, in what sequence sub-activities should be done, when to act, etc. Consequently, they have to improvise and coordinate their efforts ad hoc. In most collaborative efforts there is a mix of predefined and situated coordination. Involved actors may for instance already know the goal, but not who performs what, or they may know who does what, but not when to do it. To compensate for lacking predefined knowledge of how the actual unfolding of activities in an exercise will be, the participants must update themselves on the status of the situation.

To handle a crisis, not only does the team need to coordinate their work, they also need to take decisions together and be responsible for managing and monitoring their own processes and executing tasks; they need to be able to self-manage [46]. Flodeen, Haller, and Tjaden [47] studied an ad hoc group of incident responders to see how a shared mental model for decision making can be developed through training. Such a shared mental model increases the performance during an incident handling process because the team manages to cooperate with limited and efficient communication. They would 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.

3. Research method

The research questions called for exploratory research and a flexible design [48]. We used an *inductive research approach* as we wanted to derive patterns from our observations rather than evaluating existing hypothesis. Field studies were performed and followed by the deriving of theories from observations, which is also called theory-building research [49]. This method is in contrast to *deductive research*, where a theory is developed initially, followed by observations to evaluate it [50].

A case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context [51]. It relies on multiple sources of evidence and benefits from the prior development of theoretical propositions to guide data collection and analysis. Case studies are well suited for "development of detailed, intensive knowledge about a single 'case', or of a small number of related 'cases'" [48] and were thus chosen as the preferred research strategy.

Qualitative interviews are a well-known and powerful tool for information collection in qualitative research [52]. They allow for the researchers to view the phenomenon from the interviewees' perspective and understand why and how they got that particular perspective [53]. To meet this objective, qualitative interviews are driven by open questions, a low degree of structure, and a focus on specific situations and experiences made by the interviewee. We performed *semi-structured interviews*, which are based on a set of predefined questions, but allow for additional, unplanned questions or a change in the order of questions [48]. Further, a *document analysis*, which is often used to question or to verify data obtained from other data collection methods [51], was performed in one of our studies.

Observations are typically used in an exploratory phase to find out what is going on in a specific situation, and *participant observation* is one common approach [48]. The degree of participation may vary, depending on the purpose of the observation. The complete participant conceals that she is an observer and participates as if she was a full member of the group being observed, while the *participant as observer* and the *marginal participant* need to be trusted by the group members as her role as observer is known to them. The presence of the observer might affect the group being observed, and there are a number of biases that need to be handled with care as well, such as selective attention, selective encoding, selective memory, and interpersonal factors [48]. Still, participant observation is powerful in dealing with complex situations.

The data analysis followed an integrated approach, which combines the inductive development of codes with a start list of categories, i.e. groups of codes, in which the codes can be inductively developed [54, 55]. A code is a descriptive label for a word, sentence, paragraph, or other chunks of data [56], and coding is a means of organizing and interpreting qualitative data.

Validity issues need to be considered when designing a research project and evaluated when analyzing the credibility of research results. *Construct validity* concerns whether a study measures what it sets out to measure [48]. Both interviewees and the researcher may be biased, either consciously or unconsciously [57]. Bias may be overcome by a number of strategies, such as triangulation and member checking. Data triangulation means using several methods for collecting evidence, such as interviews, document analysis, and observations. This allows for studying a phenomenon from different perspectives and increases data quality [51]. Member checking involves returning data material to the respondents for review and shows that their contributions are valued. *External validity* refers to the degree to which the findings from a study can be generalized to other settings [48]. Generalizability is strengthened by increasing the number of studies. A description of the industrial case context is of great importance when considering whether results from qualitative studies are transferrable to a given setting. A discussion on validity issues of our studies is provided in Chapter 5.

In the following, the studies performed in this doctoral project are presented with respect to research design, data collection, and data analysis. Then, the industrial case context with the participating DSOs is introduced, before privacy and confidentiality issues are described.

3.1 Data collection and analysis

Literature studies (P1-P4). Security challenges and research needs for smart grids were studied in order to identify research questions for this thesis. The studies are presented in P1 and P2. Identification and evaluation of empirical studies and experience reports on incident management practices were performed as a systematic literature review [58] and documented in P3. A literature study on theories and principles from resilience engineering was performed to identify possible approaches to be applied in information security incident management, as presented in P4.

Study 1: Current practice (P5-P7). This study was based on semi-structured interviews and a document analysis. Requested documents included existing plans and procedures and evaluation reports from past incidents. Content of this documentation was mapped to findings in interviews and a comparison between the participants' views and documentation was performed. Documentation was however not received from all participating organizations due to confidentiality restrictions.

ISO/IEC 27035 [1] was used as a basis for developing the interview guide. The first version of the interview guide that was used for large DSOs, is found as an appendix in P5. We revised this interview guide before interviewing the small DSOs: some questions were added (6, 17, 30, 31, 33, and 34) and one was removed. The removed question asked what the most important actions were in the response phase, but the question was too vague and was interpreted very differently by interviewees in the first phase. 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 revised interview guide is included in Appendix II.

The interview guide was not distributed in advance, as we wanted to collect experiences and practices from the employees directly, rather than having them refer to a set of predefined procedures. Three roles were interviewed in each organization: IT managers, IT security managers, and control room managers. In the small DSOs, the IT manager and the IT security manager was the same person. In total, 19 interviews in six large and three small DSOs were conducted. Each interview lasted for approximately one hour.

The start list of categories for coding was based on the five phases of ISO/IEC 27035 [1], cf. Figure 1. Nodes were defined in advance in a hierarchy of two levels. One researcher conducted all the interviews and performed the coding. The confidentiality agreements signed with some of the participating organization posed limitations on who may access the material revealed in the interviews. Fellow researchers assisted in reviewing the coding categories, discussing findings, and drawing conclusions, without compromising the confidentiality agreements. Nvivo [59] was used for coding and analysis of the data material. The results were documented in P6 and P7. Additionally, P5 analyzed preliminary results in light of resilience engineering principles.

Study 2: Awareness (P8). This study was based on semi-structured interviews. The interview guide was developed based on a categorization of elements comprising cyber situation awareness (CSA). One fellow researcher and one expert from a supplier of control systems assisted in evaluating the questions. The interview guide is presented in Appendix II together with a mapping between the CSA capabilities and the interview questions.

IT security managers for the control systems were asked to participate. The interview guide was distributed in advance, so that the DSOs could determine who would be the right participant(s). Two of the interviews were performed as group interviews with three persons, while the other four were individual interviews. A total of six interviews were conducted, and the participating DSOs were the same large DSOs as in Study 1. Due to this low number of interviews, extensive coding was not needed. A summary of each interview was written, so that the fellow researchers could discuss findings and contribute to the analysis. The summaries provided sufficient insight for writing up the results, which were documented in P8.

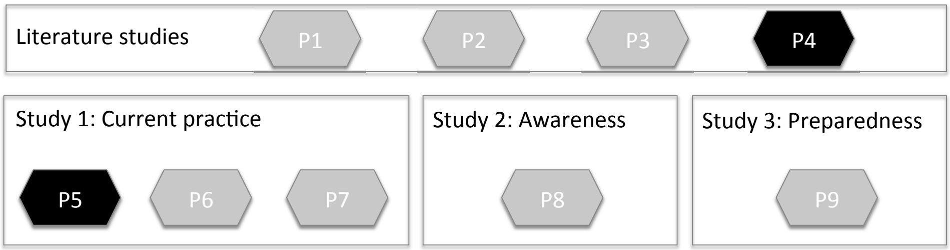


Figure 3: The studies performed and the resulting papers. All papers contribute to both research questions, except from P4 and P5, which address RQ 2 only; thus colored differently than the others.

Study 3: Preparedness (P9). A holistic multiple case study [51] was performed in Study 3. We contributed to planning the tabletop exercises in each of the organizations and acted as a participant observer [48] studying leadership, decision-making, and involvement. Further, we facilitated a plenary evaluation after the exercise, where all participants reflected upon what worked well and what could have been done differently. Three organizations were studied, and they all used the same scenario as a basis for their exercise, although they organized the exercise slightly different from one another. The participants did not receive any information about the exercise in advance, other than the topic being an information security incident and the activity being a table-top exercise.

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. The results were documented in P9.

The studies and the resulting papers are illustrated in Figure 3. P4 and P5 address RQ 2 only, while the others contribute to both research questions.

3.2 Industrial case context

In total, seven large and three small DSOs participated in our empirical studies, c.f. Table 2. The large DSOs are among the top 15 largest DSOs in Norway with respect to the number of energy subscribers, 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 thousands subscribers.

Four of the large DSOs have outsourced the operation of IT systems and networks to an external supplier, while the remaining two operate these in-house. The three small DSOs rely on an external supplier as well. All the DSOs

Table 2: Types of DSOs participating in our empirical studies.

Study	Participating organizations
1	Six large and three small distribution system operators (DSOs)
2	The same six large DSOs as in Study 1
3	Three large DSOs; two from Study 2 and one additional

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.

3.3 Privacy and confidentiality issues

All interviews in Study 1 and 2 were voice recorded and transcribed. They were registered at the Data Protection Official for Research[2]. All respondents signed a consent agreement, cf. Appendix II[3]. Most DSOs required that the researcher who performed the interviews, signed a non-disclosure agreement.

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

[3] The consent agreement is in Norwegian. An English translation of the text is included in this appendix as well.

4. Results

The research questions were explored through literature studies (P1-P4) and three empirical studies (P5-P9). Knowledge acquired through all studies are synthesized into key findings, as presented in the following, cf. Table 3. The key findings concern practices in the electric power industry.

Table 3: A summary of key findings and how they relate to the research questions.

No	RQ	Key finding	Paper
1	1	Detection mechanisms are insufficiently applied.	P1, P3, P6, P7, P8
2	1	The absence of major incidents limits preparatory activities.	P2, P6, P7, P8
3	1	Outsourcing reduces preparatory activities.	P3, P6, P7, P9
4	1	The risk perception among small DSOs is lower than among large DSOs.	P7
5	2	Training for information security incidents is not prioritized.	P4, P5, P6, P7, P8, P9
6	2	IT and control personnel understand information security differently.	P1, P2, P6, P7
7	2	Post-incident evaluations are not performed.	P3, P4, P5, P7, P9
8	2	Business managers have different perspectives and priorities than technical personnel.	P9

4.1 Factors affecting incident management practices

Figure 4 illustrates the key findings regarding current incident management practices and the relationships between these findings.

Key finding 1: Detection mechanisms are insufficiently applied.

Detection mechanisms currently in use by DSOs are not sufficient in light of current threats. Information security incidents in general can be detected in a number of ways, such as security monitoring mechanisms, employees, system administrators, external notifications, and log reviews [P3]. Current tools have their limitations regarding accuracy and usability [P3]. Further, firewalls and detection systems are best suited for detecting known attacks [P8]. New attacks that are specifically tailored and targeted, will not be detected by such mechanisms. Human and organizational abilities such as understanding early signs of incidents and being prepared for responding to unexpected incidents are therefore of crucial importance, in addition to automatic detection mechanisms [P1, P3, P8].

DSOs do not have sufficient mechanisms for monitoring and detecting incidents on the inside of the control systems [P8]. Detection systems are not widely implemented, and none of the DSOs have systematic approaches to following-up on logs and alerts, due to a lack of resources. Human operators are relied on for detection of irregularities. DSOs do have firewalls for detecting

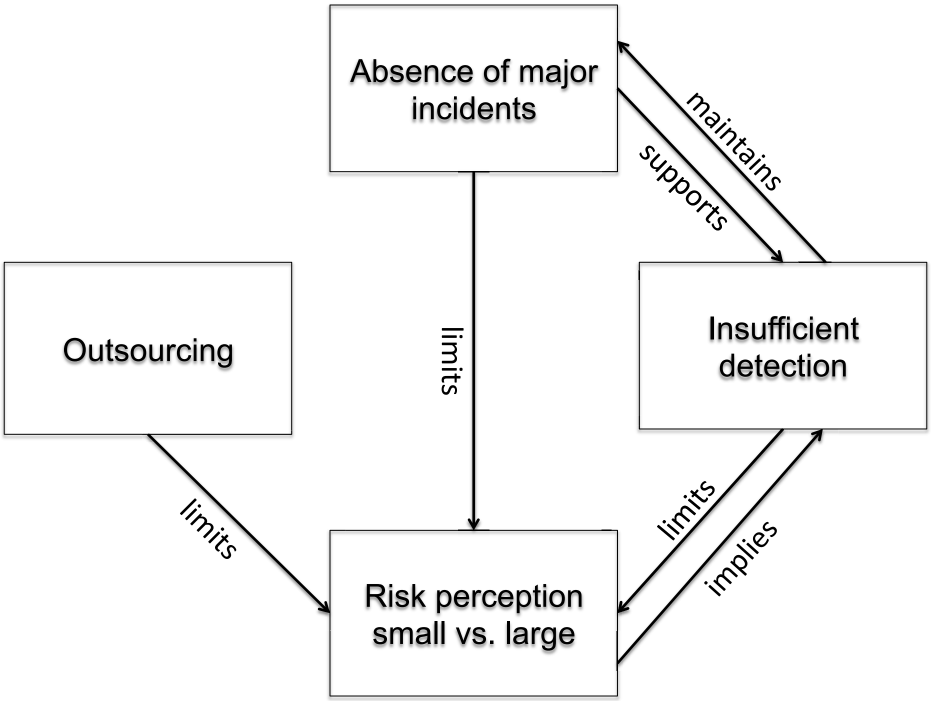


Figure 4: Key findings regarding current incident management practices (RQ1) and how the findings affect each other.

suspicious traffic into the control systems, but if an attacker is able to pass this level of security, he could operate on the inside without being monitored or detected. None of the DSOs have ever experienced any targeted attacks in the control systems [P8], although one of the large DSOs has had a malware infection in a part of the system controlling windmills [P6]. This infection was detected by one operator, who got a virus alert on his computer, as the malware spread through shared disks.

Unauthorized access to power switches was stated by all respondents to be the worst possible scenario [P6, P7, P8], far more severe than unavailable control systems. A DSO is able to operate the power grid without control systems for quite some time, while unauthorized control of power switches might lead to immediate power outages and safety risks for human operators at the premises. Therefore, several interviewees mentioned shutting down the control systems to be the prime countermeasure in case of an attack [P6, P7, P8]. However, this requires that the attack is actually detected.

Key finding 2: The absence of major incidents limits preparatory activities.

Current trends show that targeted attacks are on the rise and that the electric power industry is among the attractive targets [P8]. Power outages and other types of damage to control systems caused by hackers have been observed already [P2], but the Norwegian electric power industry has not been hit until the Dragonfly attack happened in 2014 [12]. Study 1 and 2 were carried out before this attack, and the level of preparedness and the priority assigned to incident management planning and preparatory activities among DSOs were limited at that point, particularly compared to the recommendations by ISO/IEC 27035 [P6, P7]. Nevertheless, the general feedback from the DSOs was that things go well: information security incidents do not disturb DSOs' business operations, and based on their experiences, they did not feel the need to realize major improvements in this area.

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 [P6, P7]. Even though the respondents have a realistic view of potential attackers and possible threats [P8], 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. An attack against one DSO affects the level of awareness in other DSOs. The Dragonfly attack has lead to preparedness exercises for information security receiving higher priority and to improved understanding of threats and of the importance of monitoring and analysis of incidents [P7, P8].

Key finding 3: Outsourcing reduces preparatory activities.

Outsourcing of IT services relieves an organization of several practical tasks, which are more efficiently solved by large-scale professional suppliers. However, a number of challenges related to incident management arise in outsourcing scenarios: common plans and procedures [P6], defining responsibilities [P3], and collaborative exercises [P7]. DSOs that have outsourced their IT services to an external supplier, put less effort into establishing plans and responsibilities than other DSOs [P6]. They assume that their suppliers have plans and are well prepared for responding to any types of incidents. One IT security manager in a large DSO expressed that he expected their IT supplier to perform training. Further, DSOs are confident that collaboration with their

IT supplier will be smooth and successful in case of an incident, even though collaborative plans and exercises are rare [P7].

> *"This I have never asked for, to see the procedures for responding to an information security incident. Maybe I should."*
>
> — *IT security manager in a large DSO*

One small DSO reported that they have a collaborative plan with their supplier, but they had never seen the need for collaborative exercises [P7]. One large DSO had agreements with one supplier about assistance in emergency situations, but had never included this supplier in exercises [P9], and most DSOs did not know whether their supplier had plans for incident response, or whether they performed exercises on their own. Even though there is a lack of formally defined responsibilities, none reported on having experienced any problems due to this. The reason might be the absence of major incidents so far. Whether the confidence the DSOs have in their suppliers is well-founded or not, is impossible to answer without investigating practices among suppliers.

Key finding 4: The risk perception among small DSOs is lower than among large DSOs.

Small DSOs do not see themselves as attractive targets, they can operate for a long time without their control systems, and they are confident in their own and their IT supplier's ability to respond to the worst case scenarios even though preparedness exercises for information security are never performed [P7]. Small DSOs believed that the large DSOs are more attractive targets than themselves, as they considered areas where authorities, major organizations, and a large number of residents are located to be of more interest for attackers wanting to achieve a certain impact and/or attention [P7]. Preparedness exercises based on information security incidents therefore received an even lower priority in the small DSOs than in the large DSOs. The large DSOs were more aware of their own position as possible targets for worst case scenarios. The small DSOs were asked whether they served customers that could be attractive targets for attacks, which they confirmed. This was an issue that they had previously not considered.

Small DSOs considered the consequences of attacks against their control systems to be limited, as manual operation would be manageable for a long time due to a low number of substations and good knowledge about their grid and the geographical area they serve. One small DSO stated that their control systems consisted of one server that was not connected to any other computer networks, hence the attack surface was rather limited [P7]. Large DSOs claimed to be able to operate the electric power grid without control systems as well, but not for as long as the small DSOs reported [P6, P7].

> *"It is crucial to us as a small organization to have a professional, large, and competent IT supplier on which we can rely on in such situations."*
>
> — *IT/IT security manager in a small DSO*

Small DSOs relied on their supplier to have the necessary plans, procedures, exercises, competence, equipment, and the ability to respond appropriately to incidents. Large DSOs showed the same tendency, but to a much lesser degree, and they had more IT and information security competence in-house. Besides, they realized the need for better preparations based on current and emerging threats and attacks happening to similar organizations around the world.

4.2 Challenges for improvement

Figure 5 illustrates the key findings regarding challenges for improving incident management practices and the relationships between these findings.

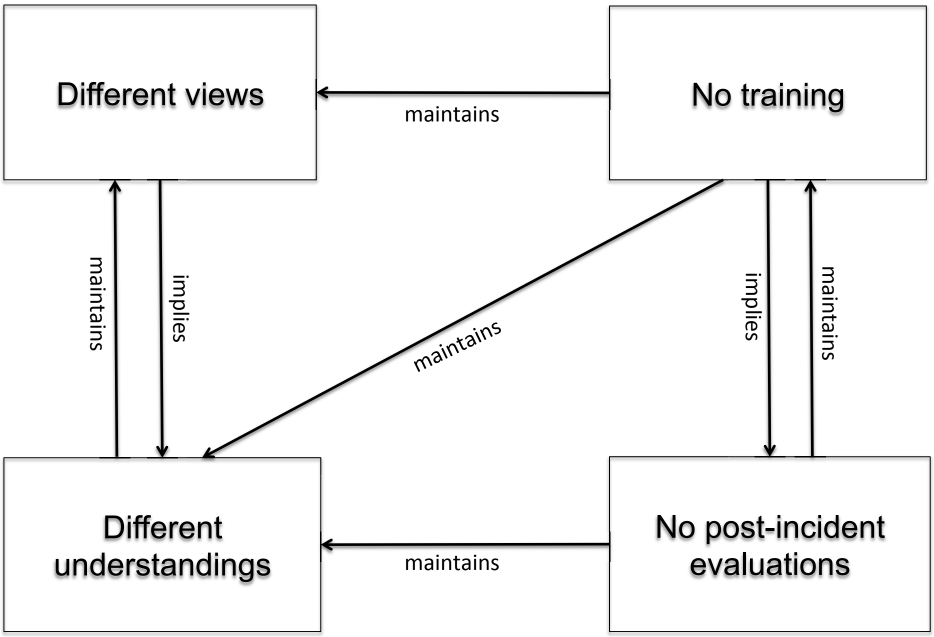


Figure 5: Key findings regarding challenges for improving incident management practices (RQ2) and how the findings affect each other.

Key finding 5: Training for information security incidents is not prioritized.

Plans for incident response have limited value if they are not rehearsed [P4]. Training drills allow for testing of existing plans and procedures and identification of improvements of such. Further, generic skills for dealing with expected and/or unexpected events are improved [P4], i.e. situated coordination or improvisation [P9], and the group develops self-management and grows team knowledge [P9].

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 emergency situation [P5, P6, P7]. Training involves a certain cost, time, and workload, which are perceived as hindrances. Besides, protecting the physical grid and the production process from fire and other physical damages is viewed as more important than protecting the IT systems, as stated by an IT manager in a small DSO [P7]. Finally, real incidents rarely occur, which adds to the perception of training not being necessary, even though information security policies require regular tests of emergency preparedness plans, including IT/infrastructure issues [P6].

> *"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*

Some of the large DSOs were working on documenting their plans for incident response when Study 1 was carried out. They found it difficult to run preparedness exercises without having written plans as a baseline [P5, P6]. In two of the three large DSOs from Study 3, existing documentation of plans and procedures was not made available during the exercise. Although some participants commented on this afterwards and wanted to have documentation available in the next exercise, situated coordination is more important than documentation during an incident response process [P9]. A certain baseline of written documentation should be in place, but the ability to adapt to situations and improvise could be trained for without this documentation being complete [P4]. An IT security manager in a large DSO said that they lack practice and established procedures in order to be well prepared for responding to the worst case scenario. He still felt confident that they would be able to improvise [P6].

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 [P6]. 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 [P6, P7, P8].

> *"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*

Key finding 6: 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, they have been the subjects of different security objectives [P2]. Further, while IT systems for a long time already have been exposed to typical Internet threats such as malware infections and deliberate hacker attacks, control systems have been operated in closed networks without these kinds of threats [P2]. A common understanding of all networked systems, threats they are exposed to, and potential consequences of incidents, is needed in the future (if not already) where IT and control systems are interconnected and dependent on each other [P1, P2].

There is a gap in knowledge and understanding of information security between IT and control personnel. IT and IT security managers responded quite uniformly when asked to define an information security incident and provide examples of such [P6]. The control room managers, on the other hand, were not able to provide a clear definition, although they did mention relevant examples. Both types of personnel anticipated similar worst case scenarios [P6], but control room personnel's ability to recognize an incident is questionable, based on their understanding, experience, and lack of sufficient technical mechanisms for such [P8]. Further, compared to IT personnel, control room personnel has quite limited experiences in responding to information security incidents [P6, P7].

One of the first questions asked to 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 [P6]. IT and IT security managers considered all three properties for the administrative systems: availability for invoicing systems in order to ensure cash flow, integrity for backups, and confidentiality for customer databases [P6].

> *"The greatest challenge is that they don't understand how IT intensive their new world will be."*
>
> *— IT manager in a large DSO*

Key finding 7: Post-incident evaluations are not performed.

Learning improves the ability to anticipate future trends and events by producing relevant understandings of what can happen in the future [P4]. 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 [P3]. Learning from incidents should include systematic analysis, use of lessons learnt to make changes, and storing and sharing information [P4].

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 [P7]. Several DSOs said that they perform evaluations after other types of incidents and believed they would do this after information security incidents as well [P7]. 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 [P5], as Hollnagel stated as being just as important as learning from failures [34].

> *"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 kind of reporting of exceptions and mishaps [P7]. However, none reported to have a systematic approach to information security metrics [P5, P7]. 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 needs for improvements [P9]. An understanding of why the existing lacks have emerged, was however not aimed for [P9]. Study 3 showed 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 would usually do in internal evaluations, according to the internal facilitators [P9]. In the third DSO we ran out of time for a thorough evaluation, which was therefore replaced by a short around-the-table discussion. The internal facilitators carried out a short written survey as well, asking the participants about their opinions after the exercise. The questions did not concern improvements to practices or documentation, only the exercise itself. The results from the evaluation could have been richer and more useful if more time was used for a thorough evaluation, as we experienced in the two other DSOs.

Key finding 8: Business managers have different perspectives and priorities than technical personnel.

Information security involves more than IT personnel, as an incident might have severe consequences for both the organization, its customers, and society at large. In an emergency situation, the goal from a business perspective is usually to maintain normal operations as continuously as possible. However, there are different strategies that may be used for this: to resolve the incident with as little disturbances to the operations as possible, to understand why the incident occurred, or to make sure that the incident will not reoccur. 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 [P9].

One of the large DSOs we observed included their Emergency Management Team in the exercise [P9], 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.

Different perspectives and priorities emphasize the need for collaborative exercises that include all personnel that will be involved in a real incident: IT, IT security, control room, networks/infrastructure, business representatives, suppliers. A holistic view needs to be ensured in order to resemble a real emergency situation [P9]. Members of management groups tend to have little time for exercises. Therefore, exercises should be performed frequently, so that all personnel receive regular training. The time spent on each exercise could be limited to make it easier for key personnel to make time for it in a busy schedule [P9]. Such a time limitation makes the exercise more realistic as well, as real incident response processes require quick decisions to be made [P9].

5. Discussion

Key findings were presented in the previous chapter and are now discussed in light of the research questions. Then, implications for both research and practice are stated before limitations are described.

5.1 RQ 1: Which factors affect information security incident management practices?

Incident management practices are affected by the level of risk perception, organizational structure, and the amount of available financial and human resources. Figure 6 shows how the findings presented in the previous chapter relate to these factors. Detection mechanisms currently in use are not sufficient in light of current threats. Organizations are therefore not able to monitor malicious activities in all their systems, and they lack resources to following-up on logs and alerts. As long as no major incidents are experienced, the perceived risk will most likely not increase significantly, and following, detection mechanisms might not be improved. The risk perception is further affected by the size of the organization and whether IT operations are outsourced. Outsourcing of IT services limits the efforts put into planning and preparatory activities due to a strong confidence in suppliers. Finally, small organizations have a lower risk perception than large ones. They do not perceive themselves as being attractive targets for attacks, and they are able to maintain continuous operations even without all systems functioning.

5.1.1 Risk perception

The level of perceived risk among DSOs does not capture the full set of actual risks. Thus, a low priority is assigned to information security activities, including preparations for incident management. Risk perception results from psychological, social, and cultural factors [60], and individuals therefore perceive risk differently based on their personal characteristics, experiences, and knowledge. Both technical/formal risk assessments and personal risk assessments, combined with perceptual factors such as fear will influence an individual's risk perception [61]. As individual risk perceptions affect risk behavior, they might also influence the risk perception in an organization [62].

The consequences of a power outage attack should be considered beyond the effects for one single DSO. 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, 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 in itself, but it might serve customers that are attractive targets for attacks, an issue previously not considered by the small DSOs in our study. Besides, one small DSO might not be attractive alone, but striking several small DSOs at the

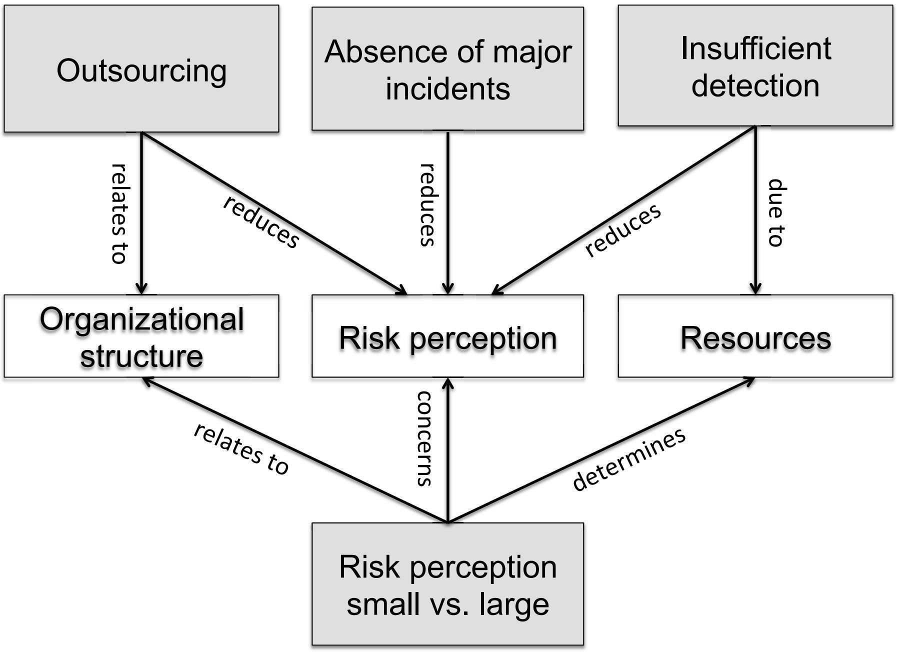


Figure 6: Key findings for RQ 1 relate to the following factors: organizational structure, risk perception, and resources.

same time might be easier than attacking one large DSO, particularly as a number of small DSOs have outsourced to a few suppliers, hence relying on common technologies with common vulnerabilities. Attackers who would want to harm the country as a whole, might consider striking several small DSOs, possibly by attacking their supplier, as a strategy.

An attack might have other consequences than power outages. Industrial espionage is a possible motivation for attacks against the power industry, with the goal of 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 [63]. 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.

There is a large difference between unavailable control systems and minor, undetected errors in the information provided by the control systems. The degree to which a DSO claims to be dependent on the control systems was apparently determined by the DSO's ability to maintain continuous power supply to their customers without the control systems. Availability was the only concern when we asked about their dependency on ICT. 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 and human injuries 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.

> *"Only amateurs attack machines; professionals target people."*
>
> — *Bruce Schneier*[4]

One explanation for a low risk perception is the low number of incidents detected. Limited resources to following-up on logs and alerts further add up to the impression that everything is going well. The probability of a major incident striking tomorrow is however completely independent from past history of incidents. Besides, the fact that a low number of incidents are detected does not mean that attacks are not happening. There might be malicious activity inside the networks that is not being detected due to insufficient detection mechanisms. DSOs should learn from incidents experienced by electric power organizations in other countries and expect similar incidents to strike themselves at any time.

We found that outsourcing reduces an organization's risk perception, as they have a high confidence in their supplier. The existence of plans or having a response team in place seems to have a significant effect on the feeling of preparedness according to Witchalls and Chambers [64]. Whether plans for incident response exist or not at the supplier's side has not been investigated. It is thus the DSO's confidence that determines their risk perception rather than the actual existence of plans.

5.1.2 Organizational structure

Outsourcing of IT services reduces internal efforts in preparatory activities. Further, small organizations put less efforts into such activities than large ones, while at the same time a small organization is more transparent than a large one, which can be advantageous during an emergency situation.

Information sharing is easier in small organizations than in large ones. In small organizations, key personnel have co-located offices, which simplifies communication and collaboration. During a crisis it is important to have an overview, understand relations between pieces of information, and make the right decisions, which is easier in small organizations as personnel, particularly

[4] http://www.schneier.com

administrative personnel, tend to have more than one role. In one of the small DSOs in our study, one person had the following three roles: IT manager, IT security manager, and financial manager. This leads to a handful of employees having insight into several areas and a more complete overview than employees in larger organizations. Sharing, rather than finding, information was stated as challenging by Ahmad et al. [21], but our findings indicate that this is more prominent in large organizations than in small ones. Large organizations are more likely to suffer from organizational dividing lines, a lack of dynamic collaborations across these lines, and unclear responsibilities in some areas, which supports Hollnagel's claim that large high-complexity organizations with centralized management structures have challenges with anticipating threats and foreseeing consequences [2].

Despite the advantages of individuals having more than one role, some limitations follow as well. There might not be enough time for one person in a small organization to fulfill all his assigned roles satisfactorily. Some tasks may hence be given low priorities due to other, more pressing tasks. As small organizations perceive information security risks as being moderately low, tasks regarding information security are given low priority, such as documenting incident management procedures, performing preparedness exercises, stating requirements to suppliers on procedures and training, and regular follow-up meetings with suppliers.

We found that outsourcing of IT services makes both small and large organizations put limited efforts into incident management activities. They are confident in their suppliers being well prepared and capable of responding appropriately to information security incidents. Outsourcing of services seems to result in outsourcing of responsibilities as well. One small DSO justified their confidence in their supplier by the fact that their supplier served several similar organizations. Even though outsourcing relieves an organization of several practical tasks, the organization still needs to be knowledgable about threats to be able to formulate appropriate requirements to their supplier. A small organization is however just one out of several customers for the IT supplier, and they therefore feel that they are not in the position of making demands.

As we have not investigated practices among the suppliers, we cannot state that the suppliers do not have plans and procedures in place and that they do not perform exercises. What we found, was however that DSOs were not concerned about this matter and in many cases had not even asked the suppliers to see existing documentation. It was just assumed to be in place, or DSOs had not thought of asking for it. Such an ignorance is a way of *not* taking the responsibility for own business operations. As long as no customers state clear requirements related to incident management procedures and exercises, the supplier will most likely not improve in this area. One explanation is that suppliers are constantly driven by revenue and will not provide services that will not pay off. It is thus important to remember that outsourcing does *not* relieve the customer of their responsibilities.

5.1.3 Resources

The amount of resources available affects the efforts put into preparatory activities for incident management and the abilities of following-up on logs and alerts from detection systems. Outsourcing of services is used as a means to ensure necessary competence, but as discussed in the previous section, the outsourcing organization is still responsible for stating appropriate and sufficient requirements.

Documenting the profit of information security investments is a challenge, as a success criteria of investments is the *absence* of incidents. Well functioning security mechanisms will then be visible in the budgets as an expense, and the absence of incidents will not be visible [65]. It is far more evident when security mechanisms fail or are insufficient, so that incidents have impact. Even then, documenting the cost of an incident is difficult. Besides, the current low risk perception limits investments in detection mechanisms and other information security measures.

Small organizations are regulated by the same directives as the large ones, but they do not the same amount of financial resources and personnel. According to one of the small DSOs in our study, collaborations with other small DSOs are valuable. Small organizations would greatly benefit from Communities of Practice (CoP) [66], which are informal groups of shared expertise where knowledge and experience can be exchanged. Such a CoP is not established by management; the members are self-selected and the group sets their own agenda and establishes their own leadership. Management can only encourage the establishment of CoPs and provide supporting infrastructure. A CoP for information security incident response would be a means of sharing knowledge and experiences across a number of organizations and thus compensate for the lack of extensive capabilities in-house.

5.2 RQ 2: What are the challenges for improvement of practices?

Different types of personnel, such as business managers and technical personnel, have different perspectives and priorities when it comes to information security. Besides, there is a gap between how IT staff and control system staff understand information security. To create good incident response teams there is a need for cooperation of individuals drawn from various functional areas, i.e. the team needs to be cross-functional [67]. At the same time, divergent interests and points of view are inevitable when individuals from multiple functional areas work together in a team due to their differing orientations towards goals, interpersonal relations, and key external constituents [67]. Furthermore, an incident response team needs to be self-managing. In a self-managing team

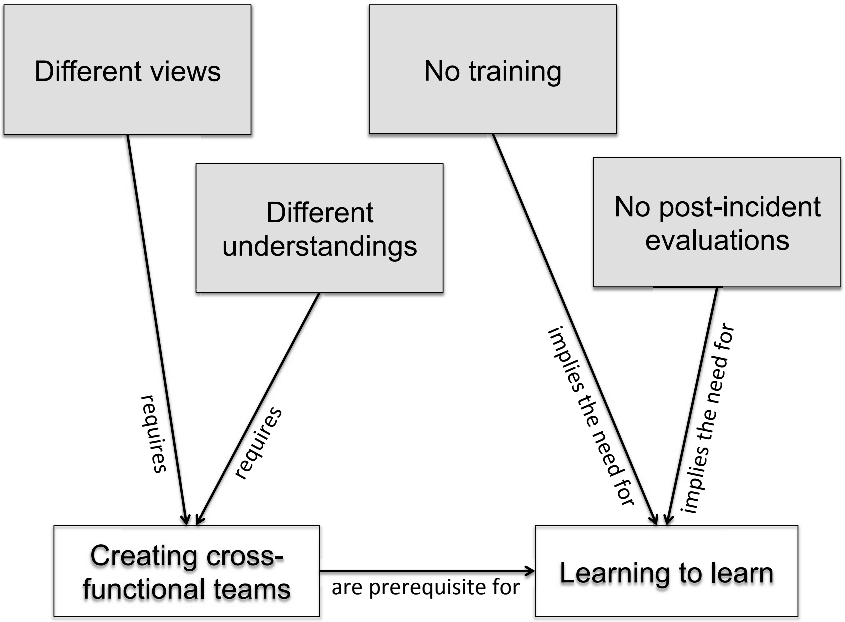


Figure 7: Key findings for RQ 2 sum up to the need for creating cross-functional teams and learning to learn, which are challenges for improving incident management practices.

members have the responsibility not only to execute the task, but also to monitor, manage, and improve their own performance [46]. They need to learn how to improve their activities. However, training for responding to information security incidents is currently given low priority and evaluations after training sessions and minor incidents are not performed. *Learning to learn* would make organizations able to take advantage of training sessions and evaluations and thereby improve their incident response practices. Figure 7 shows how the findings for RQ 2 relate to the need for creating cross-functional teams and learning to learn. These are challenges for improving information security incident management practices, as discussed in the following.

5.2.1 Creating cross-functional teams

Incident response is a highly collaborative activity [24] 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, in order 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 teams need superordinate goals. Superordinate goals will have a positive and significant direct effect on cross-functional cooperation [67]. 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. [34].

The difference in understanding of information security goals that we found between IT staff and control staff is in agreement with Jaatun et al. [26], 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 staff, as they found. Rather than feeling mistrust, both IT staff and control 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 [39].

If a DSO is not able to establish a cross-functional team, the group will be training for solving 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 crisis, effectively [44]. Exercises provide a means for growing shared understanding of the team knowledge.

One challenge of 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. Frequent training is important because these teams exist only when an incident occurs.

5.2.2 Learning to learn

Learning from previous incidents, as well as preparedness exercises, is important for improving own practices for responding to incidents. Scholl and Mangold [22] 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 was described by Cooke [68] as “the collection of organizational capabilities that enable the organization to extract useful information from incidents of all kinds 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

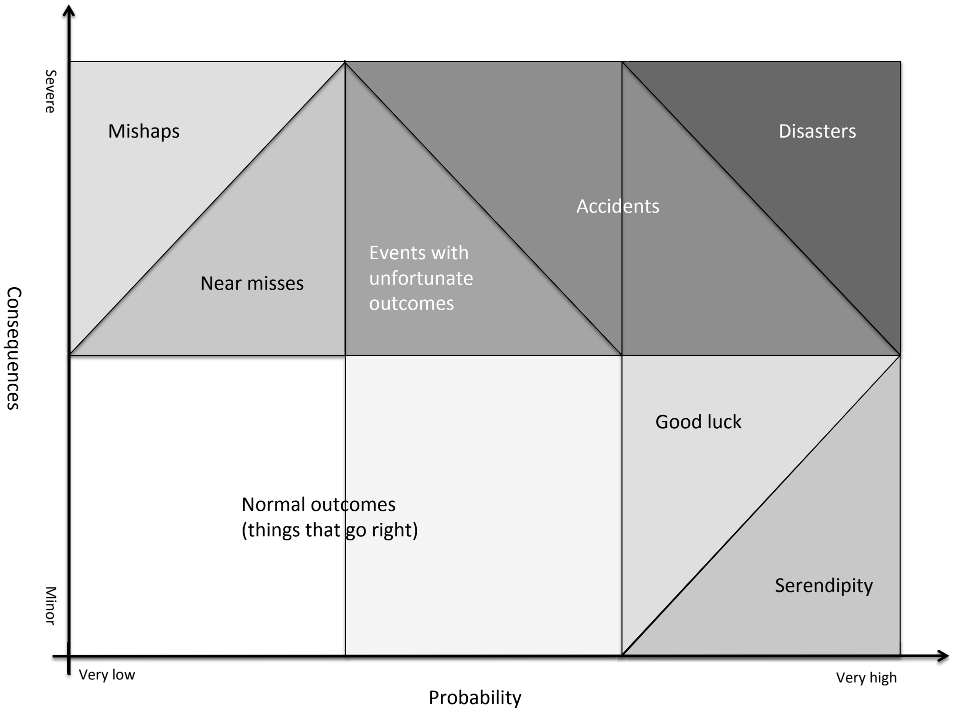


Figure 8: Risk matrix (slightly revised from Hollnagel [2]).

learning, they need to have a realistic perception of actual threats and possible consequences. In our research we found that training for incident response 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. [69], who 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.

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 [21]. 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, c.f. Figure 8. There is a large number of incidents that do *not* have unfortunate outcomes, but still could be used as learning material [2, 22, 70]. 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.

In general, there are two main obstacles to organizational learning: embarrassing and threatening issues [71]. 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 [72] describes as giving the impression of being better than one actually is. These characteristics create individual and organizational behavior that is counterproductive when it comes to learning from unwanted incidents.

Study 3 confirmed the importance of training, as it showed how training enabled participants to link events occurring some time apart and to improve the information flow related to IT and IT security operations between different parts of the organization. There are several strategies for performing and learning from preparedness exercises.

> *"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 [73]*

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 [74]. The organization needs to learn how to carry out single- and double-loop learning [75]. Single-loop learning is to change practice as problems arise in order to avoid the same problem in the future, i.e. learning how to handle one specific incident. Double-loop learning is about using the problems being experienced to understand their underlying causes and then to take some action to remedy these causes. One example is to understand whatever caused the incident to happen. To learn to single-loop learn implies learning to improve performance at an increasing rate: *Are we doing things right when solving the incident?* To learn to double-loop learn implies learning to carry out 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. [21], 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 [70], and should cover both organizational and technical issues, and 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. The role of the facilitators appears immature compared to the description by Hackman et al. [76], which states that a facilitator can help the members in:

1. Minimizing problems with coordination and motivation, and help them build commitment to the group and its task and goal,
2. Avoiding inappropriate weighting of different individuals' ideas and contributions, and help them learn how to share their experience to build the group's repertoire of skills, and
3. Avoiding failures in implementing their performance plans, and help them develop creative new ways of proceeding with the work.

There are three times during the team's lifetime when such coaching is effective:

1. At the beginning, when the group has just started to work and they are more open to interventions that will help them perform well, which is the stadium where the teams in Study 3 currently are at,
2. After they have gained some experience, as they will be open to interventions that help them reflect on the performance strategies, and
3. At the end, learning from their experience.

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 business confidential information. Our impression is that the interviewees were being honest as several of the interviewees reported weaknesses and lacks 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.

Time and resource constraints put a limitation on the number and selection of interviewees. We have interviewed personnel from middle management. Managers might provide information on how things ideally should be done, not just on how things actually are being done. Technical personnel, who performs a large part of the daily tasks concerning incident management, could have provided a slightly different perspective, 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.

We could have studied one or two organizations in depth and interviewed more employees from each organization, including representatives from suppliers. However, we wanted to investigate current practices in the industry by studying a larger number of organizations of different sizes and characteristics.

Data triangulation. Interviews and documentation were intended to provide two different views on incident management, as the interviewees would describe their practice as they know it, while documentation could show the planned procedures. The documentation received was however sparse on information about incident response. Some definitions and procedures were described, but the interviews constituted the major part of the data material in our study (Study 1: Current practice). Besides, confidentiality issues prevented three DSOs from sharing documentation, and non-disclosure agreements and encrypted electronic transfer were not sufficient instruments for overcoming these issues. As information security researchers we should appreciate such caution regarding sharing of confidential documents, although it poses limitations to the data triangulation. Kotulic et al. [77] pointed out this challenge of obtaining sensitive data as limiting to research on information security management in general and recommended focusing on a few selected companies. This opens for building trust between the company and the researcher, which will ease collection of sensitive data. Besides, the companies in focus can be more involved in discussing and approving the results.

All interviewees in Study 1 and 2 and the facilitators of the exercises in Study 3 were provided with a draft of the reports, and hence given the opportunity to comment on the results. As one researcher did most of the analysis in all three studies, this member checking for reducing researcher bias was important.

External validity. Our studies are restricted to DSOs in the electric power industry in Norway, and both the DSOs and the participating interviewees were thoroughly described in the papers P5-P9. A brief presentation was provided in Chapter 3 as well.

5.4 Implications for practice and research

The results from this case study lead to a number of recommendations for practice and suggest directions from future research. The following recommendations for practice are proposed:

- *Continuous evaluation of risks:* Organizations need to develop and improve their knowledge and understanding of current threats and potential consequences. Internal discussions between personnel from different functional areas is one means in this process, in addition to close communication with suppliers and the use of experience reports and threat reports from external parties. Continuously updated risk assessments form the basis for balancing the efforts put into information security activities with the organization's acceptable level of risk.

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

- *Learning to learn:* 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 rather than single-loop learning has to be aimed for, as it makes the organization 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 a potential of triggering such communities of practice, although both the creation and operation have to carried out by self-selected members. Sharing of knowledge and experience is valuable, particularly for small organizations with limited in-house resources.

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

There is a need for longitudinal studies in individual organizations in order to investigate actual incident management practices in more depth. This project was based on interviews and preparedness exercises in several organizations and gave insight into general practices. Direct observations of how personnel from different functional areas cooperate in practice and how they respond to minor incidents and near misses, would increase the understanding of both factors that affect current practices and challenges for improvement.

Further, there is a need for investigating 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 project, but they are part of the cross-functional teams responding to information security incidents.

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

6. Concluding remarks

The main objective of this project was to *explore information security incident management practices in electric power companies and understand challenges for improvements.* Factors that affect current practices have been identified and discussed, along with challenges for improving practices. Implications of the results for both research and practice have been proposed.

We found that incident management practices in an organization are affected by the level of risk perception, organizational structure, and the amount of available financial and human resources. Currently implemented detection mechanisms are not sufficient in light of current threats, thus organizations are not able to monitor malicious activities in all their systems. Besides, they lack resources for following-up on logs and alerts. As long as no major incidents are experienced, the perceived risk will most likely stay unchanged, and organizations will not see the need for improving their detection mechanisms. The risk perception is further affected by the size of the organization and whether IT operations are outsourced. Outsourcing of IT services limits the efforts put into planning and preparatory activities due to a strong confidence in suppliers. Finally, small organizations have a lower risk perception than large ones due to their feeling of not being attractive targets for attacks and their ability to maintain continuous operations even without all systems functioning.

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

This thesis has demonstrated application of organizational theory to information security incident management. Adaptive management strategies, cross-functional teams and learning to learn have been discussed in particular. More organizational research on information security issues should be carried out in order to increase the understanding and enable improved practices.

Well functioning incident response capabilities are an important part 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.

Bibliography

[1] ISO/IEC, “ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management,” 2011.

[2] E. Hollnagel, “The four cornerstones of resilience engineering,” in *Preparation and Restoration, Resilience Engineering Perspectives*, ser. Ashgate Studies in Resilience Engineering, C. P. Nemeth, E. Hollnagel, and S. Dekker, Eds. Ashgate Publishing, Ltd., 2009, vol. 2, ch. 6.

[3] EU, “20 20 by 2020: Europe’s climate change opportunity,” The European Union, Tech. Rep., 2008.

[4] NVE, “AMS - Smarte strømmålere,” Norwegian Water Resources and Energy Directorate, 2014.

[5] M. B. Line, I. A. Tøndel, and M. G. Jaatun, “Cyber security challenges in Smart Grids,” in *2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, Dec. 2011.

[6] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. v. 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.

[7] D. Albright, P. Brannan, and C. Walrond, “Did Stuxnet take out 1000 centrifuges at the Natanz enrichment plant?” Institute for Science and International Security (ISIS), Tech. Rep., 2010.

[8] D. Albright, P. Brannan, and C. Walrond, “Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report,” Institute for Science and International Security (ISIS), Tech. Rep., 2011.

[9] N. Falliere, L. O. Murchu, and E. Chien, “W32.Stuxnet Dossier,” Symantec, Tech. Rep., February 2011.

[10] N. Perlroth, “Researchers find clues in malware,” 2012. [Online]. Available: http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html

[11] McAfee, “Global Energy Cyberattacks: ”Night Dragon”,” McAfee (R) Foundstone (R) Professional Services and McAfee Labs (TM), 2011.

[12] Symantec, “Dragonfly: Cyberespionage Attacks Against Energy Suppliers,” Symantec Security Response, 2014.

[13] 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.

[14] J. J. Cusick and G. Ma, "Creating an ITIL inspired Incident Management approach: Roots, response, and results," in *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, 2010, pp. 142–148.

[15] NIST, "NIST 7628-3: Guidelines for Smart Grid Cyber Security," 2010.

[16] ISO/IEC, "ISO/IEC 27000:2009 Information security management systems - Overview and vocabulary," 2009.

[17] T. Grance, K. Kent, and B. Kim, "NIST SP 800-61: Computer Security Incident Handling Guide," National Institute of Standards and Technology, 2008.

[18] E. Brewster, R. Griffiths, A. Lawes, and J. Sansbury, *IT Service Management: A Guide for ITIL Foundation Exam Candidates*, 2nd ed. BCS, The Chartered Institute for IT, 2012.

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

[20] 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)*, 2011, pp. 107–121.

[21] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident Response Teams - Challenges in Supporting the Organisational Security Function," *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[22] F. Scholl and M. Mangold, "Proactive Incident Response," *The Information Systems Security Association Journal*, 2011.

[23] R. Werlinger and D. Botta, "Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis," *Workshop on Usable IT Security Management (USM '07)*, Jul 2007.

[24] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Information Management & Computer Security*, 2010.

[25] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, 2011.

[26] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and 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.

[27] M. Fabro, T. Roxey, and M. Assante, "No grid left behind," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 72–76, 2010.

[28] D. Batchelder, J. Blackbird, D. Felstead, P. Henry, J. Jones, and A. Kulkarni, "Microsoft Security Intelligence Report," Microsoft, 2014.

[29] K. Stouffer, J. Falco, and K. Scarfone, "NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, 2011.

[30] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen, "Cyber SA: Situational Awareness for Cyber Defense," in *Cyber Situational Awareness*, ser. Advances in Information Security, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Springer US, 2010, vol. 46, pp. 3–13.

[31] G. P. Tadda, "Measuring performance of Cyber situation awareness systems," in *11th International Conference on Information Fusion*, June 2008, pp. 1–8.

[32] U. Franke and J. Brynielsson, "Cyber situational awareness - a systematic review of the literature," *Computers & Security*, vol. 46, pp. 18 – 31, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814001011

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

[34] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, Eds., *Resilience Engineering in Practice - a Guidebook*. Ashgate Publishing Ltd., 2011.

[35] A. Hale and D. Borys, "Working to rule, or working safely? Part 1: A state of the art review," *Safety Science*, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925753512001312

[36] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good, "NIST SP 800-84: Guide to Test, Training and Exercise Programs for IT Plans and Capabilities," National Institute of Standards and Technology, 2006.

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

[38] S. Gåsland, "Gjør øvelse mester? Om læringsfaktorer i beredskapsøvelser initiert av NVE," University of Oslo, Tech. Rep., 2014.

[39] C. Hove, M. Tårnes, M. B. Line, and K. Bernsmed, "Information security incident management: Identified practice in large organizations," in *8th International Conference on IT Security Incident Management and IT Forensics (IMF)*, May 2014, pp. 27–46.

[40] L. H. Rykkja, *Organisering, samfunnssikkerhet og krisehåndtering*, 2nd ed. Universitetsforlaget, 2014, ch. Kap. 8: Øvelser som kriseforebygging.

[41] T. W. Malone and K. Crowston, "The Interdisciplinary Study of Coordination," *ACM Computing Surveys*, vol. 26, no. 1, pp. 87–119, Mar. 1994. [Online]. Available: http://doi.acm.org/10.1145/174666.174668

[42] G. A. Okhuysen and B. A. Bechky, "Coordination in Organizations: An Integrative Perspective," *The Academy of Management Annals*, vol. 3, no. 1, pp. 463–502, 2009. [Online]. Available: http://dx.doi.org/10.1080/19416520903047533

[43] R. E. Kraut and L. A. Streeter, "Coordination in Software Development," *Communications of the ACM*, vol. 38, no. 3, pp. 69–81, Mar. 1995. [Online]. Available: http://doi.acm.org/10.1145/203330.203345

[44] K. Lewis and B. Herndon, "Transactive Memory Systems: Current Issues and Future Research Directions," *Organization Science*, vol. 22, no. 5, pp. 1254–1265, Sep. 2011. [Online]. Available: http://dx.doi.org/10.1287/orsc.1110.0647

[45] N. Lundberg and H. Tellioğlu, “Understanding Complex Coordination Processes in Health Care,” *Scandinavian Journal of Information Systems*, vol. 11, no. 2, pp. 157–181, Jul. 1999. [Online]. Available: http://dl.acm.org/citation.cfm?id=350717.350748

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

[47] R. Floodeen, J. Haller, and B. Tjaden, “Identifying a Shared Mental Model Among Incident Responders,” in *7th International Conference on IT Security Incident Management and IT Forensics 2013.* Los Alamitos, CA, USA: IEEE Computer Society, 2013, pp. 15–25.

[48] C. Robson, *Real world research*, 3rd ed. John Wiley & Sons Ltd., 2011.

[49] A. Bhattacherjee, *Social Science Research: Principles, Methods, and Practices.* Global Text Project, 2012.

[50] B. J. Oates, *Researching Information Systems and Computing.* Sage Publications Limited, 2005.

[51] R. K. Yin, *Case Study Research - Design and Methods, 4th ed.*, ser. Applied Social Research Methods. SAGE Publications, 2009, vol. 5.

[52] M. D. Myers and M. Newman, “The qualitative interview in IS research: Examining the craft,” *Information and Organization*, vol. 17, no. 1, pp. 2–26, Jan. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.infoandorg.2006.11.001

[53] C. Cassell and G. Symon, *Essential Guide to Gualitative Methods in Organizational Research.* Sage Publications Limited, 2004.

[54] R. Bogdan and S. K. Biklen, *Qualitative research for education: an introduction to theory and methods.* Allyn and Bacon, 1982. [Online]. Available: http://books.google.no/books?id=wIOcAAAAMAAJ

[55] J. Lofland, *Analysing social settings.* Wadsworth Pub, 1971. [Online]. Available: http://books.google.no/books?id=fIOjKQAACAAJ

[56] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis: An Expanded Sourcebook.* SAGE Publications, 1994.

[57] 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, no. 6, pp. 875–894, 2009. [Online]. Available: http://dx.doi.org/10.1007/s11135-008-9164-0

[58] B. Kitchenham and S. Charters, “Guidelines for performing Systematic Literature Reviews in Software Engineering,” EBSE Technical Report, 2007.

[59] NVivo, “NVivo,” http://www.qsrinternational.com/.

[60] O. Renn, *Risk Governance: Coping with Uncertainty in a Complex World.* Routledge, 2008.

[61] T. Aven and O. Renn, *Risk Management and Governance: Concepts, Guidelines and Applications*, ser. Risk, Governance and Society. Springer Berlin Heidelberg, 2010, vol. 16.

[62] T. Rundmo, “Associations between risk perception and safety,” *Safety Science*, vol. 24, no. 3, pp. 197 – 209, 1996. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925753597000386

[63] A. Sood and R. Enbody, “Targeted Cyberattacks: A Superset of Advanced Persistent Threats,” *IEEE Security & Privacy*, vol. 11, no. 1, pp. 54–61, Jan 2013.

[64] C. Witchall and J. Chambers, “Cyber incident response: Are business leaders ready?” The Economist Intelligence Unit (EIU), 2014.

[65] N. P. Repenning and J. D. Sterman, “Nobody ever gets credit for fixing problems that never happened: creating and sustaining process improvement,” *IEEE Engineering Management Review*, vol. 30, pp. 64–64, 2002.

[66] E. C. Wenger and W. M. Snyder, “Communities of Practice: The Organizational Frontier,” *Harvard Business Review*, vol. January-February, 2000.

[67] M. B. Pinto, J. K. Pinto, and J. E. Prescott, “Antecedents and Consequences of Project Team Cross-Functional Cooperation,” *Management Science*, vol. 39, no. 10, pp. 1281–1297, October 1993.

[68] D. L. Cooke, “Learning from Incidents,” in *Proceedings of the 21st International Conference of the System Dynamics Society*, 2003.

[69] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, “Unrealistic optimism on information security management,” *Computers & Security*, vol. 31, no. 2, pp. 221–232, 2012.

[70] U. Kjellén, *Prevention of Accidents Through Experience Feedback*. Taylor and Francis, 2000.

[71] C. Argyris and D. A. Schön, *Organizational learning: A theory of action perspective*. Addison-Wesley, 1978.

[72] G. Morgan, *Images of Organization*. SAGE Publications, 2006.

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

[74] C. Argyris, *Increasing Leadership Effectiveness*. John Wiley, 1976.

[75] C. Argyris and D. A. Schön, *Organizational Learning II: Theory, Method and Practice*. FT Press, 1996.

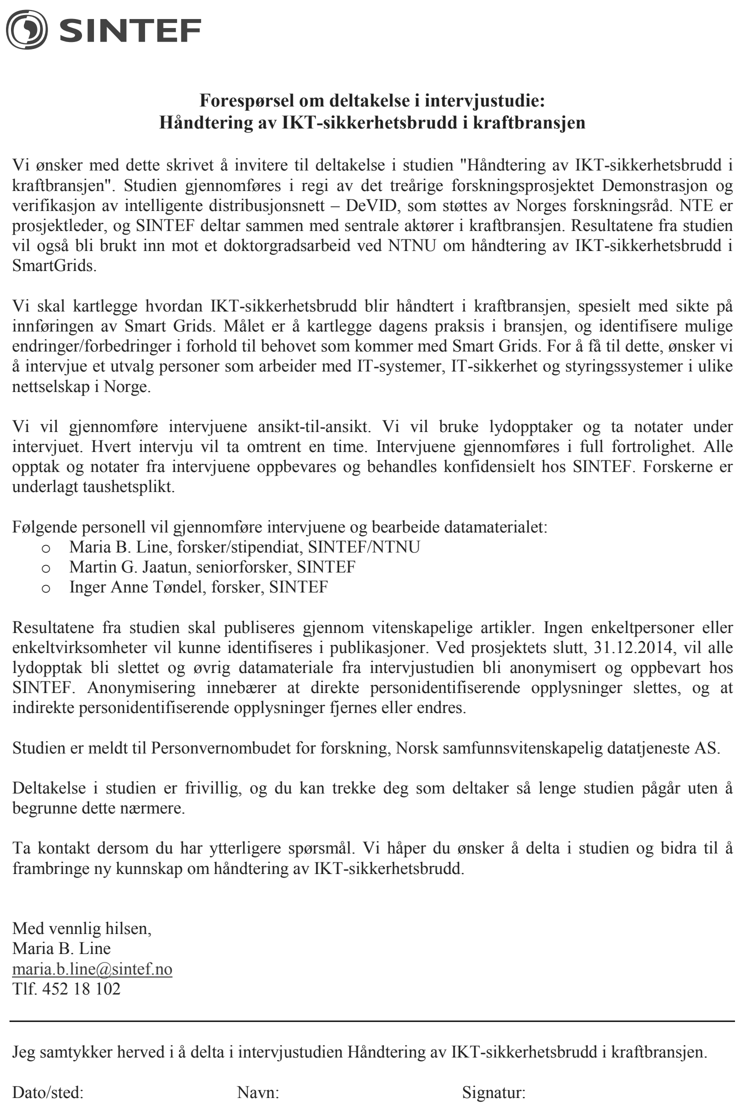
[76] J. R. Hackman, R. Wageman, T. M. Ruddy, and C. R. Ray, *Team effectiveness in theory and practice*. Oxford, UK: Blackwell, 2000.

[77] A. G. Kotulic and J. G. Clark, “Why there aren’t more information security research studies,” *Information & Management*, vol. 41, no. 5, pp. 597 – 607, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378720603000995

Part II

APPENDICES

Letter of consent (in Norwegian)



SINTEF

Forespørsel om deltakelse i intervjustudie:
Håndtering av IKT-sikkerhetsbrudd i kraftbransjen

Vi ønsker med dette skrivet å invitere til deltakelse i studien "Håndtering av IKT-sikkerhetsbrudd i kraftbransjen". Studien gjennomføres i regi av det treårige forskningsprosjektet Demonstrasjon og verifikasjon av intelligente distribusjonsnett – DeVID, som støttes av Norges forskningsråd. NTE er prosjektleder, og SINTEF deltar sammen med sentrale aktører i kraftbransjen. Resultatene fra studien vil også bli brukt inn mot et doktorgradsarbeid ved NTNU om håndtering av IKT-sikkerhetsbrudd i SmartGrids.

Vi skal kartlegge hvordan IKT-sikkerhetsbrudd blir håndtert i kraftbransjen, spesielt med sikte på innføringen av Smart Grids. Målet er å kartlegge dagens praksis i bransjen, og identifisere mulige endringer/forbedringer i forhold til behovet som kommer med Smart Grids. For å få til dette, ønsker vi å intervjue et utvalg personer som arbeider med IT-systemer, IT-sikkerhet og styringssystemer i ulike nettselskap i Norge.

Vi vil gjennomføre intervjuene ansikt-til-ansikt. Vi vil bruke lydopptaker og ta notater under intervjuet. Hvert intervju vil ta omtrent en time. Intervjuene gjennomføres i full fortrolighet. Alle opptak og notater fra intervjuene oppbevares og behandles konfidensielt hos SINTEF. Forskerne er underlagt taushetsplikt.

Følgende personell vil gjennomføre intervjuene og bearbeide datamaterialet:

- Maria B. Line, forsker/stipendiat, SINTEF/NTNU
- Martin G. Jaatun, seniorforsker, SINTEF
- Inger Anne Tøndel, forsker, SINTEF

Resultatene fra studien skal publiseres gjennom vitenskapelige artikler. Ingen enkeltpersoner eller enkeltvirksomheter vil kunne identifiseres i publikasjoner. Ved prosjektets slutt, 31.12.2014, vil alle lydopptak bli slettet og øvrig datamateriale fra intervjustudien bli anonymisert og oppbevart hos SINTEF. Anonymisering innebærer at direkte personidentifiserende opplysninger slettes, og at indirekte personidentifiserende opplysninger fjernes eller endres.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Deltakelse i studien er frivillig, og du kan trekke deg som deltaker så lenge studien pågår uten å begrunne dette nærmere.

Ta kontakt dersom du har ytterligere spørsmål. Vi håper du ønsker å delta i studien og bidra til å frambringe ny kunnskap om håndtering av IKT-sikkerhetsbrudd.

Med vennlig hilsen,
Maria B. Line
maria.b.line@sintef.no
Tlf. 452 18 102

Jeg samtykker herved i å delta i intervjustudien Håndtering av IKT-sikkerhetsbrudd i kraftbransjen.

Dato/sted: Navn: Signatur:

Letter of consent (translated from Norwegian)

Request for participation in interview study: Information security incident management in the electric power industry

We hereby invite you for participation in the study "Information security incident management in the electric power industry." The study is conducted as part of the DeVID research project – Demonstration and Verification of Intelligent Distribution Grids – supported by the Norwegian Research Council. NTE is leading the project and SINTEF is participating together with a number of important stakeholders in the electric power industry. The results from the study will also be used in a PhD project at NTNU on information security incident management in smart grids.

We are going to survey how IT security incidents are responded to in the electric power industry, particularly in light of the implementation of smart grids. The goal is to assess current practice and identify required changes/improvements. We therefore want to interview a number of employees working with IT systems, IT security, and industrial control systems in different distribution system operators (DSOs) in Norway.

The interviews will be carried out face-to-face. A voice recorder will be used and we will make notes during the interview. Each interview will last for approximately one hour. All recordings and notes from the interviews will be stored and processed at SINTEF, according to confidentiality requirements. The researchers will respect the professional privacy of the information given.

The following personnel will be conducting the interviews and will analyze the data material:

- Maria B. Line, Research scientist/PhD student, SINTEF/NTNU
- Martin G. Jaatun, Senior research scientist, SINTEF
- Inger Anne Tødel, Research scientist, SINTEF

The results from the study will be published in scientific papers. No individuals or single organizations will be identifiable in the publications. By the end of the project, 31 Dec. 2014, all recordings will be deleted and other data material from the interview study will be anonymized and stored at SINTEF. Anonymization implies that directly-identifiable information is deleted, and indirectly-identifiable information is removed or altered.

The study is registered with the Data Protection Official for Research. Participation in the study is voluntary and you may withdraw as a participant at any time without providing a reason.

Please contact us if you have any questions. We hope that you will want to participate in the study and contribute to a better understanding of information security incident management.

To be signed: I hereby consent to participate in the study Information security incident management in the electric power industry.

Interview guide for Study 1 (translated from Norwegian)

Individual

1 How many employees are there in your organization?
2 Which position and/or role do you have?
3 For how long have you had this position?
4 Which systems and procedures are within your responsibility?
5 Can you describe how your position connects to the work related to security, ICT and automation systems?
6 According to the regulations for emergency preparedness, three roles are mandatory for a DSO: Emergency preparedness manager, Emergency preparedness coordinator, and IT security coordinator. How are these roles assigned in your organization?

ICT security incidents

7 To which degree does the organization depend on ICT?

- How much downtime can be endured for your systems?

8 How would you define an ICT security incident?
9 Can you describe your latest ICT security incident?

- How was this incident responded to?
- How well did the response work?
- Why did the response work as it did?

10 What is the worst ICT security incident your organization could experience?
11 If you think about how the latest ICT security incident was responded to, would this be sufficient to handle the worst possible ICT security incident?

- Would you have done the same if it was a targeted hacker attack?

12 How frequently do you experience ICT security incidents?

- If you have never experienced ICT security incidents, what could be the reasons for that?

13 What kind of ICT security incidents do you experience?

- What kind of consequences are typical for this kind of incidents?

Responding to ICT security incidents

14 Which plans exist for ICT security incident management?
15 Are the plans used in practice?

- If not, why not?

16 Do you perform training on incident management?

- If yes, how? (Scenarios, exercises, courses?)
- Who take part in these training activities?
- If not, why not?

17 Can you tell me about general emergency preparedness exercises that you perform? (Who, how often, what kind of scenarios?)

- How is ICT included in these exercises?

18 How are ICT security incidents usually detected? (Automatic tools? Intrusion detection systems? Firewalls? Users? Manual audit of logs?)

19 How are ICT security incidents initially reported?

20 Who is involved in responding to ICT security incidents?

21 Do you experience challenges related to cooperation on responding to incidents?

- If yes, what kind of experiences? (Are they related to communication? Terminology? Responsibilities? Knowledge and experience? Procedures?

22 What kind of supplementary work is performed when regular operation is restored?

23 How are ICT security incidents registered and reported afterwards?

24 Is information on incidents reported to top management?

25 Is information on incidents disseminated to end-users, internally or externally?

26 Do you report ICT security incidents to the police?

27 Are the experiences from ICT security incidents used as input to further risk assessments and improvements of procedures afterwards? (Or is incident response mainly ”‘firefighting”’?

- If yes, which parts of the organization are involved in this process?

28 Do you have any numbers for the costs of ICT security incidents?

- If yes: How frequently and how are these followed-up? Who is responsible?

29 Did you establish any other indicators or measurements for ICT security incidents? (E.g., downtime due to incidents, number of incidents per month)

- If yes: How frequently and how are these followed up? Who is responsible?

Possible improvements and cooperation

30 Do you have any practices that work well, that you would like to recommend to others?

31 What are the most challenging parts of ICT security management?

32 Do you see any possible improvements to how you respond to ICT security incidents?

- If yes, which?

33 The fact that you are a small DSO, how would this affect the area of ICT security incidents?

34 Did you establish any cooperation with other DSOs - small or large?

35 Do you participate in any cross-organizational cooperation in the industry regarding information security? (Work groups, seminars, regular meetings?)

- If yes, to which degree is ICT security incident management on the agenda?

36 The Smart Grid leads to a closer integration of ICT and automation systems in the future. How do you think this will affect ICT security incident management?

Interview guide for Study 2 (translated from Norwegian)

Cyber situation awareness:
Targeted attacks towards industrial control systems

An information security incident is commonly defined as something that compromises confidentiality, integrity, and/or availability of information. In this interview we are focusing on targeted attacks rather than technical failures. Furthermore, only the industrial control systems in the DSO are in question. The administrative IT systems are outside the scope of this study.

General

1 What is your role in the organization?
2 How many operators work in the control room?
3 How many power subscribers do you serve?
4 Can you estimate the number of computers and running applications?
5 Did you ever observe an attack to your control systems? Or malware?

  (a) Would you consider any of them as targeted?
  (b) Are you aware of any successful attack in your control systems?
  (c) How were these detected?
  (d) Were you able to identify the attacker(s)?

6 Do you think that anyone could be interested in attacking your systems? Who could this be?
7 Do you have any customers that could be potential victims for targeted attacks?

  (a) Could such an attack also hit your organization?

8 What is the worst possible consequence of a targeted attack?

Policies

9 Have you performed any criticality assessment of resources (computers, applications, information items, other) in the control systems?

  (a) Do you know about dependencies between certain resources?
  (b) Do any resources become more critical at specific points in time, or do they always keep the same level of importance?
  (c) Do you feel that the level of protection for the most critical resources is appropriate?
  (d) How is the IT defense different for the critical resources vs. non-critical ones?

10 Do you perform regular cyber security assessment?
11 How do you deal with the reported vulnerabilities; what kind of patching regime do you have?

12 Do you have any documentation of the technical security mechanisms on the control systems?

13 How are the control systems connected to the administrative network in your organization (i.e., one-way flow of data, VPN, no connection at all)?

14 How do you deal with employees and/or external consultants bringing their own computer, or other devices like USB memory sticks and similar, into the control room?

Preparedness

15 Do you have response procedures for cyber attacks?

   (a) How are they different from other failure response procedures? (Graceful degradation, restoring backups, limiting access, removing malware?)

16 Are control room operators made aware of the threats that they can encounter in their day-to-day job?

17 Have you ever performed exercises based on a scenario of targeted attacks towards the control systems?

   (a) Why/why not?
   (b) If any, were they table-top exercises or more realistic action-based exercises?
   (c) Do you have regular simulated attack practices?
   (d) Do you practice the worst-case scenarios?

18 What would be a beneficial way of training for responding to targeted attacks towards your control systems?

Technical security mechanisms

19 Do you encrypt critical data items while in transfer and stored?

20 Do you have off-site backups?

21 Do you only have network-edge defenses (e.g., IPSes), or do you also have detection mechanisms that can detect malicious activity inside the network?

   (a) Are such defenses host-based (antiviruses) or do they look at network traffic too?

22 Which specific defenses do you have? For each mechanism, use the following keywords to guide the conversation:

   (a) What is the purpose of this mechanism?
      i Does it detect attacks?
      ii Does it prevent attacks?
      iii Does it react to attacks?
      iv Does it predict attacks?
      v Does it give more information about an attack that has already happened?

(b) Input

  i Which type(s) of input is needed (e.g., network, OS, service, or organization level logs)?

  ii Where does the input come from (e.g., is it automatically deduced by the device, entered manually, or the output of another device)? Is input needed initially or continuously? How often is it entered? How many man-hours per week are required? How sophisticated is the input? Does it need to be configured, or is it a black-box system?

  iii How high-level is the input? Is it human readable or raw?

(c) Output

  i Which type(s) of output is generated (i.e., attack alerts, network/OS/service/organization level logs)?

  ii Where does the output go (i.e., to a human analyst or to another system)?

  iii How high-level is the output? Is it human readable or raw? What is the size of the output?

  iv Is the output actionable? Is it connected to an automated system? Does the action need human intervention?

(d) Integration with the workflow and organization missions

  i Is the system constantly running, do you run it when something happens, or is it run periodically?

  ii Does the system need a human analyzer to be run, or do you run it and leave it be? If the system needs human configuration/input/intervention/analysis, how often does it happen? Is there a position/duty in the organization associated with it?

  iii Is the tool/technique applied to the organization‘s most critical resources or to the whole organization? Are the most critical assets more protected, or monitored more often? How is the application of the tool different for a not-so-important resource and a mission-critical resource?

(e) Internal model

  i Is the model static or dynamic? Does it learn and change through time? Does it need initial/ongoing configuration? Does it learn (supervised/unsupervised; i.e., does it need human intervention for learning or does it learn on its own?)?

  ii Does it learn the systems normal behavior? Does it learn the attacker's goals? Does it predict the next steps of the attacker?

(f) Efficiency

  i Does it work satisfactorily, or do you see any needs for improvements?

ii What is the amount of information that a security administrator (or all of them) should look at manually and daily? (Either in bytes, or lines, or pages)

iii What is the amount of information generated daily by the security logging tools?

iv What is the number of attacks reported daily/monthly/annually (either false positive or true positive)?

v How many of them, after manual inspection, turn out to be true?

The Cyber Security Awareness Mapping

The questionnaire was purposely designed to cover in-place defenses and policies, incident response capabilities, and cyber situation awareness. Table 4 shows the relation between these areas and the questions. Each row represents one of the capabilities under-study and the numbers in each row are the number of the questions that are trying to evaluate the associated capability.

- General: general information about the organization
- CSA-Comprehension: comprehension of the current situation
- CSA-Impact: impact assessment
- CSA-Evolution: understanding how attacks evolve
- CSA-Behavior: attacker behavior analysis
- CSA-Causes: attack causal analysis
- CSA-Confidence: confidence in the acquired information
- CSA-prediction: prediction of future attacks or future steps of an attacker
- Defenses: the technology-based cyber defenses in place
- Policies: the policy-based cyber defenses in place
- Response: the incident response capability.

Table 4: Mapping between CSA capabilities and the questions in the interview guide.

Category							
General	1	2	3	12			
CSA-Comprehension	4	5	21	22			
CSA-Impact	8	9	10	22			
CSA-Evolution	22						
CSA-Behavior	6	7	16	22			
CSA-Causes	22						
CSA-Confidence	22						
CSA-Prediction	22						
Defenses	5	9	13	14	19	21	
Policies	9	10	11	14	17	19	20
Response	11	15	16	17	18		

Part III

PAPERS

PAPER 1

Cyber Security Challenges in Smart Grids

Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun

IEEE PES Innovative Smart Grid Technologies 2011, Manchester, UK.
ISSN 2165-4816. DOI: 10.1109/ISGTEurope.2011.6162695

©2011 IEEE. Reprinted with permission.

Is not included due to copyright

PAPER 2

Why securing smart grids is not just a straightforward consultancy exercise

Maria B. Line

Security and Communication Networks, vol.7, no.1, p.160-174, January 2014.
ISSN 193-0114. DOI: 10.1002/sec.703

Reprinted with permission from John Wiley and Sons.

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2013)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.703

SPECIAL ISSUE PAPER

Why securing smart grids is not just a straightforward consultancy exercise

Maria B. Line*

Department of Telematics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway

ABSTRACT

The long-term vision for modernization of power management and control systems, *smart grid*, is rather complex. It comprises several scientific traditions: supervisory control and data acquisition systems, automation systems, information and communication technology, safety, and security. Integrating information and communication technology systems and power management and control systems causes a need for a major change regarding system design and operation, in which security controls are required and implemented, and how incidents are responded to and learned from. This paper presents concerns that need to be addressed in order for the implementation of smart grids to succeed from an information security point of view: a unified terminology, a fusion of cultures, improved methods for assessing risks in complex and interdependent systems, preserving end users' privacy, securing communications and devices, and being well prepared for managing unwanted incidents in a complex operating environment. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS
information security; smart grids; advanced metering infrastructure; information and communication technologies; privacy

***Correspondence**
Maria B. Line, Department of Telematics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway.
E-mail: maria.b.line@item.ntnu.no

1. INTRODUCTION

Smart grids will result in increased instrumentation for monitoring and control in the low voltage distribution grid, distributed generation (micro wind turbines, solar panels, etc.), energy storage, and electric vehicles. The parts of the grid that include generation and high-voltage transmission of power are already modernized and do not need such large-scale investment in order to meet future demands. The distribution grid is the part of the power grid that transmits power from substations to end users such as companies and private households. Figure 1 shows the power grid value chain from the generation, via the transmission and distribution grids, to the end users [1].

The deployment of advanced metering infrastructures (AMIs) is the first big leap in the direction of the smart grid vision. This allows for automatic reading and gathering of customers' power consumption. The distribution system operators (DSOs) may use this data for both billing and grid management purposes. The customers can be charged more correctly than before; as the prices vary each hour throughout the day, the customers may be rewarded for using less power during the most costly hours. They may receive tariff information through the smart meter as a means to control their own power consumption. This pricing mechanism may contribute to reducing the consumption peaks that are expensive to both the customers and the DSOs. The DSOs will receive close-to-real-time information on power demand and consumption that they can use for managing production and response.

In addition to smart meters, the households may also be equipped with consumer appliances with web interfaces and remote control. The introduction of AMI will contribute to improving the utilization of the power grid, reducing restoration times, and giving users more control over their consumption and bill.

Several countries have started to roll out AMI. In Italy, the large DSO Enel SpA has rolled out AMI to more than 30 million customers, which makes this the largest AMI deployment so far. Canada, the UK, and the Netherlands are other countries that have started, and also, in Norway, there are demonstration and research activities in this area, especially through Demo Steinkjer (Nord-Trøndelag E-verk; www.demosteinkjer.no) and Smart Energy Hvaler (Fredrikstad Energi AS; www.smartenergihvaler.no).

With the AMI comes two-way communication between the DSOs' back-end systems and the customers' smart meters. This implies a tighter coupling between power automation systems and general information and communication technology (ICT) systems.

Copyright © 2013 John Wiley & Sons, Ltd.

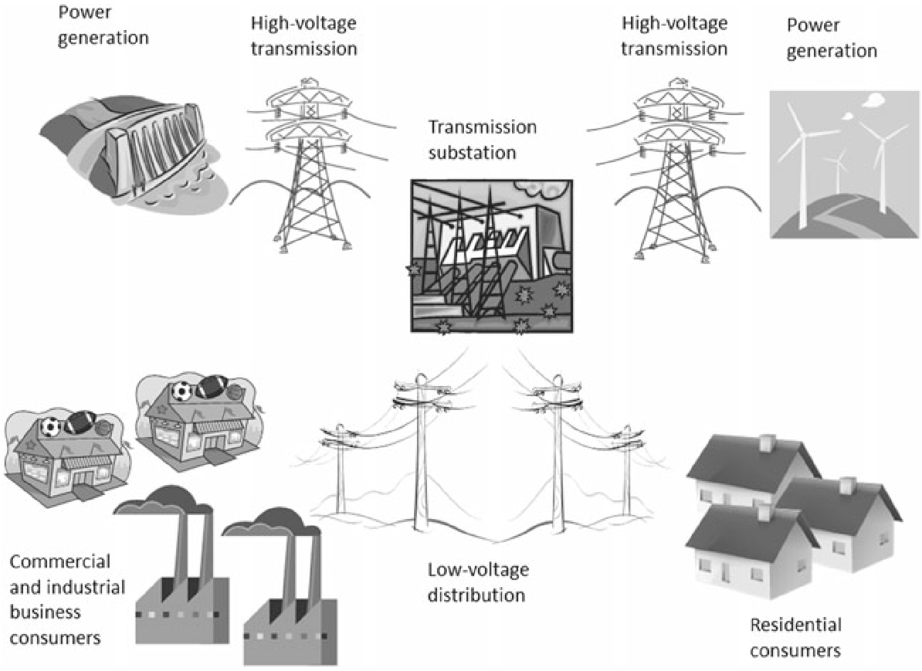


Figure 1. The power grid value chain.

Power automation systems have traditionally been based on proprietary technologies operating in closed networks. They have been designed to fulfill quite specific purposes and, by many, have not even been recognized as ICT, even though they are indeed a combination of hardware, firmware, and software. The information security objectives have been limited as connectivity and availability have been the most prioritized properties; confidentiality and integrity have not received the same attention. The attack surface has been quite limited as well, mainly because the systems have operated without network connections and they have not been connected to the Internet. Incidents usually occur as a result of hardware failures, and lack of monitoring may make it difficult to identify the exact location of the failure.

Information and communication technology systems, on the other hand, consist of commercial-off-the-shelf technologies operating on TCP/IP networks, and they are usually designed to fulfill multiple purposes. Such technologies are widely used, they frequently have quite open and accessible interfaces, and attackers find it attractive to exploit known and unknown vulnerabilities and cause minor or major damage. Incidents usually occur as a result of software failures, directly or indirectly, and complexity makes it difficult to avoid and detect such failures.

The vision of smart grids imposes the meeting of the two cultures of power automation and ICT.

This paper discusses information security challenges ahead and investigates how well current research addresses these challenges. Technical aspects as well as human and organizational aspects are covered, as the success of smart grids depends not only on technological innovations but just as much on changes in work processes, competence, and understanding. Future research and development needs are also pointed out.

The multitude of concepts and terminologies in this discipline is discussed in the following section, before reflections on culture and traditions within both power automation and ICT are provided in Section 3. Special considerations required during risk assessments for smart grids are presented in Section 4, and privacy issues arising with the AMI roll-out are described in Section 5. Existing recommendations for smart grid security architectures are provided in Section 6. Section 7 discusses information security incident management from a smart grid point of view, and examples of real-life information security incidents are provided. Section 9 looks beyond the limitations that information security usually poses and shows expected positive effects of smart grids, before further work is described and concluding remarks are given in Section 9.

2. CONCEPTS AND TERMINOLOGY

As the power industry is heading towards smart grids, more branches of science and engineering must be involved. There will be a need for new expertise, products, and solutions within fields such as communication infrastructures, hardware and software products and services, and information security solutions. Hence, there is a broad spectrum of professionals addressing the topic of power automation systems. However, their approaches differ as they represent different traditions with different world views, cultures, terminology, work processes, and methods. To ensure a common understanding and efficient integration processes, a common terminology has to be established.

Thereafter, there needs to be a common understanding of the business processes and priorities in the power industry. Professionals being new to this industry must be open-minded and willing to learn about its traditions and, at the same time, bring in their own knowledge and experience, to enrich the industry. An efficient cooperation can then take place when this succeeds, when the main priorities are agreed upon and all professionals manage to contribute with their own specialties.

2.1. The system—which system?

There will be a tighter coupling between the power automation systems and ICT systems. But what does this really mean? Which systems are covered by the term *power automation systems*? And is this term the most appropriate and correct term to use? There are several terms denoting this kind of system; *power automation system* is one; others are *process control systems*, *control systems*, *supervisory control and data acquisition (SCADA)* systems, *distribution management system*, *energy management system (EMS)*, and *production systems*. Professionals working in this domain, performing monitoring and management of these systems in a control room, know what is meant by each of these terms and are able to explain the differences. However, ICT professionals who are now entering the power industry are usually not familiar with such systems, especially not to the level of detail needed in order to be able to "speak the language," which is an essential prerequisite for an efficient collaboration.

Ericsson [2] mainly uses the term *power control systems*, but he also mentions *SCADA/EMS* and *power system communication systems*. The latter refers to the fact that power control systems have been more integrated lately; SCADA systems and substations are now interconnected with other systems, and both a dedicated line and the Internet are used for communication. He does not distinguish between SCADA and EMS, but denotes them together, *SCADA/EMS*, without explaining what kinds of systems each of them refers to.

Wei *et al*. [3] use several terms, such as *power grid automation systems* and *power grid automation networks*, *automation and control systems*, *SCADA*, and *power automation systems*, but they mainly use the latter. They also include a figure illustrating how the different components and systems are connected. For the purpose of clarification, a similar figure is also presented in this paper (Figure 2). It shows a typical architecture for power automation systems, all systems related to monitoring and operation of the power grid. *SCADA/EMS* denotes the part of the system that is operated from a control room. One control room can manage several substations and also be connected to other control rooms. The upper part of the figure shows the corporate systems, which consist of what is usually denoted as regular ICT systems.

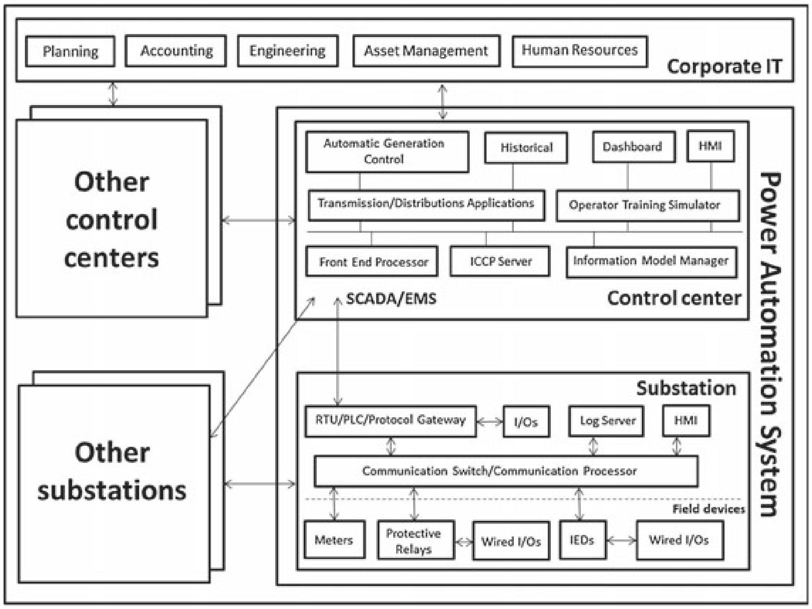


Figure 2. A typical power automation system. SCADA, supervisory control and data acquisition; EMS, energy management system; HMI, Human Machine Interface; IED, Intelligent Electronic Device.

Security Comm. Networks (2013) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

Datta Ray *et al*. [4] speak of *industrial control systems (ICSs)*, *power grid control information systems*, and *power grid operation systems*. They distinguish between *operations technology (OT)* and *information technology (IT)*, and also denote these two systems as *control systems and IT systems*, and *legacy systems and corporate IT systems*. Their message would be clearer if they could stick to one set of terms and, if necessary, mention alternative terms in the beginning. At least, they state early in the paper that they will use the terms OT and ICS interchangeably. Khan *et al*. [5] speak of *SCADA* and *distributed control system*, but do not explain the differences or connections between these two.

For an ICT professional, it may seem like distribution management system, EMS, and SCADA are all parts of the larger power automation systems. However, it is not quite clear how they are connected and/or integrated. *Process control systems* and *production systems* are general terms used in several industries. Hence, they denote similar systems as the term *power automation systems*, but the latter is industry specific. Therefore, throughout this paper, the term *power automation systems* will be used to denote all systems and functionalities operated from the control center and substations related to management of the power grid, in accordance to Figure 2.

The terms *administrative systems* and *corporate systems* are often used as a counterpart to the power automation systems. They include all ICT systems needed to operate the corporate parts of the DSO: project management, contracts, financial information, human resources, and the like. Usually, the terms *ICT* and *IT* are used interchangeably, where both denote systems that are based on TCP/IP/Ethernet technologies. The term *ICT systems* will be used throughout this paper.

2.2. Security comes in many flavors

The term *security* is subject to several different interpretations depending on who are the sender and the receiver of the message. In the field of computer science, *security* usually means *information security*; although it could also denote the more limited concepts of *computer security* or *network security*. The term *cyber security* is used in some contexts, usually related to automation and control systems. This is a term that is not explicitly defined by International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000:2009 [6], which is the standard defining the most relevant terms within information security. However, in the literature, it seems like cyber security is a constructed term that mixes the fields of cybernetics and computer security, and hence, is widely used to denote ICT security in control systems.

Information security comprises the three attributes of confidentiality, integrity, and availability [6]. Also, the properties of non-repudiation, authentication, audit, and privacy are associated attributes, without them being part of the well-established definition. An information security event is defined to be an identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, or to be a previously unknown situation that may be security relevant [6]. Then, an information security incident is defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [6].

A related term to *security* is *dependability*, which usually describes the inability of a system to affect its environment in an undesirable way. The main purpose of dependability mechanisms is to protect life, health, and the environment from damage. It is also regarded as protection against random incidents [7]. Security, on the other hand, can be seen as the inability of the environment to affect the system in an undesirable way [8], or as protection against intended attacks. However, an incident compromising a system's security can lead to the system acting in an unfortunate way, and a security breach can cause a dependability breach. The two properties dependability and security are closely connected and need to be addressed accordingly. Traditionally, the power grid has been more concerned with dependability than security. With the introduction of smart grids, where ICT systems will be a critical component, security issues need to be considered.

The fields of dependability and security have different terminologies. As an example, a dependability breach may be denoted as a *fault* or an *accident*. Security breaches, on the other hand, may exploit what are denoted as *errors* or *bugs*. A *safety hazard* may correspond to a *security threat*. Avizienis *et al*. [9] thoroughly present concepts and taxonomies of dependability, which they see as a property that includes safety reliability, availability, integrity, and maintainability. They compare these to the field of security, which they see as quite related, but still different from, dependability, as it includes confidentiality, availability, and integrity, as also defined by ISO/IEC 27000 [6]. There are substantial differences when it comes to methods and methodologies between the two fields of dependability and security. Please refer to Line *et al*. [8] for an overview of common methods within each of the fields, including an analysis of similarities and differences.

Power security, on the other hand, is a quite different concept from information security. It usually refers to the ability of providing energy to customers. There is a certain parallel to the property of availability for ICT systems, but these two should still not be mixed up. It is therefore important to specify what kind of security one refers to. In this paper, information security is the main concern, and it will be denoted as information security, not just security, to make sure that confusions are avoided.

2.3. Current standards and guidelines

Several standards and guidelines exist that deal with different aspects of information security. Governmental organizations, academic institutions, industry, and interest groups are among the publishers. Two of the most recognized publishers are ISO (www.iso.org), cooperating with the IEC (www.iec.ch), and the National Institute of Standards and Technology (NIST; www.nist.gov) at the U.S. Department of Commerce.

The ISO/IEC has published a set of standards and documents on information security matters in their 27000 series. Topics include information security management system, risk management, measurement and metrics, incident management, and network security. Cyber security and application security are two of the topics that are planned for the near future. It is natural to assume that the area of smart grids should be well suited for such joint standards.

Among the broad collection of documents from NIST, it is worth mentioning their Computer Security Incident Handling Guide [10], Guide to Industrial Control Systems Security [11], and Guidelines for Smart Grid Cyber Security [12–14]. As such, NIST considers security requirements for automation systems from an information security point of view, which is an important contribution in bringing information security expertise into the world of automation. In a survey of 104 energy security professionals [15], more than 70% of the respondents stated that security has not been adequately addressed in smart grid deployment and that smart grid security standards move too slowly to keep pace with smart grid deployment.

The aforementioned set of standards give directions on how information security could be organized, and a set of baseline requirements to both organizational and technical aspects. The general information security standards should indeed be adapted to a smart grid setting.

3. CULTURE AND TRADITIONS

Power automation systems and ICT systems have traditionally been operated separately. There have been limited, if not zero, logical connections between them, and they have served quite different purposes. The staff operating the two systems tend to have different backgrounds: electric power engineering and computer science. The technology bases are different and so are management routines. Wei *et al.* [16] point at four major differences between the power automation systems and ICT systems:

- Security objectives: whereas ICT aims at integrity, confidentiality, and availability, in that order, power automation is first and foremost concerned about human safety, before continuous operation and protection of physical components.
- Security architecture: whereas ICT has the central server with the highest security level in the middle of the network, power automation needs to protect all edge nodes just as well as the central control systems.
- Technological base: the variety of systems in use in ICT is limited compared with the number of proprietary systems and technologies used in power automation.
- Quality-of-service requirements: whereas rebooting is a common way of fixing an unstable office computer, this is not accepted in the power automation system as it results in disruption of operation, which usually has potentially huge financial consequences.

Power automation systems were built to run continuously without interruptions in quite specific operating environments. Information security measures were not among the requirements as there were no relevant threats in that category. Authentication, encryption, and detection of incidents are therefore usually not implemented in typical automation systems nor is the hardware designed with enough memory and processing capacity to support such mechanisms [17], which calls for new information security mechanisms that are specifically designed to fit the technical properties of power automation systems and still let them fulfill their operational requirements.

Incidents affecting power automation systems may however have severe consequences, both to business operation and even to life, health, and the environment. Such consequences are usually more associated with safety than security, and hence, the systems have been designed to meet safety requirements. This is also what characterizes the mindset of the staff operating power automation and distribution systems.

Fabro *et al.* [18] stress the need for understanding of cyber security as a fundamental condition for successful implementation of smart grids:

> *"(. . .) Without properly understanding the inherent risk in the Smart Grid, we risk either abandoning an exceptionally promising solution for energy issues or deploying a system that could be the Achilles heel of any industrialized nations critical infrastructure."*

3.1. Information security culture

Power automation staff are used to their proprietary systems not being connected to any external network and hence not used to think about the outside world as a possible threat towards their systems. They do not even necessarily recognize their systems as actually being ICT. ICT staff are used to computers failing from time to time, needing a reboot before they work all right again. Downtime is unfortunate, but sometimes necessary, and does not always have large financial consequences, especially not if it is planned. Testing and installing patches are quite common. In power automation, testing and installing patches are extremely difficult as they most probably lead to some downtime. *If it works, do not touch it*, is a tacit rule of thumb, which results in large parts of such systems being outdated and unpatched, and hence, vulnerable to a great number of known attacks.

Recognizing an information security incident is difficult if one is not trained for it. Experiences from the oil and gas industry show that a computer may be unstable for days

Security Comm. Networks (2013) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

and weeks without anyone recognizing it as a possible virus infection [19]. Ensuring that the organization detects and handles such an incident is a cultural challenge just as much as a technical one.

Even vendors of hardware and software within the domain of automation and control have a challenge ahead regarding information security culture. Information security needs to be a fundamental property of all products entering a networked environment, and vendors must accept their responsibility in these matters. They should ensure that their engineering processes include information security features from the beginning. In addition, they need to learn to appreciate feedback that they may have on vulnerabilities and bugs. Govindarasu and Hahn [20] discuss what the power industry has to learn about such vulnerability disclosure. There are some competent computer analysts out there testing software systems for flaws and vulnerabilities, merely because they think it is challenging and fun. Their purpose is usually not to misuse the weaknesses they might discover; they rather notify the system owner or system developer and give them the chance to fix the problems within a reasonable time frame before they eventually publish information on it to the public. This method is usually referred to as “responsible disclosure” [21]. Vendors should embrace such feedback rather than ignore it, as it is better to know about the vulnerabilities and be able to fix them, than experiencing directed attacks where the vulnerabilities are exploited.

3.2. Academia—islands of disciplines

In academia, there are quite clear divisions between departments such as computer science, electrical engineering, cybernetics, and electric power engineering, all of which need to be actively participating in the smart grid evolution. Such divisions are reflected in organizational structures, research projects, scientific publications, and teaching. When students graduate, they carry with them this mentality of isolated scientific traditions, and their future employers are most likely organized like the universities, with the same types of clear divisions. Also, there are differences between the disciplines regarding terminology, culture, and methods. Obviously, this challenges the success of smart grids, which depends on successful scientific and professional cooperation.

The industry is forced to integrate experts from different areas and minimize these established divisions. They have already realized that they will not succeed with their smart grid deployment without such collaboration. Academia, both universities and research institutions, needs to strive to overcome their existing divisions as well and overcome the multidisciplinary challenges to take part in the smart grid evolution.

Both computer scientists and electrical engineers contribute with papers within the domain of information security in smart grids. The authors’ background has a great influence on which terminology is used in a paper. In many cases, it seems like the audience is assumed to be from within the same scientific area as the author. Authors should rather take into account that readers may have a different background than themselves and that several terms and concepts may have different meanings within different scientific fields. Within the topic of smart grids, experts from a broad range of scientific fields share the interest of reading each other’s work. Papers should be written for a broader audience; hence, one should always specify concepts and terms to make sure that there will be no misunderstandings or room for personal interpretations, as discussed in Section 2.

Several scientific papers claim to present information security challenges or research related to smart grids. However, in many cases, the results are not really smart grid-specific. The authors just state that the results are applicable for the smart grid domain as well as the domain that was originally the objective of the research. This might very well be true but needs to be thoroughly justified. As the smart grid area is still quite new, papers that try to adapt well-known results from one area into this new one can be quite useful. As time goes by, it is expected that more research will be carried out with smart grids as the main focus. Results from this research will have more impact and provide more value than many of the papers published up till now.

4. RISK ASSESSMENTS

Several methods and tools exist to support risk assessments, some lightweight and some more comprehensive. Performing a comprehensive risk assessment may seem like an ordeal; therefore, it is usually a good idea to start with a high-level assessment to have a first impression of the system and the main threats and vulnerabilities. Then, some of the most interesting findings could be further elaborated through a more detailed assessment. The first phase of any risk assessment is to clearly define the object of consideration: which parts of the systems should be assessed and which parts should be left out.

Figure 3 [22] shows a conceptual model of the AMI, where the smart meter in a private home communicates directly with the front-end system at the DSO or via a concentrator in a substation. Different communication technologies can be used, depending on what is available and most suitable in the specific geographical area. Such a figure is a sufficient starting point for a high-level risk assessment. The next steps include identifying technical interfaces, possible technologies, participating actors, and preferably a set of scenarios or use cases for the system in focus. Thereafter, the assets of the systems (the values, what is to be protected) should be identified before threats (what can cause an incident) and vulnerabilities (what makes the system susceptible for the threats) are described. Possible consequences from an incident should then be documented. The resulting risk is then a product of the consequences and the probabilities of occurrence of unwanted incidents. This describes a regular risk assessment for any ICT system in general.

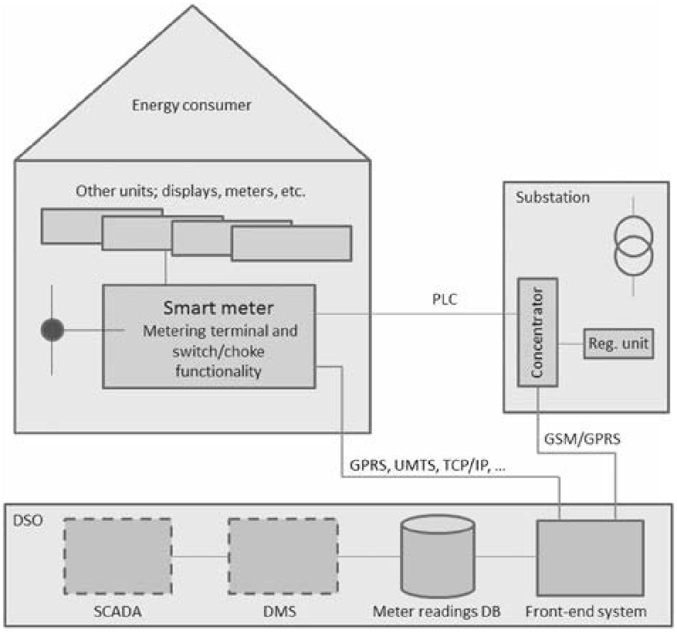


Figure 3. Advanced metering infrastructure [22]. SCADA, supervisory control and data acquisition; DMS, distribution management system; DSO, distribution system operator; GPRS, general packet radio service; UMTS, Universal Mobile Telecommunications System; PLC, Power Line Communication; DB, Database; GSM, Global System for Mobile Communication.

4.1. Cross-sectorial interdependencies

For each ICT system, there are usually some characteristics that need special attention. For the smart grids, there is the property of dependence. The power supply will depend just as vitally on ICT systems as ICT systems already vitally depend on power supply. As an example, an information security breach to the power automation systems may cause power outage. This outage may also affect the same power automation systems and put them out of function. Naturally, there should be extra power supply available, but it is quite important that this redundant supply last long enough to ensure availability for the power automation systems during a crisis. This two-way dependence must be recognized as it requires some extra thought when performing risk assessments. Methods exist that support such cross-sectorial assessments, as Kjølle *et al.* describe in [23].

Datta Ray *et al.* [4] discuss risk management approaches specifically tailored for smart grids. They recognize the challenges of studying ICT systems and power automation systems combined and provide a set of methods for modeling threats and vulnerabilities. They refer to the well-known models STRIDE for classification of the following threats [24]:

- spoofing,
- tampering,
- repudiation,
- information disclosure,
- denial of service, and
- elevation of authority or privilege;

and DREAD; for classification of the following vulnerabilities [24]:

- damage potential,
- reproducibility,
- exploitability,
- affected community, and
- discoverability.

However, they still point out the need for more research in the area of risk assessments for smart grids in order to obtain adequate support for viewing ICT systems and power automation systems in a correlated manner.

4.2. Measuring risks

The total cost for information security includes both investments on preventive mechanisms and financial consequences of unwanted incidents, both damage, and repair and recovery. These two need to be balanced. Standardized methods for calculating risks would help in determining where to put the investments. ISO/IEC 27004 [25] provides guidance on assessment of the effectiveness of an information security management system and controls. The standard supports the requirements described in ISO/IEC 27001 [26]. It describes how attributes can be quantified and converted into indicators tailored for decision making.

Some research effort has been put into the topic of measuring risk and modeling vulnerabilities in smart grids as well. Hahn and Govindarasu [27] present a framework for analyzing the exposure of cyber attacks in a smartgrid. Their framework is based on access graphs, which relate to attack trees and attack graphs—techniques that are commonly used in vulnerability modeling. Each component and interface of a system is represented as nodes, and the edges represent possible ways for an attacker of entering and leaving nodes. Each edge is weighted, and the weight is set based on the level of effort that is needed to compromise that edge. The weights can be recomputed after a change to any security mechanism is performed to see how this change affects the total vulnerability of the system. Determining the weight, however, is no exact science, but some estimates would at least show which edges are more prone to be exploited than others. A general problem with access graphs, just like attack trees and attack graphs, is that it is almost impossible to include all possible attack vectors. Also, only known vulnerabilities can be used for modeling, which leaves out zero-day vulnerabilities, existing vulnerabilities that are not yet discovered. Zero-day vulnerabilities represent a great problem, as it might be attackers that make the first discovery. Ten *et al*. [28,29] have done quite extensive research in the area of measuring risk using both generalized stochastic Petri nets and attack trees for modeling vulnerabilities in and attacks to SCADA systems. Negrete *et al*. [30] present a method for evaluating the financial impacts of cyber attacks. They use a four-layer structure: physical network, communications/control, commodity market, and cyber security. The latter is the top layer, representing investment alternatives and upgrades to the security on the communications/control layer. It does not seem obvious why the cyber security layer is the top layer, as it might relate closely to the first two layers. Still, the authors show how the impacts of attacks change depending on different levels of security investments. The impacts may also be time variant, as an attack at noon may have different consequences for the market than an attack at midnight.

Research approaches like these are praiseworthy attempts on using metrics for evaluating information security in smart grids, which is indeed a challenge. However, theoretical models and methods may seem like great ideas when initially described, but there is a lack of scientific papers thoroughly evaluating the actual use of such metrics more extensively than just as a proof-of-concept. There are some fundamental challenges that need to be overcome in order to make measurements work in practice. In some areas, estimating probabilities of occurrence of unwanted incidents is a mathematical or statistical exercise. For ICT systems, this is a complex and often impossible exercise [17]. Attackers' possible goals and strategies should be thoroughly considered, but it can be quite hard to grasp all their capabilities and motivations. The probability of someone wanting to attack a nation's power system may change from one day to the next because of political circumstances. Smart grids are just as complex as ICT systems alone—complex interdependencies in infrastructure combined with (quite often) incomplete documentation of systems and several possible threats. Probability estimation based on an experienced gut feeling may actually be the best possible alternative.

Another issue is ease of use. Implementing yet-another-process requiring personnel resources, documentation, a management system and attention from top management can be quite difficult to go through within an organization. Lightweight, not time-consuming, efficient, giving value, these are all properties of importance when designing the optimal measurement protocol.

4.3. ICT security threats—what's new?

In general, threats to ICT systems are well known, and there exist several well-known and well-functioning countermeasures. Limitations of these countermeasures are also well known, as well as how they still can be quite successfully implemented. If this was not the case, large-scale hacker attacks would succeed every day, resulting in totally unusable ICT systems and a major slowdown in efficiency in a large part of industry and public services worldwide.

Well-known threats and attacks are however continuously improved (from the attackers' point of view) to hit new types of computer systems, such as automation and control systems. The trend of connecting such systems to the Internet makes them vulnerable to attacks that can be remotely executed. With offline systems, the attacker needs to have physical access to the target systems in order to execute an attack. With online systems, targeted attacks can be executed from anywhere in the world. Also general, untargeted attacks may hit all kinds of systems as long as they are online.

Implementing all possible information security measures is never an optimal solution. This is quite costly and will not be worth the investment. Obtaining 100% security should therefore not be a goal but rather determining an appropriate level of security and implementing the measures needed to obtain this is far more realistic. Determining an information security level corresponds to determining what are the acceptable risks, and then being prepared to manage unwanted incidents.

5. PRIVACY

With the old metering technologies in place, each household reads their meters quarterly or monthly and reports to the utility company for billing. With the new smart meters implemented, the utility companies will automatically receive measurements collected much more frequently, several times a day. For billing purposes, hourly readings are needed, but for grid management purposes, the DSOs can make use of per-minute readings or even per-second readings. These are huge amounts of data related to each household. Usage data must be kept confidential as they can tell a lot about the lifestyle and habits of the specific household. In its most simple form, it will clearly show when someone is at home and when the house is empty [31].

One week of readings will give quite clear indications on when the house will be empty during the next week, which is interesting information for someone planning robberies. More detailed readings can reveal information on which activities take place inside the house, as many household appliances have unique signatures that can be read from fine-grained metering data [32]. Such information can be of interest to house robbers looking for a specific TV or other specific household appliances; to commercial advertisers, who can personalize their messages and products when they know their receivers' habits; to the police, as certain criminal actions such as growing cannabis plants will leave their own fingerprint in the usage data; to employers wondering whether their employees are skipping work; and to insurance companies doing research on their customers before paying compensations. There is no doubt that usage data must be protected from unauthorized inspections, and there must be clear rules and guidelines in place describing what this data may be used for and who should have access, as there is for other similar large-scale collections of personal information, such as money transactions, phone calls, and broadband usage.

Much research is being carried out within the area of privacy in the smart grid, and then especially related to smart metering, as this is the area where the main privacy challenges arise.

5.1. Protection of consumption data

Non-intrusive appliance load monitoring techniques [32,33] can be used for decoding energy consumption data into which individual household appliances are in use. A reading frequency of 15 min can identify some of the most common appliances. An increase of the reading frequency will increase the accuracy of appliance identification. Efthymiou and Kalogridis [34] suggest a method for overcoming this privacy issue by giving each smart meter two different IDs: one anonymous ID, which is used for the most frequent metering reports used for management and network control purposes, and one known ID, which is associated with the household and used for billing purposes. Assuming that the anonymizing process including key and certificate exchanges and the suggested escrow third party can be trusted, this method will contribute to preservation of privacy, as the most frequent readings will be anonymized and hence not possible to track back to a specific household.

However, the utility companies are interested in knowing more than just the total energy consumption from each meter. For production planning and grid management, they find it quite useful to know what kind of household each meter reading belongs to. Fhom *et al.* [35] address this privacy issue by suggesting a different approach, introducing a user-centric privacy manager that allows each individual customer to control which and how much information is disclosed to which other smart grid parties. A smart energy gateway (SEG) should be the node connecting each home, including smart appliances and the meter itself, to the power supplier, distribution network supplier, billing provider, and other relevant actors. Each purpose, or functionality, will be represented by a corresponding software agent on the SEG, and the security architecture of the SEG should support secure multiplexing access to physical resources so that the different software agents would not interact in unfortunate and unsecure ways. Introducing such a privacy manager would give the end users access to inspect what kind of data is actually collected and by whom, including the possibility of having a certain amount of control over this data collection. This would provide a degree of transparency, which is not present today.

It should be carefully considered whether users would be interested in controlling their own privacy. Some should rather be protected from themselves, from being able to perform unfortunate choices. The majority of end users will most probably not be able to understand their privacy exposures and even less able to understand how to mitigate them. The services provided must therefore be privacy-preserving and trusted by default; the principle of privacy-by-design should be followed at all times during development and in operation, such that the customers do not have to be concerned about their own privacy.

In June 2011, the European Data Protection Supervisor (www.edps.europa.eu) provided an Opinion on the Commission Recommendation on preparations for the roll-out of smart metering systems [36]. He recommends that consumers should not be forced to install a smart meter if they do not want the advantages of time-of-use tariffs. Alternatively, the functionalities of granular readings and the remote on/off control should be disabled as a default setting, and an informed consent must be given before they are enabled.

This idea follows the privacy-by-design principle and lets the consumer choose whether he allows a privacy-invasive method being used for correct billing or accepts the risk of paying higher bills than strictly necessary. The DSOs would however still want to have more accurate readings than today in order to ease and increase the quality of grid management. Two methods to consider in this matter are to keep the reading frequency lower than every hour; it might suffice to read once or twice a day. If more detailed readings are strictly needed, meter data should be anonymized and preferably aggregated in order to preserve the privacy of the consumers.

5.2. Use of consumption data

Legislation on protecting personal information varies in different countries. In some countries, it is sufficient to notify the owner when the terms or purposes of use change, as opposed to ask for consent. The US-based NIST has provided guidelines for privacy and the smart grid [13], where they discuss the concept of privacy and how smart grids may pose privacy challenges. The guidelines contain recommendations for mitigations of smart grid privacy issues as well, and the intended readers include all entities that are involved with personal information related to smart grids in some way. A European Union (EU)-initiated Task Force on Smart Grids has also identified recommendations for data handling, data security, and data protection [37]. They provide an overview of the European legislation, identify potential risks in the handling of personal data, discuss data and access rights, and analyze how such issues should be handled. They also criticize the NIST report and state that it is too much based on end users' consent; the task force would rather see clear regulations on what kind of data may be collected and for which purpose.

In Norway, the Personal Data Act [38] is quite clear in stating that personal information may only be collected for specified purposes, and the owner of the information shall be informed and asked for consent if the collected information is to be used for other purposes than first planned. The data owner has the right to refuse, and an acceptance needs to be actively granted, as opposed to a tacit acceptance. The Norwegian Data Inspectorate has provided a guide specifically related to personal data in connection with smart metering [39]. This guide is intended to help the DSOs to fulfill the requirements stated in the Personal Data Act.

The European Data Protection Supervisor is looking into whether further legislative action is needed on an EU level. He would specifically like to see more guidance on retention periods and recommends that the use of privacy-enhancing technologies and similar techniques for data minimization is made mandatory. He also points out that each consumer should have direct access to their energy usage data.

Guidelines and recommendations from institutions like NIST and EU-initiated working groups, in addition to data protection supervisors and data inspectorates, are indeed necessary for helping DSOs and other parties in preserving consumers' privacy when implementing smart metering. Privacy is an important principle that should not be sacrificed for the interest of efficiency and new technological possibilities and solutions, and having the consumers' trust is essential for smart grids to be a success.

Large amounts of personal information have been stored for a long time by several actors; securing such storage can be obtained without large research efforts. However, research is needed to fully investigate how the privacy-by-design principle can be followed in practice when developing smart meters and implementing an AMI. The development and use of privacy-enhancing technologies, anonymization, aggregation, and possibly new and still unknown techniques are indeed required.

6. SECURITY ARCHITECTURE

A thorough modernization of the aging power grid infrastructure implies the need for an appropriate information security architecture. In each device, the communication channels and the interfaces between them need to be secured, privacy issues for the consumers must be addressed, the strategy of defense-in-depth should be obeyed, and the large geographical spread of the network must be carefully taken into account. Both a high-level holistic view and in-depth focused investigations are needed in order to decide on an appropriate information security architecture.

The operational requirements governing power automation systems today cannot be circumvented. Performance must be maintained; continuous operation as well; and the properties of hardware and software already in use must be regarded when designing new mechanisms, as described in Section 3.

The worldwide approved ISO standards represent the best starting point. They could be supplemented with the comprehensive documentation published by NIST—a set of guidelines on smart grid cyber security strategy, architecture, and high-level requirements [12]. Their architecture includes a set of domains, a high-level view on actors, and a logical reference model for the smart grid, in addition to a thorough list of high-level information security requirements. The Advanced Security Acceleration Project has provided a more focused document, describing a security profile for AMI [40]. It addresses the complete AMI from the smart meter at the consumer's side to the meter data management system at the DSO's side. This documentation is also quite comprehensive and is aimed for organizations developing or implementing AMI solutions. These reports describe current good practice, although local adaptations of the recommendations, based on risk assessments and actual incidents, if any, are needed when they are put into use.

Ericsson [2] describes how the power automation grid started out as "islands of automation" and became more integrated as time went by. The utility companies have been asking for more openness—commercial-off-the-shelf products and more integrated systems. This seems to be the future for the power industry. Ericsson suggests to decouple the operational SCADA/EMS system from administrative systems to ensure an appropriate information security level. This, however, is a step backwards and does not appear as a future-oriented solution. He then discusses the approach of studying SCADA/EMS systems in terms of domains, where business operations are grouped together and each domain has an information security policy, a set of requirements, mechanisms, and one responsible "authority". It is claimed that this will ensure a minimum security level for all systems within the same domain.

Wei *et al*. [16,3] propose a novel security framework for power grid automation systems. This is designed to meet the requirements of integration in a non-intrusive fashion, performance in terms of modularity, scalability, extendibility, and manageability, and also alignment to the Roadmap to Secure Control Systems in the Energy Sector [41]. The framework consists of three layers (power, automation and control, and security), and the three major conceptual components in the framework are as follows:

- *Security agents*: protection at the networked device level, firmware or software, access control, and IDS.

- *Managed security switch*: for protection of bandwidth and prioritizing of data, used across the automation network.
- *Security manager*: in the center of the power automation network, a security agent master; obtains and downloads patches to security agents, and collects data from agents.

Test results show that the security agents did not imply significant reduction of performance on SCADA communication, some vulnerabilities were mitigated or partially mitigated, and the IDS reported some findings.

Boroomand *et al*. [42] address the topic of deciding the optimal level of automation in a SCADA setting, thereby mitigating cyber security risks. The authors motivate their work by pointing out the new security challenges following the implementation of smart grids, where security and reliability are not always aligned. The concept of varying the level of automation based on current threat level is intriguing, and finding the optimal balance between human responsibilities and automatic processes also related to incident detection and response is an interesting idea. However, it is not always the case that a system based on human decisions and actions is more secure than fully automated systems, as it seems to be assumed by the authors. Humans make mistakes, and the higher complexity of the system and tasks, the higher probability for wrong decisions or at least minor mistakes, which in the worst cases may have quite severe consequences.

Proving that certain information security mechanisms do not affect SCADA performance is a rather hard exercise. Performing tests and evaluations in smaller lab facilities may show good results, but the real world is usually a bit more complex than what we manage to set up in the lab. Also, some of the stated operational requirements are difficult to test extensively no matter how realistic the test facilities are.

7. INCIDENT MANAGEMENT

Potential computer break-ins, industrial espionage, malware attacks and denial-of-service attacks are some of the threats to ICT systems that companies face today. As smart grids are complex systems consisting of complex power grids that interact with equally complex ICT systems, these threats will in the near future also be highly relevant for the power industry as well. The ability to appropriately prepare for, and respond to, information security incidents is essential for companies that need to ensure and maintain continuous operation of their systems.

Incident management is the process of detecting and responding to incidents, including supplementary work as learning from the incidents, using lessons learned as input in the overall risk assessments, and identifying improvements to the implemented incident management scheme. ISO/IEC 27035 incident management [43] describes the complete incident management process. This is a fairly new standard (2011) but is based on a technical report that was produced in 2004. The process comprises five phases: plan and prepare, detection and reporting, assessment and decision, responses, and lessons learned. The guideline is quite extensive and will indeed be costly to adopt to the letter, but it is a collection of practical advice, key activities, and examples, and is indeed useful for companies establishing their own security incident organization. The ISO standard addresses corporate systems in general and does not contain any considerations related to power automation systems. There is a need to delve into the standard and adopt it for a smart grid setting, where corporate systems and control systems are connected in different ways.

In their Guidelines for Smart Grid Security (NISTIR 7628), NIST describes a set of high-level requirements for incident response for a smart grid information system [12]. All requirements are however on the governance, risk, and compliance level, and are therefore more high level than what the ISO standard provides. They contain no practical advice; hence, they are more useful in a planning process than during business operation. They also contain no specifics related to the cooperation of corporate systems and control systems. In part 3 of their Guidelines [14], NIST however points out the need for research on incident response for the cross-domain of ICT and power systems. More specifically, the issues of response and containment, intrusion detection and prevention, and event and impact prediction are emphasized.

NIST 800-61 [10] addresses computer security incident handling, whereas NIST 800-82 [11] contains several recommendations for securing ICSs, including a comprehensive overview of vulnerabilities. The security profile on AMI [40] that contains a large number of security concerns, guidance, and controls related to AMI also includes a separate section on incident response. The requirements are quite high level, similar to those listed in the ISO standard and NISTIR 7628 as well, but at least, they are directly addressing AMI, which is an important part of smart grids.

There are not many scientific papers describing real-life experiences regarding incident management. The Annual FIRST Conference Forum for Incident Response Teams (www.first.org) brings together such expertise worldwide, and one or two presentations each year seem to cover real-life experiences. These presentations are however not publicly available afterwards. A large amount of available publications from relevant venues are concerned with the technical reporting systems in use, vulnerability registration, establishing response teams, and computer forensics—topics that are indeed relevant but not as interesting as experience papers would be. Metzger *et al*. [44] present their real-life experiences, covering the complete process from detection, response, reporting, and even some short notes on how lessons learned were used in the improvement process at the end of the incident handling cycle.

Hennin described in 2008 the Cyber Attack Alert Tool project [45] that aimed at developing an industry standard protocol for sharing information about control system cyber incidents across all critical infrastructure sectors. The project idea seemed promising, as it was going to focus on early warnings, as opposed to the Repository of Industrial Security Incidents (www.securityincidents.org) database, which contains reports written in the aftermath of incidents and where a quite costly membership is required to gain access. However, it has turned out to be difficult to find papers describing results from the Cyber Attack Alert Tool project, so it is not known whether the project led to a breakthrough.

Although standards and recommendations exist on the area of incident management, also with respect to smart grids, there is a lack of documented research and experience related to managing incidents in an operating environment where automation systems and ICT systems are closely integrated. An efficient incident management process is just as important as technical information security measures when continuous operation is a governing requirement.

7.1. Real-life incidents

Information and communication technology security incidents are indeed not science fiction, they are already happening. During the last 10 years, there have been several examples of power outages or other types of damage to automation and control systems caused by hackers, untrusted employees, or software failures. The most famous attack up till now is Stuxnet [46–48], which appeared during summer 2010 as an advanced piece of malware created to target ICSs. Such systems have been attacked before, but not with this kind of specifically designed malware. Stuxnet is important mostly because it demonstrated that it is indeed possible to perform attacks against critical infrastructure and even infrastructure not connected to the Internet. Quite recently, it was announced that the USA and Israel were behind Stuxnet, and the intention was to attack Natanz, an Iranian power plant [49]. Natanz was indeed attacked, but a minor bug in the Stuxnet exploit made Stuxnet go “in the wild” and hit several other systems worldwide.

Another recent attack, Night Dragon [50], was identified in November 2009 as an attack targeted at the energy sector. The goal was harvesting of sensitive information related to competitive proprietary operations and financial details regarding field bids and operations. A similar attack was also discovered in Norway 2 years later [51]; 10 large companies within defense, oil, and energy experienced industrial espionage attacks where communication were being monitored, and the goal was to capture sensitive information. These two cases did not specifically target automation and control systems, but it shows that the energy sector is an attractive target for attackers, and smart grids imply that the attack surface increases; there will be more ways of attacking a company or the industry as a whole, subsequently causing damage that impact larger parts of the society.

Duqu and Flame are two pieces of malware that have similarities to Stuxnet, and researchers therefore believe that all three of them were created by the same authors [52-54]. They were detected in September 2011 and May 2012, respectively, but they are both believed to date from 2007. Duqu is a reconnaissance tool, and Flame is an espionage tool, and both have Iran’s nuclear program as the main target, just like Stuxnet did. Flame has hit private companies, academic institutions, governmental systems, and home users, not automation and control systems specifically. It has been around for a long time without being detected; antivirus suppliers have therefore not provided any functionality for detecting nor removing a Flame infection [?].

Flame and its relatives represent the kind of threats that the power industry need to be prepared for. A planned and directed attack towards the industry should be assumed to comprise attempts to cause physical damage together with attempts to gather confidential information.

8. NOT JUST NEGATIVE PROSPECTS

Information security is more often seen as a limitation than an enabler. This might be due to the nature of security; there is usually a trade-off between security and properties such as functionality, user-friendliness, performance, efficiency, and cost. Still, the fact is that many services cannot be set to life without at least a basic level of security. In the case of smart grids, which is a critical infrastructure, or more correctly a combination of two critical infrastructures (power and ICT), information security issues must be addressed appropriately.

When critical information security challenges are overcome, the smart grid represents a huge potential for the industry. It will provide for more efficient management of the grid, real-time monitoring of demand response, efficient error detection and repair, and the possibility of affecting end users’ energy consumption in such a way that a major investment in upscaling the grid capacity may be avoided, or at least postponed. End users may contribute to environmental advantages if they are able to exploit the smart grid in the right way; with more correct billing—a clear connection between consumption and the bill—they might reduce their total consumption, and they may take part in power production by having their own windmill, solar panel, or the like, and hence contribute to increasing the amount of renewable energy.

It is easy to point out many challenges, both security-wise and other, when talking about smart grids. However, when two or more scientific fields meet, there are great possibilities ahead. Cross-discipline cooperation makes people see their own field in new ways, which can lead to results and innovations that otherwise would not be discovered.

9. CONCLUSION AND FURTHER WORK

Successfully adapting good ICT security practice to power automation, distribution, and control systems, while at the same time fulfilling the current requirements for power grid operation, is a huge step in the direction of successfully securing the smart grid. Local adjustments are however needed in order to comply with existing solutions and local laws and regulations. Still, there are smart grid-specific challenges that need to be addressed that are not possible to solve through existing measures.

Technical measures are not sufficient for obtaining secure smart grids. Increased understanding, knowledge, and awareness are needed among both ICT staff and power automation staff. They need to cooperate more extensively than today, and they need to understand each other's mindsets, terminology, needs, and information security objectives. The whole organization needs to be onboard, and organizational and cultural changes cannot be bought. Neither should they be expected to have a "quick fix"; a careful and long-term approach is required. Otherwise, there is a risk of ending up with two opposites—the ICT people and the power automation people—both fighting for their views and their priorities, and both being afraid of being redundant. The top management must recognize organizational and cultural measures as a major priority area and lead the way by truly showing that collaboration and mutual understanding is needed in order for smart grids to be a success.

Securing the smart grids is therefore not just another security project. It takes more than time and money to succeed.

A large part of smart grid research today concerns AMI specifically, even though there are many uncertainties ahead regarding smart grids: are the smart meters a kind of a smart grid, will there be more to it, when will the concept of smart grids be achieved, who will do it, what are the benefits, and so on. AMI is just the beginning of the smart grid roll-out. While the industry fully focuses on implementation of the AMI, researchers should contribute looking forward to what comes next.

We plan to study how ICT security incidents are being detected and responded to—both by technical measures and by human actions—and how the aftermath is handled—information sharing, lessons learned, and how experiences are transferred into the overall work with information security in companies operating power automation and control systems. This must be studied with respect to both ICT systems and the power automation and control systems in order to identify cooperation, possible synergy effects from future cooperation, and the management system in general. This will require a socio-technical approach, as the field of research is neither only technology nor man but indeed a combination of the two. It will be impossible to improve anything without addressing both. The results of this work will hopefully contribute to efficient and successful incident management in smart grids environments, where the worlds of ICT and automation meet.

ACKNOWLEDGEMENTS

I would like to thank Professor Svein J. Knapskog (NTNU), Senior Scientist Martin G. Jaatun (SINTEF), Professor Poul E. Heegaard, and PhD student Jonas Wäfler (both NTNU) for providing invaluable input and comments and participating in fruitful discussions.

REFERENCES

1. Kluza J. Status of grid-scale energy storage and strategies for accelerating cost-effective deployment. PhD Thesis, MIT 2009.
2. Ericsson GN. Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery* 2010; **25**(3):1501–1507.
3. Wei D, Lu Y, Jafari M, Skare PM, Rohde K. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid* 2011; **2** (4):782–795.
4. Datta Ray P, Harnoor R, Hentea M. Smart power grid security: a unified risk management approach. *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2010; 276–285.
5. Khan H, Xu Z, Iu H, Sreeram V. Review of technologies and implementation strategies in the area of smart grid. *Australasian Universities Power Engineering Conference (AUPEC)*, 2009; 1–6.
6. ISO/IEC 27000:2009 Information security management systems—overview and vocabulary 2009.
7. Idsø ES, Jakobsen ØM. Objekt- og informasjonssikkerhet: metode for risiko- og sårbarhetsanalyse (in Norwegian). *Technical Report*, Norges Teknisk-Naturvitenskapelige Universitet (NTNU) 2000.
8. Line MB, Nordland O, Røstad L, Tøndel IA. Safety vs security? *Eighth International Conference on Probabilistic Safety Assessment and Management (PSAM)*, Stamatelatos M, Blackman H (eds). ASME Press: New York, 2006.
9. Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 2004; **1**(1):11–33.
10. NIST. 800-61: Computer Security Incident Handling Guide 2008.
11. NIST. Guide to Industrial Control Systems (ICS) Security 2011.
12. NIST. 7628-1: Guidelines for Smart Grid Cyber Security 2010.
13. NIST. 7628-2: Guidelines for Smart Grid Cyber Security 2010.
14. NIST. 7628-3: Guidelines for Smart Grid Cyber Security 2010.
15. nCircle, EnergySec. 2012 Smart Grid Cyber Security Survey. *Technical Report*, nCircle 2012. URL http://

www.ncircle.com/index.php?s=resources surveys Survey-Smart Grid-2012

16. Wei D, Lu Y, Jafari M, Skare P, Rohde K. An integrated security system of protecting smart grid against cyber attacks. *IEEE Innovative Smart Grid Technologies (ISGT) 2010*, 2010; 1–7, doi:10.1109/ISGT.2010.5434767.
17. Rativa LCT. Risk assessment for power system security with regard to intentional events. PhD Thesis, Institut Polytechnique de Grenoble 2008.
18. Fabro M, Roxey T, Assante M. No grid left behind. *IEEE Security & Privacy* 2010; **8**(1):72–76.
19. Jaatun MG, Albrechtsen E, Line MB, Tøndel IA, Longva OH. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection* 2009; **2**:26–37.
20. Govindarasu M, Hahn A. What the power industry has to learn about cyber vulnerability disclosure. IEEE Smart Grid Newsletter January 2012. URL http://smartgrid.ieee.org/newsletter/january-2012/479-whatthe-power-industry-has-to-learn-about-cyber-vulnerability-disclosure?utm_source=IEEE+Smart+Grid&-utm_campaign=f4bc47e6e9-January_2012_Smart_-_Grid_Newsletter1_17_2012&utm_medium=email
21. Shepherd SA. Vulnerability disclosure. *Technical Report*, SANS 2003.
22. Line MB, Johansen GI, Sæle H. Risikovurdering av AMS. Kartlegging av informasjonssikkerhetsmessige sårbarheter i AMS. *(In Norwegian). Technical Report*, SINTEF 2012.
23. Kjølle GH, Utne IB, Gjerde O. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering and System Safety* 2012; doi:10.1016/j.ress.2012.02.006. URL http://www.sciencedirect.com/science/article/pii/S09518320120 0021X.
24. Swiderski F, Snyder W. *Threat Modeling*. Microsoft Press: Redmond, Washington, 2004.
25. ISO/IEC 27004:2009 Information technology—Security techniques—Information security management—Measurement 2009.
26. ISO/IEC 27001:2005 Information security management systems—Requirements 2005.
27. Hahn A, Govindarasu M. Smart grid cybersecurity exposure analysis and evaluation framework. *IEEE Power and Energy Society General Meeting*, 2010; 1–6.
28. Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, Nov 2008; **23**(4): 1836–1846, doi:10.1109/TPWRS.2008.2002298.
29. Ten CW, Manimaran G, Liu CC. Cybersecurity for critical infrastructures: attack and defense modeling. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans* 2010; **40**(4):853–865. doi:10.1109/TSMCA.2010.2048028.
30. Negrete-Pincetic M, Yoshida F, Gross G. Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. *IEEE PowerTech Bucharest*, 2009; 1–8.
31. Lisovich MA, Mulligan DK, Wicker SB. Inferring personal information from demand-response systems. *IEEE Security and Privacy* 2010; **8**(1):11–20.
32. Hart G. Residential energy monitoring and computerized surveillance via utility power flows. *Technology and Society Magazine, IEEE* 1989; **8**(2):12–16. doi:10.1109/44.31557.
33. Drenker S, Kader A. Nonintrusive monitoring of electric loads. *Computer Applications in Power, IEEE* 1999; **12**(4):47–51. doi:10.1109/67.795138.
34. Efthymiou C, Kalogridis G. Smart grid privacy via anonymization of smart metering data. *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010; 238–243, doi:10.1109/SMARTGRID.2010.5622050.
35. Simo Fhom H, Kuntze N, Rudolph C, Cupelli M, Liu J, Monti A. A user-centric privacy manager for future energy systems. *International Conference on Power System Technology (POWERCON)*, 2010; 1–7, doi:10.1109/POWERCON.2010.5666447.
36. The European Commission Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 2012.
37. Task Force Smart Grids Expert Group 2: Regulatory recommendations for data safety, data handling and data protection 2011.
38. LOV-2000-04-14-31 Lov om behandling av personopplysninger (personopplysningsloven) (in Norwegian), Ministry of Justice and Public Security 2000.
39. The Norwegian Data Inspectorate: guide for processing of personal data in connection with automatic metering systems within the energy sector 2011.
40. ASAP-SG. Security profile for advanced metering infrastructure 2010.
41. Roadmap to secure control systems in the energy sector 2006.
42. Boroomand F, Fereidunian A, Zamani M, *et al*. Cyber security for smart grid: a human-automation interaction framework. *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010; 1–6, doi:10.1109/ISGTEUROPE.2010.5638949.
43. ISO/IEC 27035:2011 Information technology—Security techniques—Information security incident management 2011.
44. Metzger S, Hommel W, Reiser H. Integrated security incident management—concepts and real-world experiences. *Sixth International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2011; 107–121.

45. Hennin S. Control system cyber incident reporting protocol. *IEEE Conference on Technologies for Homeland Security*, 2008; 463–468.

46. Falliere N, Murchu LO, Chien E. W32.Stuxnet Dossier. *Technical Report*, Symantec February 2011.

47. Albright D, Brannan P, Walrond C. Did Stuxnet take out 1000 centrifuges at the Natanz enrichment plant? *Technical Report*, Institute for Science and International Security (ISIS) 2010.

48. Albright D, Brannan P, Walrond C. Stuxnet Malware and Natanz: update of ISIS December 22, 2010 Report. *Technical Report*, Institute for Science and International Security (ISIS) 2011.

49. Sanger DE. Obama order sped up wave of cyberattacks against Iran 2012. URL http://www.nytimes.com/2012/06/01/world/middleeast/obama-orde red-wave-of-cyberattacks-against-iran.html?_r = 1

50. Global energy cyberattacks: "Night Dragon". *Technical Report*, McAfee 2011.

51. Johansen PA. Stjeler kontrakter, tegninger, passord og hemmelige data (in Norwegian) 2011. URL www.ap.no/nyheter/iriks/Stjeler-kontrakter-tegninger-passord-og-hemmelige-data-6698674.html

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

53. Plikk N. Massivt cyberangrep pågår i Midtøsten (in Norwegian) 2012. URL http://www.aftenposten.no/digital/Massivt-cyberangrep-pagar-i-Midtosten-6838800.html

54. Greenberg A. New research shows Flame malware was almost certainly a U.S. or Israeli creation 2012. URL http://www.forbes.com/sites/andygreenberg/2012/06/11/new-research-shows-flame-malware-was-almost-certainly-a-u-s-or-israeli-creation/

PAPER 3

Information security incident management: Current practice as reported in the literature

Inger Anne Tøndel, Maria B. Line, and Martin G. Jaatun

Computers & Security, vol. 45, p. 42-57, September 2014.
ISSN 0167-4048. DOI: 10.1016/j.cose.2014.05.003

Reprinted with permission from Elsevier.

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security incident management: Current practice as reported in the literature

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

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

ARTICLE INFO

Article history:
Received 5 July 2013
Received in revised form
17 March 2014
Accepted 19 May 2014
Available online 28 May 2014

Keywords:
Information security
Incident management
Incident response
ISO/IEC 27035
Systematic review

ABSTRACT

This paper reports results of a systematic literature review on current practice and experiences with incident management, covering a wide variety of organisations. Identified practices are summarised according to the incident management phases of ISO/IEC 27035. The study shows that current practice and experience seem to be in line with the standard. We identify some inspirational examples that will be useful for organisations looking to improve their practices, and highlight which recommended practices generally are challenging to follow. We provide suggestions for addressing the challenges, and present identified research needs within information security incident management.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

Today, Information and Communication Technology (ICT) plays an important role in all organisations. ICT has brought a lot of benefits to our society. At the same time, it has made us vulnerable to failures and attacks that come via the ICT systems. As organisations have become more and more dependent on ICT, the threats towards these systems have become more prominent. The current situation can be summarised by the following quote by Ahmad et al. (2012):

> "It is inevitable at some stage that organisations will suffer an information security incident. Such an incident may result in multiple negative impacts, such as loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss."

Although a lot of measures can be taken in order to prevent information security incidents from taking place, it is not economically feasible to fully protect all systems (Anderson et al., 2012). Thus organisations need to prepare for what to do in case of incidents in their ICT systems.

The main motivation of this paper is to provide a comprehensive overview of current practice and experiences documented in the literature on information security incident management. A further motivation is to identify the challenges organisations experience when trying to follow existing standards.

The remainder of the paper is structured as follows: In Section 2 we describe our research method. Section 3 provides an overview of the most recognised and well-known standards and guidelines related to information security incident management, and Section 4 presents findings from relevant studies and experience reports. We summarise current

[*] *Corresponding author*. Tel.: +47 97088476; fax: +47 73594302.
E-mail addresses: inger.a.tondel@sintef.no (I.A. Tøndel), maria.b.line@item.ntnu.no (M.B. Line), martin.g.jaatun@sintef.no (M.G. Jaatun).

http://dx.doi.org/10.1016/j.cose.2014.05.003
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

practice, present inspirational examples, and discuss aspects that are particularly challenging, as well as future research needs, in Section 5. Section 6 offers concluding remarks.

2. Research method

The work presented in this paper has been organised as a systematic review and conducted based on recommendations by Kitchenham and Charters (2007). The goal with performing the systematic review was to identify current practice for information security incident management, and in particular experiences made. The research questions that guided the review were thus:

- Q1. How is information security incident management performed in practice?
- Q2. What experiences are reported in literature on information security incident management; what works well, what is difficult?

In the analysis work we also aimed at answering the following research question:

- Q3. To what degree does current practice resemble recommended standards and guidelines?

We limited our study to literature documenting real-life experiences and practices, either in form of experience reports or in form of empirical studies. Furthermore, we only included literature published after 2005.

Relevant literature was identified through a Scopus[2] search using search terms intended to identify all literature that covered incident management of information security incidents: ("incident management" OR "incident response" OR "incident reporting" OR "computer emergency response" OR "computer emergency management") AND ("information security" OR "cyber security" OR "ict" OR "computer security" OR "information technology").

The identified literature was then manually included or excluded in the study by one researcher. A first Scopus search was performed in March 2012, and then a second search was performed in August 2013 in order to identify any literature published since the first search. In addition, we manually went through the publicly available information from the Terena[3] and FIRST[4] conferences, whitepapers etc. from CERT/CC,[5] publications from SANS[6] and the latest IMF[7]-conference.[8] When going through the literature that was included in the study, we studied the references in order to identify additional literature. We added one study from a local university.[9]

One of the papers was analysed by two researchers. The other papers were analysed by one researcher. In the analysis the reported practices and experiences were identified and related to one of the incident management phases described in standards. We particularly identified the experiences and practices that were related to communication and collaboration during incident management, as this was a topic that was considered important in several of the identified papers and spanned all phases.

3. The incident management process

An information security event can be defined as an *"identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant"* (ISO, 2011). An information security incident is then a *"single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"* (ISO, 2011).

ISO/IEC 27035 "Information security incident management" (ISO, 2011) and NIST Special Publication 800-61 "Computer Security Incident Handling Guide" (Cichonski et al., 2008) stand out as two of the main standards and guidelines related to information security incident management. Both offer a structured approach to incident management, including planning and preparing for incident response, what to do when incidents strike, and how to extract lessons learnt afterwards. SANS (Kral, 2011) and ENISA (ENISA, 2010) have also provided guidelines for incident handling, which resemble the structure offered by ISO/IEC and NIST. The guide from SANS is quite short and contains just an overview of which activities belong to each phase. ENISA has excluded the preparations phase and just focused on the activities performed by a response team in case of an incident. ITIL (Brewster et al., 2012) describes the incident management process as consisting of six components; Incident detection and recording, Classification and initial support, Investigation and diagnosis, Resolution and recovery, Incident closure, and Ownership, monitoring, tracking, and communication during the progress of the incident handling. Activities related to planning and preparations are included in other parts of ITIL and hence not presented as part of the incident management process itself. FIRST provides a couple of guidelines on how to set up an incident response team within an organisation. These are specifically concerned with planning and preparations, and do not cover the complete incident management process. CERT/CC describes comprehensive guidelines for establishing and operating an incident response team in their CSIRT handbook (West-Brown et al., 2003). Furthermore, they describe their CERT/CC Incident Handling Life Cycle process.

[2] http://www.scopus.com.

[3] Trans-European Research and Education Networking Association, www.terena.org.

[4] Forum for Incident Response and Security Teams, www.first.org.

[5] www.cert.org.

[6] www.sans.org.

[7] IT Security Incident Management and IT Forensics.

[8] The proceedings from this conference were not available at Scopus at the time of the search, and was included because relevant material had been published at previous IMF conferences.

[9] This study was in form of a student thesis and would thus not be available in a Scopus search. Furthermore, we have performed a search for related student work from other universities, but without results (this may be because such student papers may be difficult to access outside the respective universities).

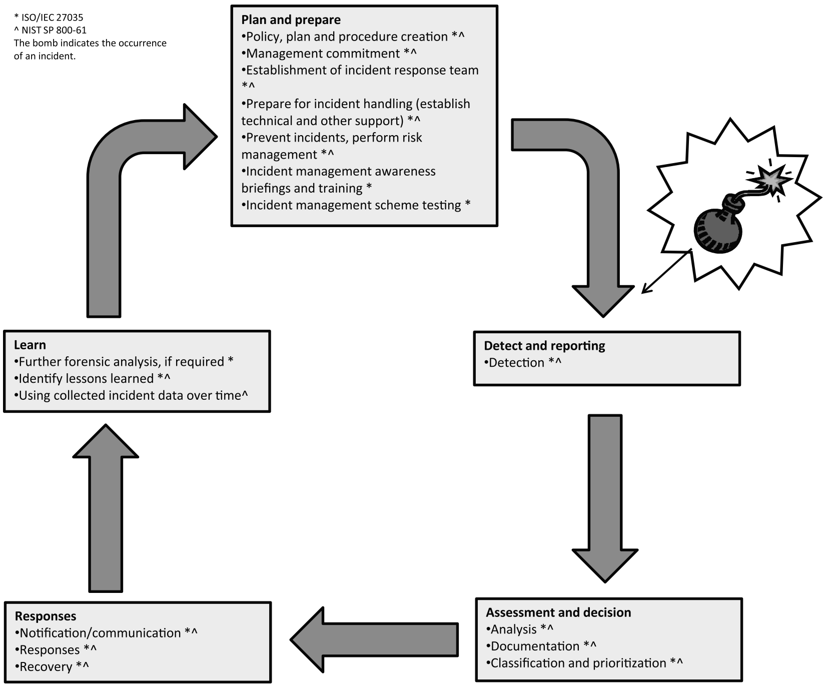

* ISO/IEC 27035
^ NIST SP 800-61
The bomb indicates the occurrence of an incident.
Plan and prepare
•Policy, plan and procedure creation *^
•Management commitment *^
•Establishment of incident response team *^
•Prepare for incident handling (establish technical and other support) *^
•Prevent incidents, perform risk management *^
•Incident management awareness briefings and training *
•Incident management scheme testing *
Detect and reporting
•Detection *^
Assessment and decision
•Analysis *^
•Documentation *^
•Classification and prioritization *^
Responses
•Notification/communication *^
•Responses *^
•Recovery *^
Learn
•Further forensic analysis, if required *
•Identify lessons learned *^
•Using collected incident data over time^

Fig. 1 – The incident management process.

This resembles the processes described by ISO/IEC and NIST; an incident is detected and considered in a triage before a report is generated. Then there are the states of analysis, obtaining contact information, providing technical assistance, and coordinating information and response, before the incident is finally resolved. Fig. 1 provides a synthesis of the incident management process as described by ISO/IEC and NIST. As can be seen from the figure, the main recommendations are similar. The ISO/IEC 27035 standard stands out as the most recognised, as it is developed by international consensus by experts worldwide. We therefore explain the recommendations in the ISO/IEC 27035 standard in more detail in the following.

ISO/IEC 27035 divides the incident management process into five phases: 1) plan and prepare; 2) detection and reporting; 3) assessment and decision; 4) responses; and 5) lessons learnt. The standard lists the following key activities that organisations should do in order to *plan and prepare* for incidents:

- Produce information security incident management policy and gain senior management commitment to that policy
- Update information security and risk management policies, so that they include incident management
- Define and document a detailed incident management scheme, including a classification scale used to grade incidents, information security incident forms, procedures and actions to use the forms, and operating procedures for the Information Security Incident Response Team (ISIRT)
- Establish an ISIRT
- Establish and preserve relationships and connections with appropriate internal and external organisations
- Establish, implement and operate technical and other support mechanisms[10], and document responsibilities and operating procedures for the operations support team
- Design and develop an awareness and training program
- Test the information security incident management scheme

For the *detection and reporting* phase, ISO/IEC 27035 includes activities that aim for detection of security vulnerabilities and events, collection of information on the events and vulnerabilities detected, and reporting on the events and vulnerabilities. Detection, collection of information, and reporting, may happen manually or automatically. The standard specifically mentions:

- Alerts from security monitoring systems such as Intrusion Detection Systems (IDS) or Intrusion Detection and

[10] This includes audit mechanisms, vulnerability management, technology watch, intrusion detection systems (IDSs), network security devices, protection means and monitoring tools, anti-malicious code software, audit log records and log monitoring software.

Table 1 – Overview of included papers.

Paper	Type of organisation studied	Incident management aspects covered	Data collection method
Ahmad et al. (2012)	Financial institution (FinanceOrg)	Main emphasis on the learning phase, although other phases are covered as well	Interviews (2 incident responders, and 2 that should be informed about incidents) and document study
Cadavieco et al. (2012)	University (University of Oviedo)	Types of incidents experienced	Document study (study of incident reports – 3 years)
Cusick and Ma (2010)	International publisher and digital information services provider (Wolters Kluwer)	All phases. Cover experiences after 18 months of running ITIL incident response.	Experience report
Hove and Tårnes (2013)	Three large Norwegian companies (one government owned, one non-commercial, one IT service provider)	All phases	Interviews (5 in total – IT security manager from all companies, supply chain manager, department manager), document study and survey ($n = 41$, participants from all three companies)
Ismail et al. (2011)	Organisations in Malaysia	Forensics	Survey (Malaysian forensic experts ($n = 2$), and desktop support specialists and project managers ($n = 2$ – in addition 5 more reported that they were not qualified to answer the questionnaire))
Jaatun et al. (2009, 2008)	Norwegian petroleum industry	All phases, but emphasis on planning and learning activities	Interviews (9, and some additional interviews at a selected offshore installation), document studies, workshops (5+)
Johnston and Reust (2006)	Not specified	Initial response and its impact on forensic examination	Not specified. Studied the response to an incident that compromised over 50 computers, some with personal data
Koivunen (2010)	National CSIRT (CERT-FI)	Reporting	Documentation study (6 incidents)
Kurowski and Frings (2011)	Two large organisations	Documentation needs and systems	Electronic survey ($n = 20$ – IT security managers)
Line (2013)	Norwegian power industry (6 Distribution System Operators (DSOs)	All phases	Interviews (19 – Head of ICT, Head of ICT security, Head of control room/power automation system)
Metzger et al. (2011)	Academic CSIRT (Leibniz Supercomputing Centre (LRZ) which operates the Munich Scientific Network)	All phases	Experience report
Möller (2007)	Academic CSIRT for Grid environments (DFN-CERT)	Setting up a CSIRT	Experience report
de Souza et al. (2011)	Large scale IT service delivery organisations	Information needs	Electronic survey ($n > 200$ – system administrators working on incident management)
Werlinger et al. (2008)	Large academic institution	Challenges of deploying and maintaining an IDS	Interviews (9 security practitioners) and participatory observation
Werlinger et al. (2010)	Organisations (9) from several sectors	Practices related to diagnostic works during incident response	Interviews (16, security manager/specialist/practitioner))

Prevention systems (IDP), antivirus software, honeypots, log monitoring systems, security information management systems and correlation engines

- Alerts from network monitoring systems such as firewalls, network flow analysis, and web filtering
- Analysis of log information from various systems and devices
- User reports, notifications from the help desk, and external notifications from third parties

After detection, information on the event should be collected. All activities in this phase should be documented, any electronic evidence should be gathered and stored securely and the incident should be registered in an Incident

Tracking System, with time and date for detection, observations, and contact information (optional). Any change control regimes should be maintained, keeping relevant databases up to date. Incidents may be escalated[11] at this stage.

In the *assessment and decision* phase, the information on security events is assessed and it is decided whether or not it is an information security incident. The standard suggests that the Point of Contact (PoC) performs an assessment to determine whether it is a false alarm or an incident. Then the ISIRT conducts an assessment to confirm the PoC's assessment and to decide on how the incident should be dealt with, who should do it, and with what priority. To support the assessment and the decision made, organisations should have agreed on a classification scale for incidents, based on impact on affected assets and systems. Then next steps involve distributing responsibility for the different activities and providing formal procedures for each notified person to follow. Documentation is important. All activities should be logged, and the standard lists activities on using guidelines for documentation, and for updating relevant databases. Incidents may be escalated if necessary for further assessments or decisions.

In the *responses* phase the incident is dealt with as planned in the assessment and decision phase. As for the previous phases, logging of actions and documentation is important. Key activities from ISO/IEC 27035 that are specific for this phase are:

- Determine if the incident is under control
- Assign internal resources and identify external resources
- Conduct forensic analysis, if required
- Communicating with internal and external people or organisations

Incidents may be escalated, and the incident rating may be changed as more information is available. When the incident has been successfully dealt with, the incident should be formally closed. This phase does not only include immediate actions, such as cutting off or shutting down systems or networks, but also later responses as restoring the system and preventing similar incidents from happening again.

The *lessons learnt* phase happens after an incident has been resolved. Several activities may be performed at this stage, and the ISO/IEC 27035 standard particularly mentions:

- Performing further forensic analysis, if required
- Identifying lessons learnt
- Reviewing, updating and improving the implementation of security controls, the security incident management policy, and the organisations' existing risk assessment results
- Reviewing the effectiveness of the response process and procedures, as well as the reporting format and the organisational structure
- Updating incident and vulnerability databases
- Sharing review results within a trusted community

As Fig. 1 shows, the activity "Using collected incident data over time" is suggested by NIST only, and not by ISO/IEC. This activity means recording metrics related to each incident, to keep track of the number of incidents being handled, the time spent per incident, and objective and subjective assessments of the incidents. The ISO/IEC states that experiences from the incident should be used for improvements, but puts the focus on subjective assessments and does not specifically suggest the use of metrics.[12]

4. Reported experiences in the literature

The first Scopus search returned 263 papers, and the second Scopus search (covering 2012 and 2013) returned 47 papers. 146 and 27 papers, respectively, were excluded based on title only, then another 92 and 7 were excluded based on title and abstract. Most of these were considered irrelevant because they proposed models, methods or tools, but did not report on real-world experiences. Some papers were excluded because they covered information security work in general (protect the system), and not what to do in case of a breach. Some were excluded because they were concerned with incident management in other areas, not specifically related to information security. However, papers that reported on experiences on incident management related to ICT in general (not only security incidents) were included if they considered security incidents.

From the two searches, 25 and 13 papers were identified as potentially relevant for this literature study. After a closer examination of the papers a total of 14 papers were included. One paper from IMF 2013 and a student thesis from a local university were included as well. An overview of all included papers can be found in Table 1. As can be seen from the table, the included papers differ in scope and focus. They cover different aspects of incident management, consider a variety of organisation types, and the data collection methods vary. As a result of these differences, it is not possible to compare the studies to say which practices are more common or which are lacking. Instead, the studies together provide broad insight to how information security incident management can be practised, and identify experiences.

In the following we summarise findings from these studies and experience reports according to the phases of ISO/IEC 27035, together with findings related to collaboration and communication in incident management. We note that not all the identified practices are easy to implement, as we discuss further in Section 5.3. In the following summaries of practices for each phase, we mark practices that many find difficult to implement with an asterix (*).

4.1. *Plan and prepare phase*

Jaatun et al. (2009) studied the petroleum industry and identified the need for a short and common plan for incident response. A finding from that study was that there were often

[11] Escalation may imply that more actors are involved and that the organisation decides to use more resources to handle the incident than what is usually done for other incidents.

[12] It should however be noted that ISO/IEC in other standards recommends the use of metrics and provides a separate standard on how to use and implement information security metrics.

several plans that impacted incident response, and that the current approach could appear scattered and randomly structured. The three Norwegian companies studied by Hove and Tårnes (2013) all had incident management plans in some form. This included plans and guidelines for handling (specific types of) security incidents, established routines, incident management handbooks for the incident response team, and plans for communication during incidents. Contingency plans could also cover major IT incidents. One of the companies had identified a lack of an established check-list to use during incident response. In the power industry (Line, 2013) plans for incident management were not widely established.

One of the main recommendations based on the experiences at LRZ-CSIRT (Metzger et al., 2011) is the establishment of a security incident response process. This implies specifying roles, responsibilities and tasks related to incident response. At LRZ-CSIRT, incident response is divided into six phases: classification, escalation, analysis, diagnosis, solution, and closing. The phases have been documented in different formats, with a short summary for administrators and service managers, a detailed description of the process (more than 20 pages) for the CSIRT team, as well as a five-page checklist that summarises the important steps. The short summary contains contact details, the most important data to be reported, and a few best practice recommendations, while the detailed descriptions contain descriptions of responsibilities, tasks, and the detailed workflows, and provide links to other documents and workflow descriptions. Solters Kluwer (Cusick and Ma, 2010) used a response script with nine basic steps. In their experience, having a simple response script was useful, as it could be quickly explained and followed without difficulty. However, the script offered limited assistance on the technical aspects.

Experiences from LRZ-CSIRT result in the recommendation that organisations clearly define what a security incident is, so that a security incident is distinguished from other issues such as system misbehaviour due to configuration errors. Ahmad et al. (2012) and Hove and Tårnes (2013) found that the definition of impact ratings was important, as this determined how incidents were handled.

Note that although plans and processes are important as a basis, some organisations consider experienced incident handlers to be of much more value during an emergency situation (Hove and Tårnes, 2013). Frequent training, including courses, table top exercises, and more realistic exercises, makes the organisation better prepared for unexpected incidents, as it is impossible to plan for all eventualities. Ownership to the routines is important, if they are to be useful. Hence, one IT manager considers the construction of a holistic plan to be the most challenging part of incident management (Hove and Tårnes, 2013).

Incident handling may include a number of different roles, e.g. system administrators and users, network administrators, the public relations department, management, and law enforcement authorities (Metzger et al., 2011). Defining responsibilities is thus important. This is particularly important in cases where IT has been outsourced (Hove and Tårnes, 2013). At LRZ-CSIRT a Security Incident Coordinator (SIC) is selected on a case-by-case basis and is granted extended decision-making power. The SIC is then responsible and can coordinate the whole process (Metzger et al., 2011). In FinanceOrg (Ahmad et al., 2012), the response to high-impact incidents is coordinated by a High-impact Incident Response Coordination Team, while other incidents are handled by a Network Incident Response Team more independently. Two of the companies surveyed by Hove and Tårnes (2013) construct teams based on the incident, and one of them has a specific team that is involved for major incidents. None of the distribution system operators (DSOs) surveyed by Line (2013) had established their own CSIRT within the organisation.

The studies and experience reports provide an overview of a lot of technical measures taken to prepare for incident detection and response. Both Werlinger et al. (2010) and Metzger et al. (2011) explain the importance of proper tools for monitoring, and also the need for centralised tools that can integrate input from several monitoring tools to gain a proper overview of the situation. Incident response teams often perform proactive activities (Ahmad et al., 2012; Hove and Tårnes, 2013; Metzger et al., 2011; Werlinger et al., 2010) like vulnerability assessments and penetration testing, and these also require the use of tools. As stressed by Werlinger et al. (2010), proper use of such tools often requires very specific knowledge about the network and the type of traffic to expect. This is rarely documented, and is thus difficult to obtain. Furthermore, they found that security practitioners tend to combine tools in unique ways to maximise their utility, and, due to usability and budget constraints, practitioners quite often created their own tools in form of shell scripts.

Metzger et al. (2011) explain their success with automating part of the incident response process, something that has made it possible to achieve adequate response in spite of limited personnel, and also outside normal business hours. As of now, more than 85 percent of all incidents are (at least partially) automatically processed. One of the reasons why this is possible is their definitions of Standard Security Incidents. These are specific types of security-related incidents that occur frequently and that are considered to be of low risk. As a consequence they allow certain simplifications of the process, compared to other incidents.

"Awareness training and official statements of the management" is mentioned by Metzger et al. (2011) as important in building a culture where incidents are reported. The study by Ahmad et al. (2012) identified a positive reporting culture at FinanceOrg where those who reported incidents were not punished, something that was an advantage for incident management. This was also the case for the power companies surveyed by Line (2013). One of the recommendations from Metzger et al. (2011) is that possible reporting ways have to be defined and each user has to be aware of these ways. At LRZ-CSIRT they used a group telephone number and a mailing list for these purposes. Möller (2007) points at the importance and challenge of making the CSIRT and its services known to its constituency, and the establishment of trust so that the CSIRT is trusted with confidential data.

In the study of the petroleum industry (Jaatun et al., 2009) it was found that individual awareness related to information security should be improved. Furthermore, scenario training, that was commonly used for HSE and other loss prevention areas, was not used for ICT incidents. The three companies studied by Hove and Tårnes (2013) perform awareness raising activities – not necessarily on a regular basis, but from time to time. They also train on incident management. The other studies did not document any general awareness raising and training activities in the organisations.

Motivations for performing training activities include increased awareness among managers, staying familiarised with routines, and having well-established roles and efficient coordination. The companies have used rehearsals to identify areas of improvement. Conducting rehearsals is however considered challenging; particularly ensuring that participants train on the right things, that the scenario is realistic and that it is useful for real situations. Training activities may include external suppliers, customers and government. In general, rehearsals are not used for low-impact incidents (Hove and Tårnes, 2013).

Summary of reported practices in the plan and prepare phase:

- Create an accessible, short plan for incident response for the entire organisation (*)
- Define what is a security incident
- Explicitly define the security response process with assigned responsibilities
- Perform incident response training
- Raise awareness (*)
- Use proper tools (*).

4.2. *Detection and reporting phase*

At LRZ-CSIRT (Metzger et al., 2011), incidents were detected in three different ways:

1. By local system and service administrators reporting incidents manually by phone or email
2. From automatic security warnings from DFN-CERT or reports from other third party services
3. Through local security monitoring mechanisms

From their experience, the manual approach was essential and the most frequently used. The compromise studied by Johnston and Reust (2006) was detected locally by system administrators that received a suspicious error message. In the studies and experience reports, most attention is however given to the local security monitoring tools in use. In the study by Werlinger et al. (2010), common detection activities identified were monitoring the organisation's IT system with various tools such as antivirus and IDS, and sending and receiving notifications. Metzger et al. (2011) report on using IDS, as well as added monitoring mechanisms in custom NAT gateways, mail monitoring mechanisms, and analysis of netflow data. All DSOs surveyed by Line (2013) have IDS/IPS, antivirus solutions, and firewalls[13] in place for their administrative ICT systems. The tools currently in use however have their limitations. The three companies surveyed by Hove and Tårnes (2013) also report on using automatic monitoring systems. This study however points to the role of users in detecting and reporting abnormal and suspicious system behaviour.

Werlinger et al. (2010) report on a lack of accuracy in tools, resulting in high false positive rates. Furthermore, usability of tools is a concern, and often there is a need to write custom tools or make adjustments to existing tools (Metzger et al., 2011; Werlinger et al., 2010, 2008). In addition, the most common tools may not be applicable or typically used for all types of systems. DSOs (Line, 2013) reported that new power automation systems might have detection systems in place, while in most cases they relied on manual detection by operators that experienced abnormalities or unexpected behaviour from the system. In some cases control room managers did not know if there were any detection systems in place or not. Some organisations (Hove and Tårnes, 2013) had outsourced the responsibility for network monitoring and detection of incidents to third parties.

Efficient detection often requires intimate knowledge about the organisation's systems and services, and due to complexity and lack of resources teams often rely on notifications to detect incidents. Notifications could come from various stakeholders, including users and other IT professionals. One of the observations by Koivunen (2010) was that, of the incidents studied, none of the victims of the security breaches seemed to have discovered the incident on their own. External reports were required to get information that an incident may have happened, or to complement the victims' limited understanding of the true scope of the incident. In each of the incident cases studied, the incident was discovered by someone with no apparent dealings with the compromised party. Intermediaries were needed in order to pass on the information, and often not all affected parties were included in the information sharing. Koivunen (2010) claims that *"victims of many internet threats are among the last ones to learn about the information security incidents affecting them"*. Some incidents are more difficult to detect. In the study by Hove and Tårnes (2013), one of the interviewees claimed that it is almost impossible to detect security incidents caused by disloyal employees.

Receiving and handling notifications were challenging in some cases. Lack of involvement from suppliers and service providers was observed in the study of the petroleum industry (Jaatun et al., 2009). Werlinger et al. (2010) found that the notifications often resulted in a need for more communication among the stakeholders. Metzger et al. (2011) experienced that some administrators did not report incidents, either because they did not know that they should or because they expected that the reporting would result in "worst-case consequences" as they were responsible for the system and therefore considered themselves fully responsible for the incident.

The case study performed by Hove and Tårnes (2013) included a survey of regular employees. In general, it was found that few of the employees knew to whom security incidents should be reported, and that they were not sure which incidents to report. Reporting channels commonly mentioned were the immediate supervisor, the local or central IT-manager, or the security manager. For all companies the IT-manager suspected underreporting of incidents. This was

[13] A firewall is not a monitoring mechanism in itself, but is a natural place to put monitoring functionality.

also supported by a quote from one of the employees: *"I have the impression that it's probably more situations that should have been reported than that are actually reported"* (Hove and Tårnes, 2013). Some studies found that security events and incidents were reported through existing help desk functions (Ahmad et al., 2012; Hove and Tårnes, 2013).

Several of the studies and experience reports explain a lot about the way incidents are registered, and it seems from the cases that current practice is that documentation begins when incidents are reported (Metzger et al., 2011). Ticketing or incident tracking systems are mentioned in several studies (Ahmad et al., 2012; Cusick and Ma, 2010; Metzger et al., 2011). In some cases, aspects of the collection and reporting process are automated (Cusick and Ma, 2010; Metzger et al., 2011). For LRZ-CSIRT (Metzger et al., 2011) standardised XML-based notifications from DFN-CERT made it possible to automatically process such alerts. Furthermore, the use of a central system for collection, correlation, and analysis of all data related to security incidents was recommended.

Even when a ticketing or incident tracking system is in place, some studies report on challenges with having all incidents registered in the system. Cusick and Ma (2010) report that some issues are observed but not logged, typically when the case is considered to be non-critical. Kurowski and Frings (2011) found that only 17% of the IT Security Managers surveyed claimed that all cases were registered in the system. As many as 50% reported that cases are received by email and telephone without being added to the ticketing system. Having complete tickets is challenging. Cusick and Ma (2010) found that engineers often only included the minimum amount of information required, i.e. just an initial description and time of resolution.

Summary of reported practices in the detection and reporting phase:

- Allow for detection through automatic tools, intra-organisational collaboration and manual reporting
- Communicate with stakeholders and suppliers (*)
- Start documentation as soon as incidents are discovered
- Document all incidents (*).

4.3. *Assessment and decision phase*

At LRZ-CERT (Metzger et al., 2011) the incident reports are supposed to include the contact details of the incident reporter, description of the identified security issues, evaluation of the sufficiency of the data and an initial classification.

Werlinger et al. (2010) found that typical activities for analysing an anomaly was to confirm, often with alternate data sources, that a compromise had actually occurred, estimating magnitude and consequences, and tracking the source of the anomaly. The diagnosis work relied on various security tools, as well as key personal skills: *"Pattern recognition, hypothesis generation, communication, bricolage (i.e. dynamic integration of security tools in novel, unanticipated ways), and tacit knowledge about their organisations and systems"* (Werlinger et al., 2010). Verification that an incident in fact has occurred may require collaboration with external organisations. Furthermore, it requires expertise and knowledge of what is normal in the system. The same way, tracking of the source of the anomaly often required specific technical expertise and knowledge of attack patterns. If it was difficult to find the source, it was considered useful to interact with other specialists that could offer novel perspectives as they were new to the investigation or had a different background. Simulations of the incident could be performed. According to the study by Kurowski and Frings (2011), the professional experience of employees is most relevant for performing analyses of incidents, followed by documentation of past incidents and help desk systems.

Koivunen (2010) points to the problem of verifying the validation of reports received from externals. It eases the process if there is already a trust relationship between the reporter and the organisation (such as the one that exists between CERT-FI and F-Secure). However, his study identified a considerable demand for the incident discoverers to retain their anonymity, and it was the experience of CERT-FI that the ultimate recipients of these reports were best being kept secret from the reporters. As a result, reports from incident-reporting clearing houses had an important role in three of the six incidents studied.

Classification of incidents is central in several of the cases described, although the approach may vary slightly. FinanceOrg (Ahmad et al., 2012) considers the criteria for incident rating to be sensitive, but explain that incidents are classified into two categories – low-impact and high-impact – based on their impact on the organisation. All three companies surveyed by Hove and Tårnes (2013) classify incidents based on impact/severity (typically high, medium or low). One company additionally categorises based on type of incident and the service or system affected. LRZ-CSIRT (Metzger et al., 2011) uses four priorities – low, medium, high and very high. Their classification is based on aspects such as the number of affected systems and services, whether internal or customer-operated machines are affected, which services and SLAs may be impacted, additional dependencies on other services, where the assumed attacker is located, and what type of attack has been observed. A cross-correlation with other open and resolved security incidents is also performed. SLAs and the maximum reaction time that has been negotiated with the affected customers are particularly important. In the study by Werlinger et al. (2010), some organisations explained that the potential cost of the incident was communicated to managers, who then decided whether to proceed.

The classification of an incident is important for what happens next, in particular it may impact who is involved (Ahmad et al., 2012; Hove and Tårnes, 2013). In the study by Werlinger et al. (2010), it was however identified that in some circumstances incidents that did not qualify as high-risk according to the organisation's criteria were still investigated by the security team in order to protect their systems.

Decisions on how to handle an incident can be particularly challenging when IT operations are outsourced and there are several suppliers involved. In the study by Hove and Tårnes (2013), this is pointed out both by the company that have outsourced IT operations and companies that act as suppliers. In one of the companies, incidents are normally handled by a team from one supplier, say Supplier A. In cases where the incident concerns systems from other suppliers, Supplier A is responsible for reporting the incident to them. Problems arise if none of the suppliers take responsibility for the dealing with the incident. Furthermore, assigning priorities for incidents may be a challenge in outsourcing environments, i.e. *"when a particular server is down, what does it mean for the customer?"* (de Souza et al., 2011).

Summary of reported practices in the assessment and decision phase:

- Define details to be contained in incident reports
- Confirm incidents
- Classify incidents
- Take special care in outsourcing scenarios (*).

4.4. *Responses phase*

Hove and Tårnes (2013) identified differing purposes for the response phase. One company stated that although it is important to get the systems up and running as fast as possible, it is important to make sure that the incident is properly resolved before restoring normal operations, and to determine whether the system is vulnerable to more attacks. One of the other companies, on the other side, stated that their main purpose is to find a temporary solution to the problem so that they can retain normal business operation and minimise business impact. This is important as they are evaluated by their customers based on the availability of the services they deliver.

Kurowski and Frings (2011) identified hardware and software documentation as the most important type of information for dealing with IT incidents. Second came documentation of past incidents. Ahmad et al. (2012) highlight the need for communication and cooperation in the responses phase. The organisation's incident tracking system facilitates communication between technical teams. This is important for documentation and provides a timeline of activities and a chain of evidence for incident handling. As such it is important for monitoring and logging the progress of the incident handling. For high-impact incidents, the collaboration process is characterised as "highly mature". Both technical and business staff is involved, with one conference call set up for each. In the business conference call, progress is explained in a non-technical way, to ensure that the business gets relevant and understandable information about the incident. Phone, email, and the helpdesk system are used for communication, particularly towards the technical personnel at the Network Incident Response Team.

Metzger et al. (2011) provide more insight into the types of responses a CSIRT typically performs. Immediate responses may include removal of affected systems from the network, creating backups and disk images, performing basic IT forensics, escalating the incident, and documenting all steps. The main goal in these early stages is to keep in touch with the individual that reported the incident and to find a way to restore the affected system. At the University of Oviedo, about 35% of the incidents required staff to go and study the computer involved (Cadavieco et al., 2012).

A challenge experienced by Metzger et al. (2011) is the lack of sufficient personnel with expertise in using forensic tools. Thus they do not use specific or custom-built forensic tools for this, but instead rely on general-purpose tools and mechanisms that are part of the default system configuration. Limited expertise on forensics is also reported by Ismail et al. (2011) and Hove and Tårnes (2013). Companies in some cases rely on third parties or the police for forensic investigations (Hove and Tårnes, 2013; Johnston and Reust, 2006).

For common and less severe incidents the LRZ-CSIRT response is performed in a fully automatic manner (Metzger et al., 2011), where examples of automatic actions include forwarding of information to responsible on-site administrator, suspension of the offending machine's internet access, and notification of the CSIRT team. Later responses, such as re-activation of blocked IP addresses are currently a manual task. After a solution has been implemented, the system is monitored extensively for a period of up to 14 days.

The companies studied by Hove and Tårnes (2013) are aware of potential privacy implications of response work. They explain that user-owned files are accessed in compliance with privacy legislation, and one of the companies has a central security advisor that is involved in cases concerning employees' privacy.

Summary of reported practices in the responses phase:

- Define response priorities
- Collaborate with technical and business staff
- Remain in contact with reporter of incident
- Automate where possible.

4.5. *Lessons learnt phase*

The study of the petroleum industry (Jaatun et al., 2009) showed that learning from incidents was considered important, but that organisations found it difficult in practice. Activities aimed towards learning seems however to be common in the surveys and experience reports we have identified. At LRZ-CERT (Metzger et al., 2011), reviews are performed after each major incident, as well as periodically. In one of the organisations surveyed by Werlinger et al. (2010), recent security incidents are discussed weekly. At FinanceOrg (Ahmad et al., 2012), the goal is to review each high-impact incident within 24 hours of the system services being restored, resulting in a post-incident report. There is no structured process for reviewing low-impact incidents, however the team involved still attempts to learn from such incidents and identify areas of improvements. Most DSOs surveyed by Line (2013) have routines for regular meetings or for evaluations after an incident had occurred, but still there are some DSOs that do not perform regular reporting or evaluations, neither in the team, nor with top management. All companies studied by Hove and Tårnes (2013) perform post-incident activities for major incidents. Additionally, one of the companies performs reviews of incidents where the incident handling was not considered efficient.

The motivation for performing learning activities include: keeping security practitioners updated on current threats (Werlinger et al., 2010), getting new ideas on how to resolve challenging incidents (Werlinger et al., 2010), discussing possible improvements of the incident management process and its activities (Hove and Tårnes, 2013; Metzger et al., 2011), performing trend analysis (Hove and Tårnes, 2013; Metzger et al., 2011), identifying direct causes (Ahmad et al., 2012; Hove and Tårnes, 2013), identifying security measures that can prevent future incidents (Ahmad et al., 2012; Hove and Tårnes, 2013; Metzger et al., 2011), and updating risk assessments of involved systems (Ahmad et al., 2012). At FinanceOrg (Ahmad et al., 2012) compliance requirements through Basel II and Sarbanes–Oxley require assessment and reporting of incidents.

It seems from the studies that learning activities primarily include personnel from the incident response team, although this is not always stated directly. The most detailed description of the learning process is that of the high-impact incidents at FinanceOrg. For these incidents, the review process consists of at least three meetings. The first meeting is a brainstorming meeting that involves only technical people. The same technical people later join in a second meeting where causal factors are examined and potential mitigations identified. The participants and the goals of the third meeting are not explained. The output of the incident review process is a post-incident report that contains the causal analysis, a new risk assessment of the affected system, and a list of tasks that multiple parties must complete.

Dissemination of incident information and lessons learnt seem to happen in varying extent and by different means in the organisations studied. In the study by Hove and Tårnes (2013), one of the companies receives monthly incident reports from the suppliers, and arranges monthly meetings where incidents are discussed. In addition, they have a quarterly meeting of their security board, where also information security incidents are discussed. At FinanceOrg (Ahmad et al., 2012), information on low-impact incidents is included in formal reports to management, where the focus is on technical means and statistical information. These reports therefore contain only generalised learning information. In addition, informal communication channels are used for dissemination of incident knowledge. There is however a lack of formal policies on what should be disseminated and which information channels should be used. Few of the surveys mention sharing incident information outside the organisation. The survey of the petroleum industry (Jaatun et al., 2009) identified a lack of openness about incidents and a lack of willingness to report incidents to the industry as a whole. One of the companies in Hove and Tårnes' study reports on sharing information on some specific incidents with trusted communities and partners, and points at the potential for using incidents for increased awareness. The IT-manager is quoted: *"never waste a good crisis"* (Hove and Tårnes, 2013).

Few report on a regular and successful use of metrics related to incident management. One of the exceptions is Cusick and Ma (2010), who use indicators like *Incident rates over time* and *Mean time to repair*, and have achieved a better view of where incidents are stemming from; which system domains and particular applications are involved. Werlinger et al. (2008) mention support for measuring to be one of many reasons for setting up an IDS. Their study also shows that reporting is an important feature of such a system, although it is challenging to configure the IDS adequately. Ahmad et al. (2012) found FinanceOrg to not have any follow-up procedures covering costs of incidents, and Line (2013) states that none of the companies in her study has implemented metrics, but some are able to estimate the cost of reestablishing regular operations after an incident occurred. Jaatun et al. (2009) identified the need for measuring the efficiency of the incident management process.

Several challenges are reported when it comes to learning from incidents. Inadequate involvement of suppliers is pointed out as a problem in the petroleum industry (Jaatun et al., 2009). A focus on direct causes, rather than underlying causal structures, is mentioned by Ahmad et al. (2012). They also identified a strong focus on technical information over policy and risk. For low-impact incidents in particular, a focus on solving the problem as fast as possible seems to have evolved into a dislike for "paperwork". Incidents are efficiently solved, and the team gathers a large amount of technical information in order to do this. Gathering additional data for future learning is however not considered. For high-impact incidents, there is an understanding of the importance of identifying the root causes of an incident, including organisational and human factors. However, they struggle with how learning should be done in practice. In particular, their high-impact incident management process does not respond to incident precursors,[14] identified dissemination challenges have not been addressed, and key areas such as policy and risk do not benefit from incident data.

Although learning from incidents has its challenges, the incident statistics reported by FinanceOrg should motivate more organisations to improve on this aspect. They claim that their learning process for high-impact incidents has resulted in a reduction of incidents of around 200 per month in 2002 down to only 16 at the time of the study.[15] From this we may surmise that learning from incidents has an important contribution to preventive measures, as illustrated by Jaatun et al. (2009) through the interaction with "external dynamics".

Summary of reported practices in the lessons learnt phase:

- Perform assessment and evaluation after every incident (*)
- Disseminate incident information (*)
- Use of metrics for learning effects and tuning of technical measures (*)
- Learn from incidents as a measure for reducing the number of incidents (*)

4.6. *Collaboration and communication in incident management*

Studies in the petroleum industry (Jaatun et al., 2009) revealed that the organisations usually had several plans covering different aspects of the incident management process. It was however found that suppliers were not adequately involved in planning for incidents, although the operator would in many cases depend on them during incident management. Furthermore, individual information security awareness was

[14] Defined by Ahmad et al. as "a consequence of events that have the immediate potential to cause a high-impact incident".

[15] The time of the study is not provided in the paper published in 2012.

Table 2 – Summary of findings of the surveys and experience reports related to the recommendations of ISO/IEC 27035.

Phase	ISO/IEC 27035 recommendation	Identified practice
Plan and prepare	Produce policy; define and document incident management scheme	Having a plan was recommended. When not available this was considered a weakness. (Ahmad et al., 2012; Metzger et al., 2011)
	Gain senior management commitment	Official statements of the management are seen as important for building a reporting culture (Metzger et al., 2011).
	Update security and risk management policies	–
	Establish ISIRT	Defining roles is considered important (Metzger et al., 2011). Some, but not all, organisations had established an ISIRT.
	Establish relationships with relevant organisations	Clearly defined roles are essential in cases where IT operations are outsourced (Hove and Tårnes, 2013).
	Implement technical and other support mechanisms	Technical tools are useful, but using them efficiently requires training and specific competence of the technology as well as how the organisation uses ICT (Werlinger et al., 2010; Metzger et al., 2011). Improved efficiency can be achieved through automation (Metzger et al., 2011).
	Awareness and training	Mentioned related to reporting culture (Ahmad et al., 2012; Line, 2013; Metzger et al., 2011; Hove and Tårnes, 2013). Awareness activities and training are prioritised in some of the companies (Hove and Tårnes, 2013).
	Test incident management scheme	Rehearsals are valuable for improving incident management (Hove and Tårnes, 2013) but few studies mention this.
Detection and reporting	Detection of security vulnerabilities and events (monitoring systems, user reports, external parties)	Manual reports (internal/external) are very important, although a lot of effort is put into monitoring tools (Werlinger et al., 2010; Line, 2013; Metzger et al., 2011; Koivunen, 2010; Hove and Tårnes, 2013). Identified problems are the usability of tools (Werlinger et al., 2008, 2010; Metzger et al., 2011) and the high number of false positives (Werlinger et al., 2010), reliance on tacit knowledge (Werlinger et al., 2010), and problems of receiving reports (Werlinger et al., 2010; Jaatun et al., 2009; Metzger et al., 2011; Koivunen, 2010).
	Collection of information	Use various tools. May require communication among stakeholders (Werlinger et al., 2010). Challenging in distributed organisations (Hove and Tårnes, 2013).
	Reporting and documentation	Documentation begins when incidents are reported. The use of a central system for collection, correlation, and analysis of all data is recommended (Metzger et al., 2011). Quality of documentation is a potential problem (Kurowski and Frings, 2011; Cusick and Ma, 2010).
Assessment and decision	Decide if security incident	Verification of incident may require collaboration with external organisations (Werlinger et al., 2010; Koivunen, 2010). Also requires knowledge of what is normal in the system (Werlinger et al., 2010).
	Classify incident	Classification of incidents is central in several of the cases described (Ahmad et al., 2012; Metzger et al., 2011; Hove and Tårnes, 2013).
	Decide on actions and distribute responsibilities; provide formal procedures	Classification is important for what happens next, including who is responsible (Ahmad et al., 2012; Hove and Tårnes, 2013). Distributing responsibilities can be challenging when different suppliers are involved (Hove and Tårnes, 2013).
Responses	Immediate responses: assign resources, determine if incident is under control	Main goal: keep in touch with the reporter and find a way to restore the system (Werlinger et al., 2010; Hove and Tårnes, 2013). For common and less severe incidents, response may be fully automatic (Metzger et al., 2011).
	Later responses	Monitoring of system afterwards (Werlinger et al., 2010).
	Forensic analysis, if required	A possible challenge is the lack of personnel with expertise on forensic tools (Metzger et al., 2011). Some have procedures for handling electronic evidence (Hove and Tårnes, 2013). Companies may rely on external parties for this (Hove and Tårnes, 2013; Johnston and Reust, 2006).

Table 2 – (*continued*)

Phase	ISO/IEC 27035 recommendation	Identified practice
	Communicate internally and externally	Need for communication. Use incident tracking systems, conference calls, phone, and email. May involve technical and business staff. Knowledge of who to contact is essential (Hove and Tårnes, 2013).
	Escalate, if necessary	Escalation mentioned as one of the response activities (Werlinger et al., 2010; Hove and Tårnes, 2013).
Lessons learnt	Further forensic analysis	–
	Identify lessons learnt	Incident statistics created (Ahmad et al., 2012; Hove and Tårnes, 2013); (periodic) review of incidents (Ahmad et al., 2012; Werlinger et al., 2010; Line, 2013; Metzger et al., 2011; Hove and Tårnes, 2013); informal discussions (Ahmad et al., 2012); creation of post-incident reports (Ahmad et al., 2012).
	Update relevant databases; share results with trusted community	Learning activities mainly include technical personnel, although reports may be created for management (Ahmad et al., 2012). Lack of willingness to share incident information outside the organisation (Jaatun et al., 2009). Limited sharing with external parties in specific cases (Hove and Tårnes, 2013).

not at a satisfactory level. Finally, and maybe most disturbing, the study revealed a "deep sense of mistrust" between process control engineers and ICT network administrators.

The identified issues can be interpreted as symptoms of unsatisfactory collaboration and communication when it comes to information security and incident management in particular. This is disturbing since incident management is collaborative in nature. This is exemplified by Werlinger et al. (2010), who found that:

- configuration of monitoring tools for incident response requires extensive knowledge of issues that are rarely explicitly documented and obtaining this knowledge may involve external stakeholders
- the complexity of the IT systems, and also the lack of resources for monitoring, cause incident detection to rely on notifications from various stakeholders, including end-users
- verification that there actually is an incident – not a false alarm – may require collaboration with external organisations
- managers often need to be involved in decision making.

The importance of collaboration and communication is reflected in the procedures for responding to high-impact incidents at FinanceOrg (Ahmad et al., 2012). Technical and business conference calls are set up in order to gather knowledge and communicate progress; in general, the management of the incident relies heavily on communication via teleconferencing, phone, e-mail and the helpdesk system. It is not without reason that Werlinger et al. (2010) list *communication* as one of the five key skills required for diagnosis work.

Hove and Tårnes (2013) emphasise the challenge of information collection and dissemination during the incident handling process. For organisations with distributed organisational structures there are many sources of information. Knowing how much information to share can be difficult. Too little information could lead to wrong decisions due to an erroneous overview of the situation, while too much information can be overwhelming and cause delays in decision-making. This is also supported by Ahmad et al. (2012) where an information security manager states that the sharing, or rather the finding, of information was one of the most challenging parts of her job. de Souza et al. (2011) found that people were the most important sources of information in working with complex incidents. In only 33% of the cases was the information from the incident tool sufficient.

In cases where IT operations are outsourced, collaboration during incident management is even more challenging. Even minor incidents can be problematic if all assume the incident to be someone else's responsibility. As pointed out by one supplier, *"It is also a political 'game'. Who will pay for it?"* (Hove and Tårnes, 2013). Moreover, customers and suppliers often handle different parts of the incident (Hove and Tårnes, 2013).

Jaatun et al. (2009) revealed that information security was viewed merely as a technical issue. This technical focus was also found in the study of FinanceOrg (Ahmad et al., 2012). For low-impact incidents in particular, the emphasis was on technical information, over policy and risk. For high-impact incidents there was an understanding that it was important to identify root causes that goes beyond the technical issues (e.g. gaps in the underlying processes). However, the learning process also for high-impact incidents involved only technical personnel in the first phases. Reporting from incidents was technical. Based on the low-impact incidents, several reports were produced for management. This was typically statistical information with a focus on the technical aspects. From the high-impact incidents, the reports were more detailed and a bit broader in scope, but dissemination to non-technical personnel was not performed satisfactorily. There was a lack of formal policy on how information should be disseminated. Furthermore, the silo structure of the organisation was a hindrance for effective sharing of experiences. The practice can probably be summarised by a finding by Werlinger et al. (2010), where the representative from one of the organisations studied explained that security incidents were discussed weekly so that **security practitioners** could learn about new threats and assist in solving challenging incidents.

5. Discussion

The empirical studies and the experience reports provide important insights into current practice when it comes to incident management (Research question 1 and 2). Below we discuss how the findings from the surveys and experience reports relate to the recommendations of ISO/IEC 27035 (Research question 3). We then describe some of the identified successful practises that may serve as inspiration for others, before going on to discuss particularly challenging practices and how these challenges may be addressed. Finally, based on the challenges we identify future research needs.

5.1. *Practice vs. the ISO/IEC 27035 standard*

Table 2 provides a summary of the recommended activities of ISO/IEC 27035 related to the identified practice in the surveys and experience reports. The main impression is that what the studies consider to be good practice is in line with the recommendations of the standard. However, the studies and experience reports document that several of the recommendations are not easy to perform in practice, as elaborated further in Section 5.3.

For some of the recommendations, there is no or only limited identified practice in the surveys and experience reports. Note that this does not necessarily mean that the activity is not performed, only that it is not documented in the papers.

5.2. *Inspirational examples*

The surveyed literature identifies examples of good practice that can motivate and inspire organisations to improve their own way of performing incident management.

- **It is recommended to have a simple plan:** Simple plans can be quickly explained and followed without difficulty (Cusick and Ma, 2010).
- **Using automation as a means to improve efficiency:** Automation[16] seems to be best practice for dealing with common and low-risk incidents (Metzger et al., 2011).
- **Documenting incidents provides benefits:** Documentation should start as soon as an incident is reported or detected (Metzger et al., 2011). An incident tracking system should be used (Metzger et al., 2011), and it is recommended to collect all data related to the incident into one single system (Metzger et al., 2011). Cusick and Ma (2010) reported on high benefits of starting using a tool for information sharing on incidents, where anyone with permission could request notifications in case of new events or changes. They said: *"This capability has been a boon to communications around production incidents and has even reduced the frequency of status requests by management [...] This has freed up the support team to focus on incident resolution [...] This feature alone has made our entire IRT [Incident Response Team] process worth the effort of creating, deploying, and maintaining."* (Cusick and Ma, 2010)
- **Learning from incidents is worth the effort:** FinanceOrg (Ahmad et al., 2012) has experienced a drastic reduction in incidents, something which is considered a result of the learning process that hey have implemented.
- **Metrics can provide increased understanding:** Cusick and Ma (2010) report that a positive side-effect of implementing the incident management process was that they could collect incident statistics automatically and identify Key Performance Indicators, like *incident rates over time* or *Mean Time To Repair*. They claim that this *"has been extremely useful in understanding the failure patterns, durations, and impacts"* (Cusick and Ma, 2010).

5.3. *Incident management challenges*

The studies and experience reports identify some aspects that seem particularly challenging, where additional support and concrete guidance is needed. This is not to say that more standards are called for, but rather identifies a need for more tools and domain-specific guidelines in some areas.

- **Creating plans and classifications of incidents:** Some of the organisations report on a lack of plans (Line, 2013), or the need for improved or simpler plans (Jaatun et al., 2009; Hove and Tårnes, 2013).
- **Gaining senior management commitment:** All agree that this is important, but it seems to be difficult in practice. One reason for this may be optimistic bias on part of the management, as documented by Rhee et al. (2012) – senior managers are less likely to focus on incident management if they do not perceive incidents as a problem.
- **Involving all employees:** As information security concerns everyone and current trends show that attacks are now targeting employees directly, not necessarily only the technical systems, all employees should be aware and well trained in recognising and reporting incidents (Hove and Tårnes, 2013). Current incident management standards describe training activities for incident handlers only, although other publications such as NIST SP 800-16 (Wilson et al., 2008) recommend not only security awareness, but also security basics training for all employees. Despite the focus on detection tools, manual reporting seems to be a key when it comes to detection of incidents (Hove and Tårnes, 2013; Koivunen, 2010; Line, 2013; Metzger et al., 2011; Werlinger et al., 2010). Organisations would benefit from advice on how to motivate reporting of incidents, how to make it easy to report incidents (both for internals and externals), and how to verify reports. Herath and Rao (2009) has documented that employees who have a good understanding of threats demonstrate better compliance with security policies, and it is reasonable to extend this to expecting that higher awareness will contribute to better manual reporting.

[16] Note, however, that this requires some mechanism to classify incidents as either high-risk or low-risk, which in turn is prone to false positives and false negatives.

- **Coping with the existing tools and their lack of usability:** A lot of the studies mention a high number of technical tools that are used for incident detection and response. Although highly useful, they generally seem to suffer from a lack of usability, a high number of false positives, and a need for very precise and rarely documented information (Metzger et al., 2011; Werlinger et al., 2010, 2008).
- **Quality of incident registrations:** Although organisations have incident tracking systems in place, incidents may still not be registered. This is a problem for low-impact incidents in particular (Cusick and Ma, 2010; Kurowski and Frings, 2011). Moreover, the quality of the registrations may be a problem, as technicians may only register the absolute minimum of information required (Cusick and Ma, 2010).
- **Collaboration among teams and across disciplines:** It seems that collaboration within the team works satisfactorily, but that communication with externals and also collaboration including both technical and business staff are more challenging (Ahmad et al., 2012; Hove and Tårnes, 2013; Werlinger et al., 2010). The impression is that response and learning activities mainly include technical staff. Still, the business units affected and management have an important role to play – particularly for severe incidents.
- **Practising incident management in outsourcing scenarios:** In cases were IT is outsourced, definition of clear responsibilities is highly important. Problems arise if a supplier does not want to take responsibility for dealing with an incident. Even minor incidents can cause problems if all assume someone else has the responsibility for dealing with the issue (Hove and Tårnes, 2013).
- **Motivating learning activities:** Organisations seem to agree that learning from incidents is important. It is however considered difficult by some (Jaatun et al., 2009). Learning from low-impact incidents also seems not to be prioritised (Ahmad et al., 2012; Hove and Tårnes, 2013). It has been claimed that *"most breaches do not happen immediately, but take place over time"* (Scholl and Mangold, 2011). Thus, by detecting initial or early events, it is possible to prevent incidents. For the same reason, learning from low-impact incidents and security events should not be omitted (Ahmad et al., 2012).
- **Sharing lessons learnt:** It seems that lessons learnt and other incident information is often available only to some selected few, although there may be several other individuals or departments in the organisation that would benefit from such information (Ahmad et al., 2012).

5.4. *Approaches to addressing the challenges*

Although current standards and guidelines for information security incident management provide good recommendations for companies, the identified challenges when it comes to implementing the recommendations of ISO/IEC 27035 point to a need for additional guidance. This guidance would in many cases need to be more concrete than what is expected from standards, and should rather be directed towards specific industries or specific types of organisations and take the form of examples and more concrete advice. Examples of additional guidance that may be needed are:

- Templates and examples of incident management plans
- Examples of successful approaches and practical advice when it comes to gaining senior management commitment
- Inspiration for campaigns directed towards training of employees in recognising and reporting incidents
- Examples of successful approaches to receive and verify manual incident reports
- Introduction to common tools used for incident detection and response, and an overview of their pros and cons
- Examples of successful approaches to increasing motivation for incident documentation among incident responders
- Recommendations on which roles should somehow be involved in incident management, and the benefits of including them
- Practical advice on dealing with the challenges of incident management in outsourcing scenarios
- Motivational examples, as well as practical advice, on how learning activities could be extended to include non-technical staff

In addition there is clearly a need for improved tools for incident management. Tools that are used for incident detection and response need better usability and must produce fewer false positives. This has also been pointed out for system administrator tools in general (Barrett et al., 2004).

5.5. *Research needs in incident management*

Of the 15 papers included in this study, four are experience reports. This leaves 11 studies. Several of these studies have limitations when it comes to academic rigour. In particular, this applies to some of the surveys, like one of the included papers that only had two respondents per questionnaire (Ismail et al., 2011). Interviews seem to be the preferred data collection method, as more than half of the resulting papers are interview studies. The challenge of performing empirical research on information security in organisations is however discussed by Kotulic and Clark (2004). They claim that there will usually be a general mistrust to any outsider who wants to obtain data on internal information security issues. To cope with this they suggest that such research studies focus on a few selected organisations, where trust can be mutually built between the researcher(s) and the involved employees/departments. They point out that some information collection strategies might be better suited than others for such confidential data, and that one of the factors for successful studies is that the organisation(s) studied is allowed to be involved in discussing and approving the results. This can explain the wide use of interviews as collection method among our identified studies, as the interviewees feel a certain control of the situation and misunderstandings may be solved right away (Robson, 2011).

Based on the material we have identified, we claim that there is a need for more empirical studies in this field. The material contains a few case studies that go deep into how information security incident management is performed in one or a few organisations. The study of Ahmad et al. (2012) is a good example in this respect. These types of studies are highly useful in increasing the understanding of what works well and what is challenging, as well as understanding the rationale behind current practice. However, in order to know more about how a wider variety of organisations practice incident response, more such studies are needed. It would be useful with more longitudinal studies and the use of additional data collection methods such as observations. The material contains a few studies that collect responses from a higher number of organisations. These provide broader perspectives. The best examples of this type of study in the material are however either not specifically considering information security incidents (de Souza et al., 2011) or are not specific enough on the context of the organisations (Werlinger et al., 2010). Because of this, it is not fully clear how the results can be reasonably transferred to information security incident management in other organisations. Thus more studies of this type are needed to improve understanding of important aspects of information security incident management.

In general, the studies show a limited use of theory to frame their research and findings. Ahmad et al. (2012) use organisational learning theories to explain the findings; as do Jaatun et al. (2009). Findings are to some extent related to previous findings in other studies (Ahmad et al., 2012; Werlinger et al., 2010, 2008; de Souza et al., 2011). Future studies should to a larger extent compare their findings to other studies in the field and use theories to shed light on the findings. Studies could also seek to evaluate the relevance of established theories from related domains.

Based on the above-mentioned challenges and the inspirational examples, a number of distinct research needs in this space can be identified.

- **Better tools:** There is a need for tool development and evaluation of the developed tools in order to assess whether or not the tools provide improved usability and accuracy. In addition, research should delve into the underlying question of why do the tools suffer from low usability and what can be done to improve development of such tools in general.
- **Tacit knowledge:** There is a need for a better understanding of the role of tacit knowledge and implementation and evaluation of strategies for dealing with the current dependence on tacit knowledge.
- **Identifying root causes:** Current learning activities are focused on technical aspects and identification of direct causes, but the root cause may well lie in policies, procedures, lack of competence, or other underlying aspects (Ahmad et al., 2012). To increase the learning outcome from incidents, organisations should receive more support for learning activities so that they are able to include relevant types of personnel in the analysis and ask questions that will help reveal underlying causes. In this respect, it is necessary with improved understanding of learning processes for incident management. Research in this field should take relevant theory into account.
- **Outsourcing:** There is a need for improved understanding of the challenges of incident response in outsourcing scenarios in order to identify strategies that are successful. This particularly concerns cases where several suppliers are serving the same customer.
- **Metrics:** Metrics seem to be used to a very limited extent when it comes to incident management, although organisations report on benefits from performing measurements on incidents. Research is needed in order to identify useful metrics and investigate how they can be meaningfully applied in different organisational environments.
- **Obstacles to improvement:** The lack of plans regarding information security incident management in some organisations points to the need to study which policies, organisational dynamics, and economic incentives prevent significant improvements in incident management and limit the adoption of guidelines.

6. Summary and conclusions

We have summarised recommendations for incident management documented in standards documents and have provided an overview of documented experiences in literature. We argue that the ISO/IEC 27035 standard is a good starting point for organisations when it comes to incident management. Implementing this standard, with all its recommendations and activities, is however not straightforward. While there are several inspirational success stories, the studied practices and experiences documented in literature have led to identification of challenging aspects that should be given particular attention when developing additional support in form of guidelines, best practice descriptions or tools. We have identified areas of further research on information security incident management, and find that in addition to specific research needs for tools and mechanisms, there is a need for more empirical research to answer the fundamental question of why the challenges remain, and how they can be resolved.

Acknowledgement

This work has been supported by the Research Council of Norway (201557) through the IMMER project – Information Security Incident Management and Emergency Preparedness in ICT-based operations. The IMMER project is managed by Intra Point. The authors are grateful to the anonymous reviewers whose insightful comments helped to significantly improve the paper.

REFERENCES

Ahmad A, Hadgkiss J, Ruighaver AB. Incident response teams – challenges in supporting the organisational security function. Comput Secur 2012;31(5):643–52.

Anderson R, Barton C, Böhme R, Clayton R, Eeten M, Levi M, et al. Measuring the cost of cybercrime. In: 11th Workshop on the Economics of Information Security (WEIS'12); 2012.

Barrett R, Kandogan E, Maglio PP, Haber EM, Takayama LA, Prabaker M. Field studies of computer system administrators: analysis of system management tools and practices. In:

Proceedings of the 2004 ACM conference on Computer supported cooperative work (CSCW '04). New York, NY, USA: ACM; 2004. pp. 388–95. http://doi.acm.org/10.1145/1031607.1031672.

Brewster E, Griffiths R, Lawes A, Sansbury J. IT service management: a guide for ITIL foundation exam candidates. 2nd ed. BCS, The Chartered Institute for IT; 2012.

Cadavieco JF, Pérez CR, Fernández CB. Information technology incident management: a case study of the University of Oviedo and the Faculty of Teacher Training and Education. Univ Knowl Soc J (RUSC) 2012;9(2):280–95.

Cichonski P, Millar T, Grance T, Scarfone K. NIST SP 800-861: Computer security incident handling guide. National Institute of Standards and Technology; 2008.

Cusick J, Ma G. Creating an ITIL inspired incident management approach: roots, response, and results. In: Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP; 2010. pp. 142–8. http://dx.doi.org/10.1109/NOMSW.2010.5486589.

de Souza CRB, Pinhanez CS, Cavalcante VF. Information needs of system administrators in information technology service factories. In: Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT '11). New York, NY, USA: ACM; 2011. p. 10. http://doi.acm.org/10.1145/2076444.2076447.

ENISA. Good practice guide for incident management; 2010.

Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 2009;18(2):106–25. http://dx.doi.org/10.1057/ejis.2009.6.

Hove C, Tårnes M. Information security incident management: an empirical study of current practice. Norwegian University of Science and Technology; 2013.

Ismail S, Ahmad A, Shukran MAM. New method of forensic computing in a small organization. Aust J Basic Appl Sci 2011;5(9):2019–25.

ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management; 2011.

Jaatun MG, Albrechtsen E, Line M, Johnsen SO, Wærø I, Longva OH, et al. A study of information security practice in a critical infrastructure application. In: Rong C, Jaatun MG, Sandnes FE, Yang LT, Ma J, editors. Autonomic and Trusted Computing. Lecture Notes in Computer Science, vol. 5060. Springer Berlin Heidelberg; 2008. pp. 527–39. http://dx.doi.org/10.1007/978-3-540-69295-9_42.

Jaatun MG, Albrechtsen E, Line MB, Tøndel IA, Longva OH. A framework for incident response management in the petroleum industry. Int J Crit Infrastruct Prot 2009;2:26–37.

Johnston A, Reust J. Network intrusion investigation preparation and challenges. Digit Investig 2006;3(3):118–26. http://dx.doi.org/10.1016/j.diin.2006.08.001. http://www.sciencedirect.com/science/article/pii/S1742287606000922.

Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering; 2007 [EBSE Technical Report].

Koivunen E. Why wasn't I notified: information security incident reporting demystified. In: 15th Nordic Conference in Secure IT Systems (NordSec 2010); 2010.

Kotulic AG, Clark JG. Why there aren't more information security research studies. Inf Manag 2004;41(5):597–607. http://dx.doi.org/10.1016/j.im.2003.08.001. http://www.sciencedirect.com/science/article/pii/S0378720603000995.

Kral P. The incident handlers handbook [Technical Report]. SANS Institute; 2011.

Kurowski S, Frings S. Computational documentation of IT incidents as support for forensic operations. In: IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on; 2011. pp. 37–47. http://dx.doi.org/10.1109/IMF.2011.18.

Line MB. A case study: preparing for the smart grids – identifying current practice for information security incident management in the power industry. In: Seventh International Conference on IT Security Incident Management and IT Forensics (IMF); 2013.

Metzger S, Hommel W, Reiser H. Integrated security incident management – concepts and real-world experiences. In: Sixth International Conference on IT Security Incident Management and IT Forensics (IMF); 2011. pp. 107–21.

Möller K. Setting up a GRID-CERT, Experiences of an academic CSIRT. Campus Wide Inf Syst 2007;24(4):260–70.

Rhee HS, Ryu YU, Kim CT. Unrealistic optimism on information security management. Comput Secur 2012;31(2):221–32. http://dx.doi.org/10.1016/j.cose.2011.12.001. http://www.sciencedirect.com/science/article/pii/S0167404811001441.

Robson C. Real world research. 3rd ed. John Wiley & Sons Ltd.; 2011.

Scholl F, Mangold M. Proactive incident response. Inf Syst Secur Assoc J 2011;9(2). http://www.issa.org/?page=JournalFebruary2011.

Werlinger R, Hawkey K, Muldner K, Jaferian P, Beznosov K. The challenges of using an intrusion detection system: is it worth the effort?. In: Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08). New York, NY, USA: ACM; 2008. pp. 107–18. http://doi.acm.org/10.1145/1408664.1408679.

Werlinger R, Muldner K, Hawkey K, Beznosov K. Preparation, detection, and analysis: the diagnostic work of IT security incident response. Inf Manag Comput Secur 2010;18(1):26–42.

West-Brown MJ, Stikvoort D, Kossakowski KP, Killcrece G, Ruefle R, Zajicek M. Handbook for Computer Security Incident Response Teams (CSIRTs); 2003.

Wilson M, de Zafra DE, Pitcher SI, Tressler JD, Ippolito JB. NIST SP 800-816: Information technology security training requirements: a role- and performance-based model. National Institute of Standards and Technology; 2008.

Inger Anne Tøndel is a Research Scientist at SINTEF ICT in Trondheim, where she is the research manager of the information security research group. She has a MSc in Telematics from the Norwegian University of Science and Technology from 2004. Her research interests include incident management, risk management, privacy by design, and security requirements engineering.

Maria B. Line holds a MSc from the Norwegian University of Science and Technology, Dept. of Telematics, 2002. Since then Line has been a Research Scientist at SINTEF in Trondheim. Line is currently a PhD candidate at the NTNU, Dept. of Telematics. She is studying information security incident management in the power industry, specifically targeting the challenges that come with the smartgrids. Her scientific interests include incident management, privacy, security awareness and risk assessments.

Martin Gilje Jaatun is a Senior Scientist at SINTEF ICT, where he has been employed since 2004. He received his MSc degree in Telematics from the Norwegian Institute of Technology (NTH) in 1992. Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include security in cloud computing and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org) and a Senior Member of the IEEE.

NTNU

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Telematics

To whom it may concern,

Statement of authorship on joint publication to be used in Maria B. Line's PhD thesis

(Cf. NTNU PhD regulations § 7.4, section 4 and dr.philos regulations § 3, section 5)

This statement regards the following joint publication:

> Tøndel, I. A., Line, M. B., Jaatun, M. G.: *Information security incident management: Current practice as reported in the literature*, Computers & Security vol. 45, ISSN 0167-4048, p. 42-57, 2014.

Maria B. Line was involved in the literature search and data analysis. Furthermore, she contributed to writing up findings and the discussion in this publication.

I hereby confirm that the doctoral candidate's contribution is correctly identified above, and I consent to Maria B. Line including it in her PhD thesis.

Trondheim, 16.09.2014

Inger Anne Tøndel

Inger Anne Tøndel

Martin Gilje Jaatun

PAPER 4

Examining the suitability of industrial safety management approaches for information security incident management

Maria B. Line and Eirik Albrechtsen

Forthcoming in International Journal of Information and Computer Security. ISSN 2056-4961.

©Emerald Group Publishing. Reprinted with permission. Emerald does not grant permission for this article to be further copied/distributed or hosted elsewhere without the express permission from Emerald Group Publishing Limited.

Is not included due to copyright

PAPER 5

A Study of Resilience within Information Security in the Power Industry

Maria B. Line

IEEE Africon 2013, Mauritius.
ISSN 2153-0025. DOI: 10.1109/AFRCON.2013.6757799

©2013 IEEE. Reprinted with permission.

Is not included due to copyright

PAPER 6

Information security incident management: Planning for failure

Maria B. Line, Inger Anne Tøndel, and Martin G. Jaatun

8th International Conference on IT Security Incident Management and IT Forensics (IMF) 2014, Münster, Germany.
ISBN 978-1-4799-4330-2. DOI: 10.1109/IMF.2014.10

©2014 IEEE. Reprinted with permission.

Information security incident management: Planning for failure

Maria B. Line*†, Inger Anne Tøndel† and Martin G. Jaatun†

*Department of Telematics
Norwegian University of Science and Technology (NTNU)
N-7491 Trondheim, Norway
maria.b.line@item.ntnu.no

†SINTEF ICT
N-7465 Trondheim, Norway
{inger.a.tondel, martin.g.jaatun}@sintef.no

Abstract

This paper reports on an interview study on information security incident management that has been conducted in organizations operating industrial control systems that are highly dependent on conventional IT systems. Six distribution service operators from the power industry have participated in the study. We have investigated current practice regarding planning and preparation activities for incident management, and identified similarities and differences between the two traditions of conventional IT systems and industrial control systems. The findings show that there are differences between the IT and ICS disciplines in how they perceive an information security incident and how they plan and prepare for responding to such. The completeness of documented plans and procedures for incident management varies. Where documentation exists, this is in general not well-established throughout the organization. Training exercises with specific focus on information security are rarely performed. There is a need to create a more unified approach to information security incident management in order for the power industry to be sufficiently prepared to meet the challenges posed by Smart Grids in the near future.

Index Terms

Industrial control systems, Information security, Information technology, Incident management, Power industry, Smart grids

I. Introduction

Information technology (IT)[1] is permeating all levels of industrial control systems (ICS)[2]. The two traditions of IT and ICS differ in several aspects, like terminology, security culture, security requirements, and technologies used [1]. As an example, if a computer is infected by malware, the most common response is to disconnect the computer from the network and reinstall it. The priority is on removing the malware, sacrificing the availability of the computer. In an ICS, availability is the top priority. Shutting down a component may have a significant economic cost.

Industrial control systems (ICS) are frequently used for controlling physical objects, such as oil installations, railway signalling systems, or power production systems. An ICS is often safety-critical, as a malfunctioning ICS may have severe consequences for the physical environment [2]. In the near future, if not already, ICS will consist mainly of ”regular” IT components. The two traditions of IT and ICS will then need to collaborate in order to ensure continuous operation of the systems and uninterrupted power supply. The information security incident management process should therefore be integrated with safety procedures and procedures for responding to industrial accidents at the installation.

An information security incident management process consists of different phases; preparations, responding to an incident, and post-incident evaluations and improvements [3]. Benefits of a structured approach to infomation security incident management include [3] an overall improvement of information security, reduced impact of incidents, improved focus and better prioritization of security acticities, and better and more updated information security risk assessment efforts.

We have performed a study to investigate how information security incident management is performed in organizations operating industrial control systems, more specifically in distribution system operators (DSOs) in the power industry[3]. DSOs own and manage the power distribution grid[4]. They are selected as the domain of study due to the advent of the Smart Grid, which causes the integration of IT and ICS to take several steps further [1]. For consumers, the most obvious aspect of the Smart

[1] in many contexts also referred to as Information and Communication Technology (ICT)

[2] Several terms are used interchangably to denote such systems: industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA), process control systems, automation systems. Throughout this paper the term *control systems* and/or *ICS* will be used.

[3] This work is funded partially by the Norwegian Research Council through the *DeVID* project, grant no 217528, and partially by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*

[4] The distribution grid is low voltage part of the power grid, the part that transports power into every single household and power consumer.

978-1-4799-4328-9/14 $31.00 © 2014 IEEE
DOI 10.1109/IMF.2014.10

Grid is the introduction of smart meters, but the DSOs are faced with many other IT challenges that include and go beyond the Advanced Metering Infrastructure (AMI). The increased reliance on conventional IT systems in this sector represents a paradigm shift in that personnel who have traditionally focused on safety aspects of power electronics, and ensuring sufficient delivery of electricity to consumers, now also have to worry about information security of their newly internet-enabled control systems.

The following research questions were defined for this part of our study:

- How are planning and preparatory activities for information security incident management performed by organizations depending on successful cooperation between IT systems and ICS?
- What differences can be found in how the planning and preparatory activities are performed for IT systems compared to ICS?

Identifying the practices both for the IT systems and the control systems is valuable to see which practices should be strengthened and further developed in a collaboration. People working with these systems have different experiences and competence, and it would be reasonable to think that there should be synergy effects by achieving increased cooperation.

Preliminary results from this study were presented by Line [4]. This paper is more comprehensive in all sections compared to the previous conference paper; a larger number of empirical studies are referred to as background, and the method is described in more detail, especially the industrial case context. The preliminary results were written up before a thorough analysis was performed. This analysis now forms the basis for the Findings and Discussion sections in this paper. However, the findings presented are related to the planning and preparation activities only, as opposed to the preliminary results, which covered all phases as described in ISO 27035. In this paper, a discussion of the findings and potential threats to validity is included as well.

The paper is organized as follows. Section II presents the background for our study; standards, guidelines, and related work. The research method is described in Section III. Findings from the interviews are summarized in Section IV and discussed in Section V. Section VI provides some concluding remarks and suggests further work.

II. Background

In the following we provide an overview of important standards and guidelines for incident management in this context, as well as an overview of relevant experiences documented in literature. Based on this, we outline our expectations before the interviews.

A. Recommendations in standards and guidelines

The information security incident management process covers the complete lifecycle of an incident. ISO/IEC [3] describes this process as consisting of five phases, as illustrated in Figure 1. The Plan and prepare phase runs continuously, while the next four phases are triggered by the occurrence of an incident. Other guidelines which describe the incident management process quite similarly exist as well; although the number of phases may vary, the main ideas and activities included during the lifecycle generally resemble the ISO/IEC standard. NIST [5], ENISA [6], and SANS [7] are among the providers of the most well-known guidelines.

An organization that is about to establish its response capabilities has to perform several preparatory activities. ISO/IEC [3] provides a rather detailed description of these activities. An information security *incident management policy* should be created and integrated into other corporate policies, and this policy should reflect the organization's need for incident management and how the organization will benefit from adopting a structured approach to this. Then the information security *incident management scheme* should be described, which demonstrates the specific organization's approach to incident management - including all procedures for responding to incidents, roles and responsibilities, communication structures and reporting lines, and all other activities belonging to the complete incident management process. Establishing a specific information security *incident response team* (ISIRT) is one of the recommendations from ISO/IEC, as such a team will be specially trained for resolving incidents, and coordinating and communicating with both internal and external stakeholders. The size and structure of this team should be adjusted according to the needs of the organization. *Awareness and training* of all personnel should be performed, as all employees should be able to recognize an incident and report accordingly. Last, but not least, the ISO/IEC 27035 standard recommends *regular testing* of the incident management scheme in order to check whether the established procedures and tools function appropriately. This phase of planning and preparations is a continuous process as there is an ever-present need for updates, changes, and maintenance of policies, procedures, and practices. Incident management scheme testing and training of personnel are important in order to reveal such needs for changes, and lessons learned from actual incidents will usually also contribute in the same way.

The ISO/IEC 27035 standard addresses corporate systems in general and hence does not contain any considerations specifically related to power automation systems or industrial control systems in general. The recently published ISO/IEC TR 27019 [8] is specifically tailored for process control systems in the energy industry, but provides no additional recommendations related

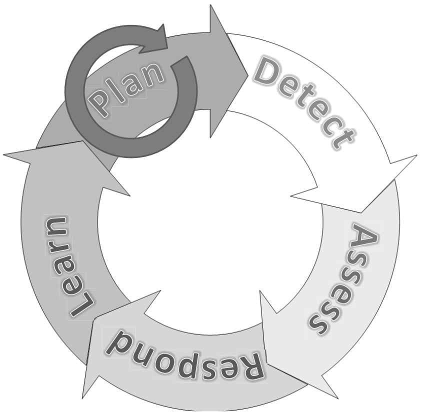


Fig. 1. The complete incident management process (ISO/IEC 27035)

to incident management beyond ISO/IEC 27002 [9]; which leaves ISO/IEC 27035 as the most comprehensive recommendations from the ISO/IEC. NIST describes a set of high-level requirements for incident response for a smart grid information system in their Guidelines for Smart Grid Security (NISTIR 7628) [10]. However, all requirements are on the governance, risk and compliance level, and are therefore more high-level than what ISO/IEC provides. They contain no specifics related to the co-operation of corporate systems and control systems. In part 3 of their Guidelines [11] NIST points out the need for research on incident response for the cross-domain of IT and power systems. More specifically, the issues of response and containment, intrusion detection and prevention, and event and impact prediction are emphasized.

B. Relevant experiences documented in literature

Experiences from literature provide more details on how planning for incident response management can be performed in practice. This literature can be used as inspiration, but also as input on which aspects of incident management are challenging and need to be given more attention. Several studies and experience reports are available, where some also provide insight to the planning phase [12]–[18]. Below we provide an overview of important findings in this literature. We organize the presentation of these findings according to the main activities recommended by ISO/IEC 27035, namely the establishment of a policy, an incident management scheme and a response team, the awareness and training activities, and the scheme testing.

The importance of establishing a team and supporting policies and documentation is emphasised also in the real world experiences documented in the literature, and detailed explanations of how this can be done are available. Metzger et al. [12] present experiences from LRZ-CSIRT[5] where a holistic approach to incident management based on ISO/IEC 27001 [19] has been implemented. They state that 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. Recommendations from this case include the need for establishing a security incident response process and defining what a security incident is, in order to distinguish it from other types of failures and errors. Hove and Tårnes [13] point out the need for defining responsibilities, especially in organizations where IT operations are outsourced or several parties are included in operations and incident response. In complex systems it may be difficult to define such responsibilities, and it may also be difficult to know where a specific incident actually originates and thus determine who is responsible for responding [13]. Having a simple, short and common plan for incident management is recommended [17], [18]. This was considered a strength when present, and a need when not present. Without it, the approach to incident management could appear scattered and randomly structured [17].

Activities on awareness, training and incident management scheme testing seem less elaborate in existing experience literature, however the literature clearly points out the need for such activities. Flodeen, Haller, and Tjaden [14] studied an ad-hoc group of incident responders to see how a shared mental model for decision making can be developed through training. Such a shared mental model increases the performance during an incident handling process because the team manages to cooperate with limited and efficient communication. They 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. Werlinger et al. [15] found that incident response is a highly collaborative activity, and that the diagnosis work is complicated by the practitioners' need to rely on

[5] The incident response team at Leibniz Supercomputing Centre

tacit knowledge, as well as usability issues with security tools. Hove and Tårnes [13] also 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, as discussed by Pariès in Hollnagel et al. [20]. Hove and Tårnes discuss challenges of training for incident management [13]; ensuring realistic training scenarios and that the training actually provides value in real situations.

Scholl and Mangold [16] claim 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. The latter claim is in line with theory on high-reliability organizations (HROs) as described by Weick and Sutcliffe [21] and requires awareness among all employees and a reporting culture.

Most of the above identified literature considers general IT systems. The only exception is Jaatun et al. [17] who describe an incident response management process for the oil and gas industry, focusing particularly on the learning process after an incident. They found that although integrated operations in the North Sea were highly dependent on IT, there was still a great deal of mistrust between traditional process control engineers and IT personnel. Furthermore, since few cyber security incidents in this sector were systematically reported, there was a low level of awareness among upper management of, e.g., the importance of doing cyber security training drills. It seemed that some control system engineers even refused to acknowledge that their systems contained vital IT components. Jaatun et al. also found that existing reporting tools used for Health, Safety and Environment (HSE) incidents were poorly suited to reporting of cyber security incidents.

In other respects, there is a lack of studies on incident management in an operating environment with automation systems and IT systems co-functioning. Current practices, compliance to standards and/or need for changes in standards, challenges and reasons for such, and future research needs should be investigated and examined in order to provide contributions to organizations facing the reality of closely integrated IT and automation systems.

C. Expectations before the interviews

We expected to reveal weaknesses in the overall information security management system; documented policies and rules not being well-established throughout the organization, and lack of training on information security incident response. These expectations were based on our general knowledge of information security priorities in several organizations. When everything goes well, nobody offers it a thought, and it is hard to argue that more focus and investments are needed for such matters [22]. Training and improvements need to be performed on a regular basis. When everything goes wrong, it is much easier to obtain more resources, but this is rarely the time to perform training - recovery is much more important at that time to ensure business continuity. Right afterwards, someone will claim the need for training on such and similar scenarios in the future, but the everyday tasks have a tendency to receive higher priority.

We also expected to find differences between IT and control systems on several issues:

- Perceptions on what is an information security incident
- Experience in handling incidents
- Perspectives on relevance and possible consequences of different incidents

These expectations were based on the fact that there are differences between the traditions of IT and ICS, as introduced in Section I. The history of control systems, where they have been operated quite isolated from other networks, would indicate that information security incidents is an issue that they have not had to deal with before.

III. Research method

The study is based on semi-structured interviews and review of documentation [23], [24]. Six distribution system operators (DSOs) in the power industry participated in the study. They all serve more than 50.000 power consumers and are considered large in a Norwegian context.

A. Data collection

Semi-structured interviews are based on a predefined set of questions contained in an interview guide, but allow for the interviewer to add unplanned questions based on the responses provided by the interviewee [24]. Our interview guide was inspired by the ISO/IEC 27035 standard [3], and was intended to cover all phases, cf. Appendix A. However, as the interviewees are mainly managers, their responses reflected the management level perspective, and we realized during the study that we did not receive as much detailed information on the response activities as we first expected.

The interviews were carried out June-December 2012 at the various DSOs' premises respectively. All interviews were voice recorded and transcribed. The study was registered at the Data Protection Official for Research[6] and all interviewees signed a consent agreement according to the privacy regulations. One test interview was carried out in DSO B, without the use of voice recording. This interview is not included in the data material, but used as a test of the interview guide and training for the

[6] http://www.nsd.uib.no/personvern/en/index.html

TABLE I
THE DISTRIBUTION SYSTEM OPERATORS (DSOS) INCLUDED IN OUR STUDY

DSO	Role of interviewees	Documentation received	IT operations outsourced	Required NDA
A	IT, IT sec, IT operations, control systems	Information security instructions, Plans for preparedness in IT systems	yes	no
B	IT, IT sec, control systems	no	no	no
C	Corporate IT, IT in branch company, control systems	no	yes	no
D	IT, IT sec, control systems	no	yes	yes
E	IT, IT sec, control systems	Information security instructions, Plans for preparedness in control systems	no	yes
F	IT sec, control systems, quality & risk	Information security policy, Information security events (quarterly report Q2-2012)	yes	yes

interviewer. The test interviewee was not interviewed again, but he is included in the mailing list of interviewees who receive information and updates from the study.

Data triangulation is a way of enhancing the rigour of the research [24], which means using multiple methods for data collection. In addition to the interviews, we thus asked 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

Three of the DSOs provided us with some documentation (c.f. Table I). Confidentiality issues prevented the other three DSOs from sharing documentation. Non-disclosure agreements and encrypted electronic transfer were not sufficient instruments for overcoming the confidentiality issues[7].

B. 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]. It was mainly performed by one researcher due to confidentiality restrictions posed by three of the participating DSOs (D, E, F, c.f. Table I)[8]. 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 three DSOs (A, B, C, c.f. Table I). The software tool NVivo[9] was used for the data analysis.

C. Industrial case context

Six DSOs are included in the study, and they were selected for being among the largest DSOs in the country, as well as being partners in the national research project DeVID. Three different roles from each DSO were interviewed; IT manager, IT security manager, and manager of control systems. One exception is DSO F, where the IT manager was unable to participate, and we talked to the manager for quality and risk instead. In one of the DSOs we also interviewed one member of the technical IT staff in addition to the IT manager. In total, 19 interviews were carried out. As we address incident management from the information security management perspective, only managers were included in the interview study. If we were to investigate in further detail the technical response activities performed when an incident occur, we would have had to include technical IT staff and preferably also representatives from external IT suppliers in the cases where the DSOs have outsourced large parts of their IT operations. In order to get the whole picture of IT and power automation, we included managers from both areas.

More DSOs than these six are partners in the national research project DeVID and could hence easily have been included. However, after the completion of the planned interviews in the six DSOs, saturation was reached [28]. For the perspectives

[7] It must however be noted that just the day after my request for documentation, 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 state 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 to the data triangulation. Kotulic et al. [25] 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 collection of sensitive data. Also, the companies in focus can be more involved in discussing and approving the results.

[8] All DSOs are partners in the DeVID project. Some considered the confidentiality agreement for the project consortium to be sufficient for this interview study, while others required the signing of an additional non-disclosure agreement (NDA) for the interviewing researcher.

[9] http://www.qsrinternational.com/

TABLE II
DISTRIBUTION OF INTERVIEWEES PER ORGANIZATION

DSO	IT manager			IT Security Manager			% IT security
	Parent co	Branch	Outsourced	Parent co	Branch	Outsourced	of full position
A			x[a]		x[a]		5%
B	x[b]			x[b]			100%
C	x[b]	x[a]					
D	x[a]				x[b]		10-20 %
E	x[a]				x		100%
F						x [a]	50%

[a] Only administrative system
[b] Both IT and ICS

of IT managers and IT security managers, saturation was actually reached before all the planned interviews were completed, as their responses were fairly aligned. The need for information from control room managers still called for completing the interviews in all six DSOs.

All the DSOs are organized as a corporation where the power supply infrastructure is taken care of by one branch company. Other branch companies may be within power production and broadband. Four out of six have outsourced their administrative IT services to an external supplier, but all these external suppliers are 100% owned by the DSOs respectively, due to their past as an internal IT department. The other two operates the administrative IT systems themselves. Control systems are operated internally by all the DSOs.

All the control system managers belong to the branch company[10]. They are responsible for the daily operations of the control systems, including information security issues. Even in the cases where IT managers or IT security managers are said to be responsible for this, it is the managers of control systems who in practice execute this authority. A brief overview of the participating organizations is presented in Table I, and roles and placement of interviewees within each organization is explained in Table II.

IV. FINDINGS

A. Dependency on IT

The responses indicate that the DSOs can better endure unforeseen downtime in their power automation systems than in the administrative IT systems. All the IT managers and IT security managers claim that their organization is 100%, or close to 100%, dependent on IT systems. The business may run for some days without IT systems, but several challenges will occur quite soon. Planning, follow-up, and maintenance will be impossible. If maps of the distribution grid are not available, no digging can be done in a certain area, which again may stop construction work. If invoicing is impossible, the cash flow will stop; this is when the IT breakdown really manifests itself.

The control system managers also state a 100% dependency of IT, although they add that unavailable IT systems do not automatically cause power failure for customers. The distribution grid can be operated manually even if the control room or other parts of the SCADA systems are unavailable, as this is a requirement in the national regulations. However, the customers will be the most important failure detection mechanism and the DSOs will face the challenge of making the right prioritizations based on information from the customers, as opposed to having functioning monitoring systems that automatically detect failures and provide richer background information on the failures. The length of the period that the DSOs are able to operate manually depends on available personnel for fixing failures, but two-three days would be manageable. If the amount of failures is too high, they are not able to keep up, which might result in a considerably reduced quality of service for customers. With a smaller amount of failures, manual operation may be possible for a long time.

The term *IT systems* is interpreted differently among the interviewees dependent on their work position. IT managers do not necessarily include SCADA systems in their definition. For control room managers, IT systems equal SCADA systems.

B. Definition of an incident

The responses indicate that IT managers and IT security managers have a much more uniform comprehension of the concept of information security incidents than control room managers. There are large variations among control system managers when they are asked to define an IT security incident. None of them provide a clear definition, and they all state that this term is not defined in the organization. One (A) thinks of it as malicious attacks, while he considers unavailability due to digging or technical failures to be outside the scope of information security. Four respondents think of it as unwanted occurrences in the IT systems, including breaches of policy or procedures, computer viruses and intrusions, and the last one (E) explains it more specifically as an occurrence that can affect functionality and/or compromise sensitive information.

[10] The one from E belongs to a the branch company for power production where the IT operations are located, same as for the IT security manager from E.

Only the IT manager in C used the terms confidentiality, integrity and availability when defining an IT security incident. The others have similar perceptions, without providing a clear definition. Examples of incidents are mentioned, like disclosure of confidential information to unauthorized persons, breach of procedure, intrusions, sabotage, computer viruses, both malicious and accidental occurrences.

> *"Good question. I have never thought of that."*
>
> — *IT manager (A) when asked to define an IT security incident*

Among IT security managers only the one from F uses the terms *confidentiality, integrity and availability*. All the others claim that their organization does not have a clear definition of what comprises an incident, but like the IT managers, the IT security managers also provide several examples of IT security incidents, like hardware thefts, hacking, viruses and sabotage. This aligns with the documentation studied. The information security policy from F states a clear definition as provided by the IT security manager, and also *authentication* is included in the written policy. The information security instructions from A and E do not contain any definition. However, several examples of information security incidents are listed in the documentation we received, as reflected by several of the informants.

A common impression among control room managers is that IT incidents have never occurred in their systems. IT security managers, to the contrary, claim that several incidents occur every week. Control room managers claim they have never experienced disruptions in power supply due to information security incidents. The power automation systems are extremely robust and resilient towards incidents involving individual components. Physical damage due to stormy weather may occur, but they do not refer to this as an information security issue.

C. Worst case scenario

Almost all interviewees state that the worst incident they can imagine is if someone hacks the power automation system, gains control of power switches and can control the power distribution system. Attackers could cause outages in large cities in a few minutes if they have the right access. They could also do the opposite; switch the power on in a part of the grid that is without voltage due to maintenance and hence cause physical harm or death to maintenance workers. This is especially mentioned by the control system manager in D. Even though several security mechanisms are in place to prevent such and similar scenarios, it is stated by the interviewees that they might still occur, even though the probability is quite low. Also, as the control system manager in F states, the attack force obtained through a combination of foreign governments and criminal actors exceeds the response capabilities of most organizations.

Other worst case scenarios mentioned include compromised customer databases with large amounts of personal information; complete deletion of databases (and all related backups) containing all information on the physical power grid; minor errors in the billing system for a long time such that rollback is impossible when the errors are finally detected; compromised information on power distribution that could be used to attack certain customers; misuse of the disconnection function in smart meters that could result in outages without the SCADA system being involved; and fire or natural disasters that destroy buildings where the control room is located.

The IT security manager from E points out that sensitive information is not handled satisfactorily. He believes that cloud services are widely used, without this being approved as acceptable and secure storage. Employees require availability of information and flexibility in when and where to work, and take with them information without considering possible implications on information security. Such breaches may have large financial consequences to the organization if for example tender documents have been compromised.

The IT security manager in F states that the combination of incidents is the worst thing, for example a hacking attack and really bad weather causing logical errors and physical damage at the same time.

D. Documentation of plans and procedures

Three of the four DSOs that have outsourced their administrative IT systems (A, C, D), lack plans for responding to incidents and seem to rather expect the IT supplier to have such plans in place[11]. The information security instructions from A contains only reporting procedures for users. However, some DSOs (A, B, D) are currently working on documenting their plans and procedures for the first time, both for IT and control systems. They have been trusting their employees to know what to do, but have realized that they also need a certain documentation base in place. It is however not clearly stated who will actually develop unified plans that take both IT and control systems into account. The ISO/IEC 27001 standard is mentioned as being used for identifying issues to be documented. The other DSOs do have reporting procedures and/or continuity plans in place.

One IT security manager (F) states that his organization has an information security policy and procedures for incident management in place. This was also among the documentation we received. However, the control room manager from the same organization is not familiar with the existence of this documentation. The control room manager in B is aware of the

[11] Whether this also goes for the fourth DSO in the same outsourcing situation is unclear, as the IT manager was not among the interviewees, and the IT security manager belongs to the external IT supplier.

existence of such plans in his organization, but they originate from the IT department and do not consider automation systems specifically. He would like to have similar documentation for his systems as well. He does not seem to be aware of the procedures currently being prepared as reported by the IT security manager.

In E they have clearly defined procedures for the administrative systems and security instructions for the power automation systems. Their control room manager states that documentation needs to be combined with highly competent personnel, because it is impossible to write detailed procedures for any possible incident.

Several interviewees admit that plans are not commonly used, either because they are non-existent or because incidents occur quite rarely. The one from IT operations in A however says that they practice quite frequently and mentions that employees are invited to hand in their laptop during summer holiday for a clean-up. Then the technical personnel familiarize themselves with the computers, analyze them and are able to test different tools. The purpose is not to reveal any breaches by the employees but to practice and experience technical support and maintenance issues.

The ISO/IEC 27035 standard is not mentioned by any of our informants. We did not ask specifically whether they were familiar with it, but it was never brought up during any of the interviews. This may indicate that the standard is not used by the organizations. It might be the case that the informants did not find an opportunity to mention it among all the questions that were asked, although this does not appear as the most plausible explanation, as the use of such a standard is closely linked to the existence of plans and procedures, which was a topic in all interviews.

> *"This I have never asked for, to see the procedures for responding to an information security incident. Maybe I should."*
>
> *— IT security manager (D)*

E. Preparedness for worst case scenarios

Three IT managers (B, D, E) claim that they will be able to respond satisfactory to a worst case scenario, due to their well organized and planned emergency preparedness in general, although they have some weaknesses related to IT-specific preparedness. They are currently working towards a more systematic IT security preparedness as well, and one (B) is planning a physical backup site, having identified this as a need in order to be better prepared. The IT security manager from B supports his IT manager in this view of them being prepared to respond to a worst case scenario. The IT security manager from D is more reluctant to claim that they are well prepared; he says that they lack practice and well established procedures. However, he feels confident that they will be able to improvise. He is not worried about the control systems in case of an incident, as this can be disconnected and operate offline. The IT security manager in E agrees with his IT manager in that they are prepared, although it should be noted that they present quite different scenarios to be the worst cases to occur (compromised sensitive information vs. sabotage/natural catastrophe/hacking attack).

The other IT managers assume that their organization will not be able to respond appropriately to a worst case scenario. As reasons they state that there are too few preparedness training drills, and that those that are performed have a too limited scope. Some perform dry runs from time to time.

The control system manager from D believes that their current procedures and practices would suffice if the worst case scenario should occur. However, as he states, it will be a future task to consider whether the response was appropriate or poor.

Several of the interviewees state that the control systems can be disconnected from the outside world and continue operation, something they perceive as an efficient response to incidents where the control systems are hacked. One (A) however points ut that this does not solve anything; it would stop the attack, but it would prevent you from further investigating the incident with respect to who is behind it and what could be the consequences.

F. Training

None of the IT managers or IT security managers report that they perform regular training exercises where an information security incident creates the basis for the scenario. But the authorities initiate general emergency preparedness exercises from time to time, and in some cases the scenario is based on such an incident.

The IT security manager in A expects their external IT supplier to perform training. However, the IT manager in A, who is the manager of this external IT supplier, claims that they never perform such training. The IT manager from C (branch company) states the same; that training for incident management is never performed. The corporate IT manager in C supports this fact that training is not performed, but he adds that they have had their share of incidents. He would like to see more training drills instead of the real incidents. Some IT security managers (D, E) agrees that training should be performed more often. "Fumbling and hubbub" constitute the most useful exercises, as put by the IT security manager from E.

> *"We are not good at post-evaluating real incidents and consider them as training exercises, we are too solution-oriented."*
>
> *— Corporate IT manager (C)*

Different reasons are given for the lack of training: training activities have not been prioritized, other tasks receive higher priority, and training involves a certain cost.

> *”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 (C) on training exercises*

The IT security manager in F argues that training is assigned a low priority due to the fact that real incidents rarely occur, hence they do not feel the need for being better prepared for responding efficiently. Still, their information security policy states that the plan for emergency preparedness is to be tested regularly, and that IT/infrastructure should be included.

In B they run comprehensive preparedness exercises internally in addition to the ones initiated from the authorities, as reported by their IT manager and IT security manager. These are not specifically related to IT security incidents, but there have been scenarios that include such elements, like fire in a building where the data centre and/or communication systems are located. Both dry runs and more realistic drills are performed.

Among the control room managers, the experiences with training vary. In E they manage to look at real incidents as training, adding some effort to the response activities; hence feeling more confident afterwards that their systems function as intended. The control room manager in F reports that they perform regular exercises on responding to communication breaches in the control systems. This aligns with the requirements in their plan for emergency preparedness as well. They have never considered training for information security incidents, but during the interview he realizes that the consequences, and hence the response activities, could be similar for those two scenarios. Hence, their regular training does strengthen their information security incident response capabilities as well as their general emergency preparedness. On the other hand, the other control room managers (A, B, C, D) state that they do not perform training for information security incident management. Reasons provided include merging of companies, moving, cost, time, and workload. Also the number of incidents experienced is quite low, so the need for training has not been identified in all DSOs. All these four interviewees feel that their training efforts are not satisfactory, but only one (C) states that they intend to improve in this area. *The personnel operating the control systems would benefit from training on scenarios like ”what do we do if the control systems break down?”,* reports the control manager from C.

V. Discussion

This paper set out to identify how planning and preparatory activities for information security incident management were performed in organizations that depend on successful cooperation between people working on conventional IT systems and ICS (Research Question 1). It also set out to identify differences in the planning and preparatory activities performed in these two disciplines (Research Question 2). The results show that current planning and preparatory activities are limited, at least compared to the recommendations in current standards and guidelines. ISO/IEC 27035 recommend activities related to the following: establishment of a policy, an incident management scheme and a response team, awareness and training, and scheme testing. In the following we summarize current practice on activity areas recommended in ISO/IEC 27035, before outlining the differences identified between the practices of IT and ICS staff. Then we move on to discussing the validity of our findings.

A. Current practice

We expected to find that documented policies were not widely established throughout the organizations, as well as a lack of training on information security incident response. These expectations were confirmed in the interviews.

In general, responsibilities in information security incident management seem to be inadequately established. This seems especially to be the case when IT system maintenance is outsourced. Documented plans and procedures for incident management in the IT systems do not widely exist. Where such plans do exist, some informants state that they do not sufficiently consider ICS. Just as often as answering yes/no to the question on whether plans exist, the interviewees started describing their plans. This suggests that the personnel most frequently involved in incident management have tacit knowledge and experience in the necessary actions to be taken in case an incident occurs. In daily practice this can be sufficient, as long as this personnel is available when incidents occur. Some DSOs have however found that they cannot solely rely on tacit knowledge for this, and are in the process of creating plans. Still they are aware that you cannot document everything, and have to rely on competence of personnel in addition to documentation.

Although the DSOs are highly dependent on the availability of competent personnel should an incident strike, they only report on limited awareness and training activities on information security incident management. In cases where procedures are documented, these do not seem to be well established or, in some cases, even known by staff expected to work according to the procedures. Any training activities performed seldom take information security incidents into account. Some of the activities reported as training in the interviews are also not really tailored to incident management, but are rather part of general computer maintenance. The reported reasons for not performing more training on information security incident management include cost and time issues, but in general it does not seem that they see the need for more focus in this area. Currently they experience a limited number of incidents.

Clearly, training activities seem to be difficult to prioritize. Whether training is also difficult to carry out is not clear. The interviewees who report that they perform drills from time to time do not report on specific challenges related to planning them or going through with them. However, training might be continuously postponed due to the lack of knowledge on how to plan and/or accomplish such trainings.

Incident management scheme testing seem not to be performed by the DSOs. This can also be related to the unavailability of a scheme to test. But despite a general lack of plans for handling information security incidents, and a lack of training on this, quite a few DSOs still seem to have a relatively high degree of confidence that they can handle even a worst case scenario. They trust the competence of their employees and their ability to improvise and find solutions if an incident should occur. They also rely on their ability to disconnect their most critical systems from the outside world in case of a serious incident.

The findings in this survey seem to be in line with documented experiences in literature (see Section II-B), although the DSOs seem to lag behind on the establishment of policies, an incident management scheme and a response team [12], [13], [18]. Hove and Tårnes [13] documented specific challenges relating to outsourcing, and also the importance of having experienced incident handlers over a strict reliance on documentation. Lack of training for incident response is also identified in previous studies and experience reports. The challenges identified by Hove and Tårnes [13] when it comes to training (realistic scenarios, value for real situations) did however not come up in the performed interviews.

The relatively high trust in own abilities to handle worst case incidents can probably be explained by unrealistic optimism in risk perception in the information security domain, as documented in the study by Rhee et al. [29]. In order to mitigate this optimistic bias, they suggest that organizations perform more security awareness training and apply a more systematic approach to information security management. Such an approach seem to be currently lacking in the DSOs taking part in this study. The awareness by some of the interviewees on the importance of competence and ability to improvise is in line with resilience theory [20], but there seem to be a lack of understanding of what actions need to be in place in order to improve resilience in an organization, including risk awareness, response capacity and support [30].

B. Differences between IT and ICS

Table III presents a brief overview of the findings from our study of DSOs. A previous study in the oil and gas industry [17], where the implementation of integrated operations was in progress at the time, revealed similar gaps between IT and ICS as our recent study in the power industry. This gives us reasons to believe that similar organizations in other industries as well would report along these lines, given that the integration of IT and ICS has reached the same stadium as in the power industry.

We expected to find differences between IT and ICS staff when it came to perceptions of what an information security incident is, experience in handling incidents, and in the percieved consequences of incidents. As Table III shows, we were correct in our expectations when it comes to definitions and percieved consequences of incidents. From an IT perspective, such incidents happen frequently, and are concerned with compromise of information. From an ICS perspective the understanding of what an information security incident is seem to be more unclear, and they are mainly concerned with consequences for power supply. Variations existed among control room managers, and they commonly claim that information security incidents have never occurred in the control systems. IT managers and IT security managers are much more aligned, which could be explained by their common background and experience with the same type of IT systems and the same kind of information security threats. Control room managers give mixed responses on the relevance of minor information security incidents, but they all suggest malicious hacker attacks where the hacker gains control of power switches as the worst case scenario. This indicates that they have a fairly good understanding of the vulnerabilities and existing threats to their control systems in the situation of dependency of conventional IT systems. As such, they are aligned with the IT managers and IT security managers.

Also regarding experience in handling incidents, the findings resemble our expectations. Information security incidents occur frequently in the administrative IT systems in the DSOs, while rarely, if ever, in the control room. However, they do experience incidents in the control room as well, like component failures and communication breach, but these incidents are not defined as being information security incidents. Still, the consequences posed by all these examples might be quite similar. This suggests that control room managers and their operators might be better prepared for responding to information security incidents than the first impression might indicate. However, as the definition of an information security incident is not all clear, the biggest challenge of incident response in the control room might be to actually recognize such an incident and be able to determine the most appropriate first steps for the response phase.

Procedures for general emergency preparedness are usually well established and well practiced among control room operators, as reported by control room managers. The DSOs are required to perform exercises regularly, as a measure for ensuring continuous power supply. Traditional exercises have however rarely been based on incidents caused by IT systems. IT and ICS are viewed as two separate parts of the organization, and there has been limited collaboration between the two.

C. Threats to validity

Construct validity concerns whether a study measures what it sets out to measure [24]. Interviewees may be biased, either consciously or unconsciously [31]. The topic being information security incidents could increase this bias as well; their conscious or unconscious desire to make their organization and themselves look good from the outside. Our impression is that they were being honest in their reportings as several of the interviewees did not report a perfect situation, rather lackings in a

TABLE III
SUMMARY OF FINDINGS

	IT systems	**Control systems**
Dependency on IT	Claim to be 100% dependent, can endure for some days, until cashflow stops.	Claim to be 100% dependent, but can operate power grid manually without control room. Endurance of manual operation is determined by number and severity of failures that occur.
Definition of incident	Confidentiality, integrity, availability mentioned by some. Both malicious and accidental occurrences - unwanted. Occurs frequently.	No common definition exist in the organizations. Malicious attacks, unwanted occurrences in the system. Occurs rarely, if ever.
Worst case scenario	Compromised/deleted databases with customer information and/or information on the physical power grid	Malicious hacker attacks in control systems, gaining control of power switches, causing outages.
Documented plans	Not widely established. In progress in some DSOs.	Established in one DSO, otherwise in progress or non-existing.
Preparedness for worst case	Various perceptions: Well-organized and planned general emergency preparedness, and/or ability to improvise. Also reported doubt on own preparedness due to lack of training.	Current practice and competence is perceived as sufficient. Disconnecting the control room is highlighted as the most appropriate and plausible measure towards worst case scenario (malicious hacker attack).
Training	No regular drills based on information security scenario. Regular general emergency preparedness exercises; occasionally, these deal with information security/IT incident.	Regular general emergency preparedness exercises; information security never forms the basis.

number of areas. Some even expressed their gratitude for us performing this study, as it gave them an opportunity to discuss these issues internally. Being able to point to us as external, independent researchers, strengthened their message.

All interviewees belong to a management level in the organization. The IT security manager often reports to the IT manager, but there are still employees on lower levels performing a large part of the daily tasks within incident management. Not including such employees as interviewees is an obvious limitation of this study, as the managers might provide information on how things should be done, not just on how things actually are being done. However, it was necessary to make such a limitation due to time constraints. Also, the planning and preparations activites, as this paper reports, are the responsibility of the managers. So for this part of the study, the selection of interviewees appears appropriate.

An alternative strategy would be to study only one or two organizations in depth, and then include more employees from each organization as interviewees. This would probably make us better able to say something about differences between written plans and procedures and actual daily practice. However, we wanted to cover a larger number of organizations in order to see what is widespread current practice.

Data triangulation [23] increases the quality of data as it allows a phenomenon to be studied from different perspectives. Interviews and documentation provides two different views on incident management, as the interviewees would describe their practice as they know it, while documentation will show the planned procedures. We did not distribute the interview guide in advance, as we did not look for the ”correct” answers, but rather the interviewees’ perceptions, understandings and actual practice. Then we studied the received documentation to see whether there were any significant differences between the two. A third source of evidence was considered, but has unfortunately not been feasible: participating in a post-incident evaluation meeting at a specific DSO. This would have provided us with detailed information on how an actual incident was responded to. The DSOs have expressed willingness in including us in such a meeting, but we have not been able to follow-up on this as it would require us to be actively asking for it regularly; we would not expect them to call us.

We did not interview the IT manager in DSO F as he was not able to make it, even though we did schedule the interview in advance. We instead got to talk to the Manager for quality and risk. We asked each DSO for specific roles and described the purpose for this, but we could not control in detail who were identified by each DSO to participate. As most of the interviews required travelling and hence planning ahead, we were not able to go back to the DSOs in order to meet the most appropriate person if he was not present on the agreed time and date. We asked the IT manager in DSO F to respond to our questions in writing, because that would give us a richer data material than no response at all. However, we never received anything from him.

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 that we value the contributions of our informants. We received feedback regarding the case context description, which we updated accordingly.

External validity refers to the degree to which the findings from a study can be generalized to other settings [24]. Our study is restricted to large DSOs and the roles of the requested interviewees were clearly defined. We have provided a detailed description of the industrial case context (cf. Section III, which is of great importance when considering whether our results are transferrable to a given setting. As our expectations regarding findings were generally met, it may be assumed that the participating DSOs do not stand out in any particular way compared to similar organizations. There is a lack of similar studies[12] on incident management in organizations depending on successful collaborations between IT and ICS, hence we believe that our study should be repeated for similar and slightly different case contexts than ours. Generalizability will be strengthened by increasing the number of studies.

VI. Concluding remarks and further work

This paper has presented findings related to the planning and preparations activities for information security incident management. There are differences between the IT and ICS disciplines in practice, as we expected beforehand. As the Smart Grids emerge, IT will be permeating the control systems even more than today; more commercial off-the-shelf products, more connectivity, and more integration [1]. Further studies are required to investigate how these differences should be addressed for a unified approach to incident management to be achieved.

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

Training for IT security incidents is reported as challenging; especially being able to prioritize it among several pressing tasks. However, general emergency preparedness exercises are frequently performed. Future work should investigate why training for IT security preparedness is more difficult and how knowledge could be transferred from the areas of general emergency preparedness exercises, industrial safety training and resilience, in order to design and implement training programs for organizations where IT and SCADA systems and staff need to collaborate.

> *"The big profit for the industry will be in accomplishing successful interaction between IT and power. That will also gain information security in smart grids."*
>
> *— IT manager*

The ISO 27035 was not brought up in any of the interviews. This calls for an investigation on the knowledge of this standard and to which extent it could assist DSOs and similar organizations in improving their information security incident management process.

Activities performed during and after an incident were also covered in the same interviews, and these findings will be presented and discussed in a follow-up paper. We have recently performed additional interviews in small DSOs, where *small* is defined as *supplying less than 10.000 power consumers*. The follow-up paper will also summarize findings from these interviews, including a comparison of large and small DSOs on their approaches to incident management.

Acknowledgment

We are grateful to the distribution system operators who contributed with informants for our interviews.

References

[1] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, Dec. 2011.

[2] Éireann P. Leverett, "Quantitatively Assessing and Visualising Industrial System Attack Surfaces," University of Cambridge, 2011.

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

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

[5] T. Grance, K. Kent, and B. Kim, "NIST SP 800-61: Computer Security Incident Handling Guide," National Institute of Standards and Technology, 2008.

[6] ENISA, "Good practice guide for incident management," 2010.

[7] P. Kral, "The Incident Handler's Handbook," SANS Institute, Tech. Rep., 2011.

[8] "ISO/IEC TR 27019:2013 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry," 2013.

[9] "ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management," 2005.

[10] NIST, "7628-1: Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology, 2010.

[11] NIST, "7628-3: Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology, 2010.

[12] 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)*, 2011, pp. 107–121.

[13] C. Hove and M. Tårnes, "Information Security Incident Management: An Empirical Study of Current Practice," Norwegian University of Science and Technology, 2013.

[14] R. Floodeen, J. Haller, and B. Tjaden, "Identifying a Shared Mental Model Among Incident Responders," in *7th International Conference on IT Security Incident Management and IT Forensics*. IEEE Computer Society, 2013.

[15] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Information Management & Computer Security*, 2010.

[16] F. Scholl and M. Mangold, "Proactive Incident Response," *The Information Systems Security Association Journal*, 2011.

[17] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and 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.

[12] With the exception of the related work of Jaatun et al. [17]

[18] J. Cusick and G. Ma, “Creating an ITIL inspired Incident Management approach: Roots, response, and results,” in *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, 2010, pp. 142–148.

[19] “ISO/IEC 27001:2005 Information security management systems - Requirements,” 2005.

[20] E. Hollnagel, J. Pariès, D. D. Woods, and J. Wreathall, Eds., *Resilience Engineering in Practice - a Guidebook*. Ashgate Publishing Ltd., 2011.

[21] K. E. Weick and K. M. Sutcliffe, *Managing the unexpected*. John Wiley, 2007.

[22] N. P. Repenning and J. D. Sterman, “Nobody ever gets credit for fixing problems that never happened: creating and sustaining process improvement,” *IEEE Engineering Management Review*, vol. 30, pp. 64–64, 2002.

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

[24] C. Robson, *Real world research*, 3rd ed. John Wiley & Sons Ltd., 2011.

[25] A. G. Kotulic and J. G. Clark, “Why there arent more information security research studies,” *Information & Management*, vol. 41, no. 5, pp. 597 – 607, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378720603000995

[26] R. Bogdan and S. Biklen, *Qualitative research for education: an introduction to theory and methods*. Allyn and Bacon, 1982. [Online]. Available: http://books.google.no/books?id=wIOcAAAAMAAJ

[27] J. Lofland, *Analysing social settings*. Wadsworth Pub, 1971. [Online]. Available: http://books.google.no/books?id=fIOjKQAACAAJ

[28] G. Guest, A. Bunce, and L. Johnson, “How many interviews are enough? An experiment with data saturation and variability,” *Field Methods*, vol. 18, no. 1, February 2006.

[29] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, “Unrealistic optimism on information security management,” *Computers & Security*, vol. 31, no. 2, pp. 221 – 232, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404811001441

[30] K. Bernsmed and I. A. Tøndel, “Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management,” in *Seventh International Conference on IT Security Incident Management and IT Forensics (IMF)*, 2013.

[31] 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, no. 6, pp. 875–894, 2009. [Online]. Available: http://dx.doi.org/10.1007/s11135-008-9164-0

Appendix A
Interview guide

Individual

1) How many employees are there in your organization?
2) Which position and/or role do you have?
3) For how long have you had this position?
4) Which systems and procedures are within your responsibility?
5) Can you describe how your position connects to the work related to security, ICT and automation systems?

ICT security incidents

6) To which degree does the organization depend on ICT?
7) How would you define an ICT security incident?
8) Can you describe your latest ICT security incident?
   - How was this incident responded to?
   - How well did the response work?
   - Why did the response work as it did?
9) What is the worst ICT security incident your organization could experience?
10) If you think about how the latest ICT security incident was responded to, would this be sufficient to handle the worst possible ICT security incident?
    - Would you have done the same if it was a targeted hacker attack?
11) How frequently do you experience ICT security incidents?
    - If you have never experienced ICT security incidents, what could be the reasons for that?
12) What kind of ICT security incidents do you experience?
    - What kind of consequences are typical for this kind of incidents?

Responding to ICT security incidents

13) Which plans exist for ICT security incident management?
14) Are the plans used in practice?
    - If not, why not?
15) Do you perform training on incident management?
    - If yes, how? (Scenarios, exercises, courses?)
    - If not, why not?
16) How are ICT security incidents usually detected? (Automatic tools? Intrusion detection systems? Firewalls? Users? Manual audit of logs?)
17) How are ICT security incidents initially reported?
18) Who is involved in responding to ICT security incidents?
19) Do you experience challenges related to cooperation on responding to incidents?
    - If yes, what kind of experiences? (Are they related to communication? Terminology? Responsibilities? Knowledge and experience? Procedures?
20) What kind of supplementary work is performed when regular operation is restored?
21) How are ICT security incidents registered and reported afterwards?
22) Is information on incidents reported to top management?
23) Is information on incidents disseminated to end-users, internally or externally?
24) Do you report ICT security incidents to the police?
25) Are the experiences from ICT security incidents used as input to further risk assessments and improvements of procedures afterwards? (Or is incident response mainly "‘firefighting"’?
    - If yes, which parts of the organization are involved in this process?
26) Do you have any numbers for the costs of ICT security incidents?
    - If yes: How frequently and how are these followed-up? Who is responsible?

27) Did you establish any other indicators or measurements for ICT security incidents? (E.g., downtime due to incidents, number of incidents per month)
    - If yes: How frequently and how are these followed up? Who is responsible?

Possible improvements

28) What are the most important actions performed in order to restore regular operation and limit the consequences from an ICT security incident?
29) Do you see any possible improvements to how you respond to ICT security incidents?
    - If yes, which?
30) The Smart Grid leads to a closer integration of ICT and automation systems in the future. How do you think this will affect ICT security incident management?
31) Is there any cross-organizational cooperation in the industry regarding information security? (Work groups, seminars, regular meetings?)
    - If yes, to which degree is ICT security incident management on the agenda?

NTNU

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Telematics

To whom it may concern,

Statement of authorship on joint publication to be used in Maria B. Line's PhD thesis

(Cf. NTNU PhD regulations § 7.4, section 4 and dr.philos regulations § 3, section 5)

This statement regards the following joint publication:

> Line, M. B., Tøndel, I. A., Jaatun, M. G.: *Information security incident management: Planning for failure*, in Proceedings from the 8th International Conference on IT Security Incident Management and IT Forensics (IMF), ISBN 978-1-4799-4330-2, May 12-14 2014, Münster, Germany.

Maria B. Line planned and carried out the interview study described in this publication. She performed the data analysis and was the lead author, writing a major part of the paper.

I hereby confirm that the doctoral candidate's contribution is correctly identified above, and I consent to Maria B. Line including it in her PhD thesis.

Trondheim, 16.09.2014

Inger Anne Tøndel   Martin S. Jaatun

Inger Anne Tøndel   Martin Gilje Jaatun

PAPER 7

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

Maria B. Line, Inger Anne Tøndel and Martin G. Jaatun

Submitted to International Journal of Critical Infrastructure Protection.
ISSN 1874-5482.

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]. 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 [2].

Well-known attacks like Stuxnet [3, 4, 5] and NightDragon [6], and statistics presented by ICS-CERT [7] 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 [7] 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 [8].

We have studied current practice for information security incident management among electric power distribution system operators (DSOs)[1]. 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. [9]. 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.

[1] This work is funded by the Norwegian Research Council, grants no 217528 and no 234644/F11, and by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*.

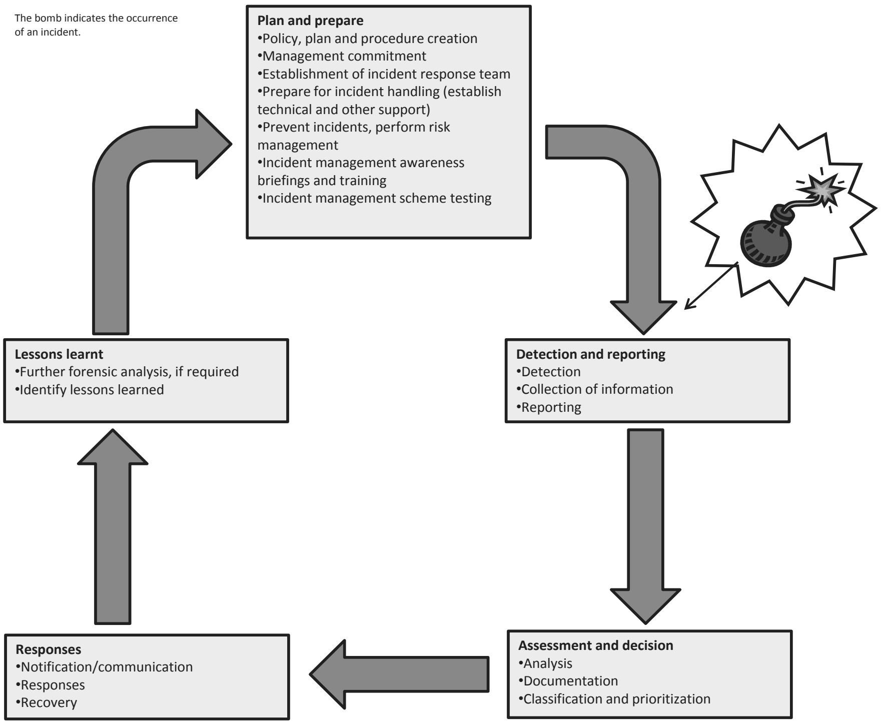

The bomb indicates the occurrence of an incident.
Plan and prepare
•Policy, plan and procedure creation
•Management commitment
•Establishment of incident response team
•Prepare for incident handling (establish technical and other support)
•Prevent incidents, perform risk management
•Incident management awareness briefings and training
•Incident management scheme testing
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).

2. Background

A number of standards and guidelines provide recommendations regarding the general information security incident management process, including ISO/IEC 27035 [8], NIST 800-61 [10], ITIL [11], and ENISA [12, 13]. 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) [14], 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. [15] 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. [16] and Line [17], 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 [15].

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 [15]. Flodeen et al. [18] 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 [19]. Hove et al. [20] 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 [21]. 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. [20].

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 [22, 23].

3.1. Data collection

Semi-structured interviews are based on an interview guide and allow for unplanned questions [23]. Our interview guide was inspired by the ISO/IEC 27035 [8][2]. We revised the interview guide from the study of large DSOs before interviewing the small DSOs: some questions were

[2] The interview guide is to be found at the bottom of this page: www.item.ntnu.no/people/personalpages/phd/maria.b.line/start. The interview guide used for large DSOs can be found as an appendix in Line et al. [9].

added (6, 17, 30, 31, 33, and 34) and one was removed[3]. 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[4]. All interviews were voice recorded and transcribed. The study was registered at the Data Protection Official for Research[5]. 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[6].

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 [25, 26]. This was performed by one researcher due to confidentiality restrictions posed by four of the participating DSOs (D, E, F, Z)[7], c.f. Table 1. Two fellow researchers were involved in discussing coding categories and findings, and writing up this report. They had access to the transcriptions

[3] It concerned the most important actions in the response phase, but the question was too vague and was interpreted very differently by interviewees in the large DSOs.

[4] There was one exception: the last interview at DSO Y was for practical reasons carried out over the telephone. The need for including this interviewee was identified during the first interview at this DSO, when the researcher visited their premises, and it was difficult to arrange for a re-visit due to time restrictions.

[5] http://www.nsd.uib.no/personvern/en/index.html

[6] 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 [24] 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.

[7] The large DSOs (A-F) are partners in the DeVID project, the small DSOs (X-Z) are not. The DSOs B and C considered the confidentiality agreement for the project consortium to be sufficient for this interview study, while the other DSOs (A, D, E, F) required the signing of an additional non-disclosure agreement (NDA) for the interviewing researcher.

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

from the interviews conducted in the other DSOs (A[8], B, C, X, Y, c.f. Table 1) and reviewed the codes that emerged during the analysis. The software tool NVivo[9] 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. [9]. The second phase included three small DSOs (X-Z)[10], 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

[8] DSO A required an additional NDA to be signed, but this NDA allowed for all the three researchers to have access to the data material.

[9] http://www.qsrinternational.com/

[10] Denoting the small DSOs G, H, I would be the obvious choice following the large DSOs A-F, but by using X, Y, Z instead, the reader will find it easier to distinguish the small from the large DSOs.

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[11]. 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	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.	–

[11] It became evident during our interviewee with their IT manager that the IT responsibilities were divided between him and the finance manager. The IT manager was acting as internal IT support, while the finance manager was responsible for the service agreements with their IT supplier.

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

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. [9]. 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 [9]: 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[12]. 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.*

[12] The cost of not-delivered power is well-defined in the Norwegian power industry.

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 [27]. 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 [28]. 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. [15]. Rhee et al. [29] 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 [30]. 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 [31]. 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. [32], 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 [33]. 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 [34].

Documented experiences on incident management from other sectors show that efficient and successful incident management requires collaboration between several parties [15]. 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 [15]. Hove et al. [20] 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[13]. 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

[13] All organizations licensed according to Energiloven (Energy Act) must have in-house expertise for all tasks covered by the license.

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 [3, 4, 5].

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 [7]. 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 [20].

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[14].

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.

[14] 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.

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 [35].

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 [36], 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 [22]. 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 [23], 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 [23]. 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[15] 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 [37]. 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 [38]. 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 preparednes 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,

[15] With the exception of the related work of Jaatun et al. [16].

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 is funded by the Norwegian Research Council through the *DeVID* project, grant no 217528, and by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*.

References

[1] M. B. Line, I. A. Tøndel, M. G. Jaatun, Cyber security challenges in Smart Grids, in: 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe), 2011. doi:10.1109/ISGTEurope.2011.6162695.

[2] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. Eeten, M. Levi, T. Moore, S. Savage, Measuring the Cost of Cybercrime, in: 11th Workshop on the Economics of Information Security (WEIS'12), 2012.

[3] D. Albright, P. Brannan, C. Walrond, Did Stuxnet take out 1000 centrifuges at the Natanz enrichment plant?, Tech. rep., Institute for Science and International Security (ISIS) (2010).

[4] D. Albright, P. Brannan, C. Walrond, Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, Tech. rep., Institute for Science and International Security (ISIS) (2011).

[5] N. Falliere, L. O. Murchu, E. Chien, W32.Stuxnet Dossier, Tech. rep., Symantec (February 2011).

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

[7] ICS-CERT, ICS-CERT Monitor, `https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT\_Monitor\_Oct-Dec2013.pdf` (Oct/Nov/Dec 2013).

[8] ISO/IEC, ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management (2011).

[9] M. B. Line, I. A. Tøndel, M. G. Jaatun, Information security incident management: Planning for failure, in: 8th International Conference on IT Security Incident Management and IT Forensics (IMF), 2014, pp. 47–61.

[10] T. Grance, K. Kent, B. Kim, NIST SP 800-61: Computer Security Incident Handling Guide, National Institute of Standards and Technology (2008).

[11] 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, 2012.

[12] ENISA, A basic collection of good practices for running a CSIRT, European Network and Information Security Agency (2008).

[13] ENISA, Good practice guide for incident management, European Network and Information Security Agency (2010).

[14] NIST, NIST 7628-3: Guidelines for Smart Grid Cyber Security (2010).

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

[16] 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 2 (2009) 26–37.

[17] M. B. Line, A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry, in: 7th International Conference on IT Security Incident Management and IT Forensics (IMF), 2013, pp. 26–32.

[18] R. Floodeen, J. Haller, B. Tjaden, Identifying a Shared Mental Model Among Incident Responders, in: 7th International Conference on IT Security Incident Management and IT Forensics 2013, IEEE Computer Society, Los Alamitos, CA, USA, 2013, pp. 15–25.

[19] R. Werlinger, K. Muldner, K. Hawkey, K. Beznosov, Preparation, detection, and analysis: the diagnostic work of IT security incident response, Information Management & Computer Security.

[20] C. Hove, M. Tårnes, M. B. Line, K. Bernsmed, Information security incident management: Identified practice in large organizations, in: 8th International Conference on IT Security Incident Management and IT Forensics (IMF), 2014, pp. 27–46.

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

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

[23] C. Robson, Real world research, 3rd Edition, John Wiley & Sons Ltd., 2011.

[24] A. G. Kotulic, J. G. Clark, Why there arent more information security research studies, Information & Management 41 (5) (2004) 597 – 607. doi:http://dx.doi.org/10.1016/j.im.2003.08.001.
URL `http://www.sciencedirect.com/science/article/pii/S0378720603000995`

[25] R. Bogdan, S. Biklen, Qualitative research for education: an introduction to theory and methods, Allyn and Bacon, 1982.
URL `http://books.google.no/books?id=wIOcAAAAMAAJ`

[26] J. Lofland, Analysing social settings, Wadsworth Pub, 1971.
URL `http://books.google.no/books?id=fIOjKQAACAAJ`

[27] T. Aven, O. Renn, Risk Management and Governance: Concepts, Guidelines and Applications, Vol. 16 of Risk, Governance and Society, Springer Berlin Heidelberg, 2010.

[28] T. Rundmo, Associations between risk perception and safety, Safety Science 24 (3) (1996) 197 – 209. doi:http://dx.doi.org/10.1016/S0925-7535(97)00038-6.
URL `http://www.sciencedirect.com/science/article/pii/S0925753597000386`

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

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

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

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

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

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

[35] Financial Services - Information Sharing and Analysis Center, www.fsisac.com.

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

[37] G. Guest, A. Bunce, L. Johnson, How many interviews are enough? an experiment with data saturation and variability, Field Methods 18 (1). doi:10.1177/1525822X05279903.

[38] L. Munson, Massive cyber attack on oil and energy industry in Norway, Sophos – nakedsecurity (August 2014).

NTNU

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Telematics

To whom it may concern,

Statement of authorship on joint publication to be used in Maria B. Line's PhD thesis

(Cf. NTNU PhD regulations § 7.4, section 4 and dr.philos regulations § 3, section 5)

This statement regards the following joint publication:

> Line, M. B., Tøndel, I. A., Jaatun, M. G.: *Does size matter? Information security incident management in large and small industrial control organizations,* submitted to International Journal of Critical Infrastructure Protection.

Maria B. Line planned and carried out the interview study described in this publication. She performed the data analysis and was the lead author, writing a major part of the paper.

I hereby confirm that the doctoral candidate's contribution is correctly identified above, and I consent to Maria B. Line including it in her PhD thesis.

Trondheim, 23.04.2015,

Inger Anne Tøndel

Inger Anne Tøndel

Martin Gilje Jaatun

PAPER 8

Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?

Maria B. Line, Ali Zand, Gianluca Stringhini, and Richard A. Kemmerer

2nd Smart Energy Grid Security Workshop (SEGS) 2014, Phoenix (AZ), USA.
ISBN 978-1-4503-3154-8. DOI: 10.1145/2667190.2667192

©2014 ACM. Included here by permission.

Is not included due to copyright

PAPER 9

Understanding Collaborative Challenges in IT Security Preparedness Exercises

Maria B. Line and Nils Brede Moe

International Conference on ICT Systems Security and Privacy Protection (IFIP SEC) 2015, ISSN 1868-4238, Hamburg, Germany.

Understanding Collaborative Challenges in IT Security Preparedness Exercises

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

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

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

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

1 Introduction

Preparing for information security incident management requires training. Basic structures such as well documented procedures and clear definitions of roles and responsibilities need to be in place, but during an incident, there is no time to study documentation in order to figure out the most appropriate response strategies; involved personnel needs to be well trained and well experienced, and hence able to make the right decisions under pressure [1]. Wrong decisions may cause the incident to escalate and lead to severe consequences.

The electric power industry is currently implementing major technological changes in order to achieve smart grids. These changes concern new technologies, higher connectivity and more integration, which increase the attack surface and the potential consequences of attacks [2]. At the same time, current threat reports show that targeted attacks are on the rise, and critical infrastructures are attractive targets [3]. However, recent studies of the electric power industry show that preparedness exercises for IT security incidents are not commonly performed [4, 5] though guidelines exist for how to plan and perform such exercises [6, 7]. Reasons for not performing such exercises seem to relate to their perception of the probability of being attacked and their understanding of potential threats and consequences, and that more pressing tasks receive higher priority. Still, personnel from both the IT staff and the industrial control staff express confidence in their organization's incident response capabilities.

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

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

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

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

2 Background

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

2.1 Tabletop exercises

Tabletop exercises prepare personnel for responding to an emergency situation. They allow for discussions of roles, responsibilities, procedures, coordination, and decision-making, and are a reasonably cost-efficient way of reviewing and learning documented plans and procedures for incident response. Tabletop exercises are usually performed in a classroom without the use of any specific equipment. A facilitator presents a scenario and initiates the discussion. According to the National Institute of Standards and Technology (NIST), a tabletop exercise should consist of the following four phases; Design the event by identifying objectives and participants, Develop the scenario and guides for the facilitator and the participants, Conduct the exercise, and Evaluate by debriefing and identifying lessons learned [6]. As a training method it suffers from the weakness that it does not provide practical demonstrations of the effects of an incident or the emergency management's true response capabilities [9].

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

2.2 Coordination in preparedness exercises

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

Further, responding to an IT security incident is creative work, as there might not be one correct solution and a number of both uncertainties and interdependencies need to be taken into account. In creative work progress towards completion can be difficult to estimate [15] because interdependencies between different pieces of work may be uncertain or challenging to identify. This makes it difficult to know who should be involved in the work, and whether there is a correct order in which parties should complete their own specialized work [14]. Further, in creative work it is essential to improve the knowledge transactions between team members. This is captured in a transactive memory system (TMS), a shared cognitive system for encoding, storing and retrieving knowledge between members of a group [16]. TMS can be understood as a shared understanding of who knows what and also on the degree to which individual knowledge sets are differentiated.

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

To handle a crisis, not only does the team need to coordinate their work; they also need to take decisions together and be responsible for managing and monitoring their own processes and executing tasks, i.e they need to be able to self-manage [19].

3 Method

Since the goal of this research was to explore and provide insight into challenges experienced during IT security preparedness exercises, it was important to study such exercises in practice. We designed a holistic multiple case study [20] of three IT security preparedness exercises in three different organizations. According to Yin, case studies are the preferred research strategy when a "question is being asked about a contemporary set of events over which the investigator has little or no control" [ibid p. 9]. In the following, we present the scenario used, the organizations studied, and how data collection and analysis were performed.

3.1 Scenario

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

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

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

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

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

3.2 Case Context

The three organizations in our study are Norwegian Distribution System Operators (DSOs) and they are among the ten largest DSOs in Norway. For organizations A and B, this was their first execution of such a collaborative exercise for IT security. Organization C had performed a similar exercise once before, and the Emergency Management Team performs preparedness exercises regularly for a variety of incident types. In the following, we present the organizations and how each of them set up their exercise, as well as all participants and their number of years of experience in the organization.

Organization A. Three groups of personnel were represented in this exercise: IT operations, industrial control systems, and network infrastructure. Nine participants were present, including the Preparedness Coordinator[4], a representative from external supplier of SCADA systems, and the facilitator, cf. Table 1.

Table 1. Participants in organization A

Role	**Exp.**
IT production manager	5
IT security coordinator	25
Fiber networks manager	>20
Senior engineer, fiber networks	5
Control systems manager	20
Special advisor, remote control units	>30
Service engineer, supplier of control systems	>30
Emergency preparedness coordinator	>30
IT security coordinator for control systems (facilitator)	28

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

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

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

Table 2. Participants in organization B

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

Organization C. Twelve employees took part in the exercise, cf. Table 3. Five belonged to the Emergency Management Team and were called for when their presence was needed. One person facilitated the exercise in close collaboration with the IT security coordinator.

Table 3. Participants in organization C

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

3.3 Data collection and analysis

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

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

4 Results

The three organizations carried out the preparedness exercises according to generally recommended NIST practices. Plans and goals of the exercise were established in advance, and they all discussed the five phases of the scenario. While the three organizations used the same scenario and main agenda for the exercise, they all had diversity in goals and the number and types of participants. Our observations are hereby presented, as characterized by the following descriptions:

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

4.1 Knowledge exchange and process improvement

In organization A the IT security coordinator for control systems planned and facilitated the exercise. He presented his goals for the exercise in the beginning: *knowledge exchange across organizational boundaries, obtaining a common understanding of what is technically possible in todays' systems, identifying technical and organizational improvements, and ideas for future exercises.* The participants were seated around one big table. The scenario was already known to two of the participants; the fiber networks manager and the emergency preparedness coordinator; as they had participated in this exact same exercise the week before in a different context. This was the only organization that included one participant from their supplier.

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

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

One important insight obtained was that they would not be able to relate the event in the third phase to the two events that occurred three months earlier. Their main priority is usually to get the systems back to normal operations, while understanding *why* the incident occurred typically receives less focus, if any. A number of improvements were identified, regarding both technical and organizational aspects, in order to strengthen the response capabilities for information security incidents affecting complex IT and control systems.

4.2 Cross-functional self-managing groups

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

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

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

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

The evaluation showed that the participants were overall satisfied with the exercise. They appreciated the opportunity to meet and get to know colleagues from other parts of the organization and to get insight into their areas of responsibilities and knowledge. The participants would have liked to have more time than 20 minutes for discussions for some of the phases. Furthermore, they lacked the opportunity to hear how the other groups had solved the problems. A separate meeting for this was arranged a couple of weeks later. One participant suggested they use the existing preparedness plans and procedures actively during such an exercise. The group observers found the thorough evaluation process to be very valuable, and they saw it as an advantage that it was lead by an external (one researcher) as it made the participants put extra effort into contributing.

4.3 Involvement of Emergency Management Team

In organization C the exercise was planned by the IT security coordinator and a facilitator from the communications department. The goal of the exercise was awareness raising and practice in responding to IT security incidents that occur in the control systems. The participants were seated around one big table. Five representatives from the Emergency Management Team were present during the introduction. Three of them left the room when the scenario was presented, while two chose to stay as passive observers. The intention was that the complete Emergency Management Team should be called for at a later phase of the scenario, when the seriousness of the incident required them to be involved, in order to resemble a realistic situation. They were called for twice.

When the first phase of the scenario was presented, the IT operation manager quickly claimed ownership of the incident. He said that he would be the one to get the first alert, and that he would be the one to initiate analyses and reporting to other stakeholders in the organization. One issue that was thoroughly discussed, was the reporting from IT to the control room: when would that be done, if at all; is this relevant information for the control room staff; and is this reporting line documented. This was identified as a lack in the documented procedures when one participant checked these during the discussion. The group still knew who to contact. Another issue that received a lot of attention, was the question of shutting down the control systems. The IT operation manager would recommend this at the stage where the control room supplier calls and wants to install a security patch in the control systems (phase two), as he was worried about the malware infections spreading further into the systems. The control system manager on the other hand claimed that shutting down the control systems has extensive financial consequences for the operations, as manual operations are expensive. The Emergency Management Team decided to shut down the control systems in the fourth phase of the scenario.

During the evaluation it was agreed that such an incident would pose a great challenge for the organization. They still concluded that the situation was resolved satisfactorily in this exercise, and that they would be able to maintain power production and distribution by manually operating power stations. The facilitators felt that relevant assessments and decisions were made, and that the Emergency Management Team was involved at the right points in time. The Emergency Management Team contributed with thorough analyses and unambiguous decisions.

5 Discussion

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

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

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

Having one goal only. For a team to have good performance and to be able to effectively solve a complex problem, they need shared understanding of the team goals [21]. Having several goals for the exercise might lead to the individual members heading towards different goals. In organization A the team focused on solving the given problem while the facilitator was just as focused on knowledge sharing and fruitful discussions. As a consequence they had problems staying focused during the exercise. The main goal of an exercise should be to solve the problem, while additional goals may rather be aimed for during the evaluation afterwards, as was done in organization B.

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

Enabling self-management and growing team knowledge. For a team to solve a crisis and make good decisions it needs to be able to self-manage. Members of self-managing teams share decision authority jointly, rather than having a centralized decision structure where one person makes all the decisions, or a decentralized decision structure where team members make independent decisions. Organization A had problems self-managing as two persons made most of the decisions. It was later concluded that only a few of the team members would participate in a real situation. The others should have been present as observers to distinguish between who are part of the team and who are not.

Enabling self-management further requires the group to have the necessary competence; otherwise the group will be training for solving the problem without having the necessary competence available. However, because handling incidents is creative work, it might be challenging to identify everyone that should be present in the training up front. One of the teams in organization B clearly suffered from the lack of competence, and both organizations B and C lacked personnel from their external suppliers. The training outcome would have been better with the right personnel present.

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

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

Availability of personnel. Business runs continuously and might require sudden and unforeseen actions, which in turn might cause personnel to cancel their presence in the exercise. This will affect the group composition as happened in organization B, where last minute changes led to the lack of one type of competence in one of the groups. Further, members of management groups tend to have little time for exercises, but their presence is needed to have realism to the exercise. Limiting the time spent on exercises would most likely make it easier for key personnel to participate. All organizations experience turnover. Hence, sudden absence of critical competence might be experienced during a real-life incident as well.

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

Time management. Having 20 minutes for discussing each phase was perceived as too short for some, while sufficient for others, depending on both the participants and the complexity of the given problems. Creating a time-pressure for making quick decisions was understood as making the exercise more realistic. Still, according to FEMA [9] it is wise to take the time to resolve problems. A facilitator needs to balance the amount of time spent on the different phases based on the progress and how well the team performs. Further, making time for thorough reflections after the exercise is important to improve the benefits of the exercise, as was also recommended by NIST [6]. Both organizations A and B spent 60-70 minutes on such reflections and stated that one large benefit was that of having an external facilitator for this, as the participants clearly put more effort into contributing than they would usually do during internal evaluations. A similar evaluation was planned for organization C, but they ran out of time and did not prioritize a thorough evaluation after the exercise. A short around-the-table discussion was performed.

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

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

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

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

Organization C seemed to succeed with their model where the team called for the Emergency Management Team when severity of the incident required them to. In organization C the IT personnel wanted to shut down the control systems quite early, due to their fear of malware infections; the control room manager wanted to wait, due to high costs of manual operations. These costs were compared to the consequences of an uncontrolled breakdown. We found that priorities among different parts of the organization vary, which supports the need for collaborative exercises and practicing joint decision-making, at the same time as different authority levels come into play.

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

6 Concluding remarks and future research

For industrial control organizations to withstand and/or successfully respond to attacks, personnel from different parts of the organization need to collaborate: IT, control systems, control room, networks/infrastructure, and business representatives. These groups of personnel do not have a tradition for collaborating with each other, as industrial control systems used to be isolated from administrative IT systems. A holistic view of the incident response process is needed so that the whole organization is included in training, as it would be during a real emergency situation.

There are many ways to conduct preparedness exercises. Therefore organizations need to both optimize current exercise practices and experiment with new ones. Regardless of how the exercises are conducted, there are a number of challenges to be aware of, as identified in our study. Functional exercises should be performed as a supplement to tabletop exercises in order to improve the operational capabilities as well.

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

Acknowledgments.

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

References

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

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

NTNU

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Telematics

To whom it may concern,

Statement of authorship on joint publication to be used in Maria B. Line's PhD thesis

(Cf. NTNU PhD regulations § 7.4, section 4 and dr.philos regulations § 3, section 5)

This statement regards the following joint publication:

> Line, M. B., Moe, N. B.: *Understanding Collaborative Challenges in IT Security Preparedness Exercises*, in Proceedings from the International Conference on IT Systems Security and Privacy Protection (IFIP SEC), May 26-28 2015, Hamburg, Germany.

Maria B. Line planned and carried out the observation study described in this publication. She performed the data analysis and was the lead author, writing a major part of the paper.

I hereby confirm that the doctoral candidate's contribution is correctly identified above, and consent to Maria B. Line including it in her PhD thesis.

Trondheim, 2.3.2015

Nils Brede Moe

Nils Brede Moe