UNDERSTANDING INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICES

A CASE STUDY IN THE ELECTRIC POWER INDUSTRY

UNDERSTANDING INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICES

A CASE STUDY IN THE ELECTRIC POWER INDUSTRY

Thesis for the degree of philosophiae doctor

MARIA BARTNES LINE

Department of Telematics
Norwegian University of Science and Technology
April 2015

"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

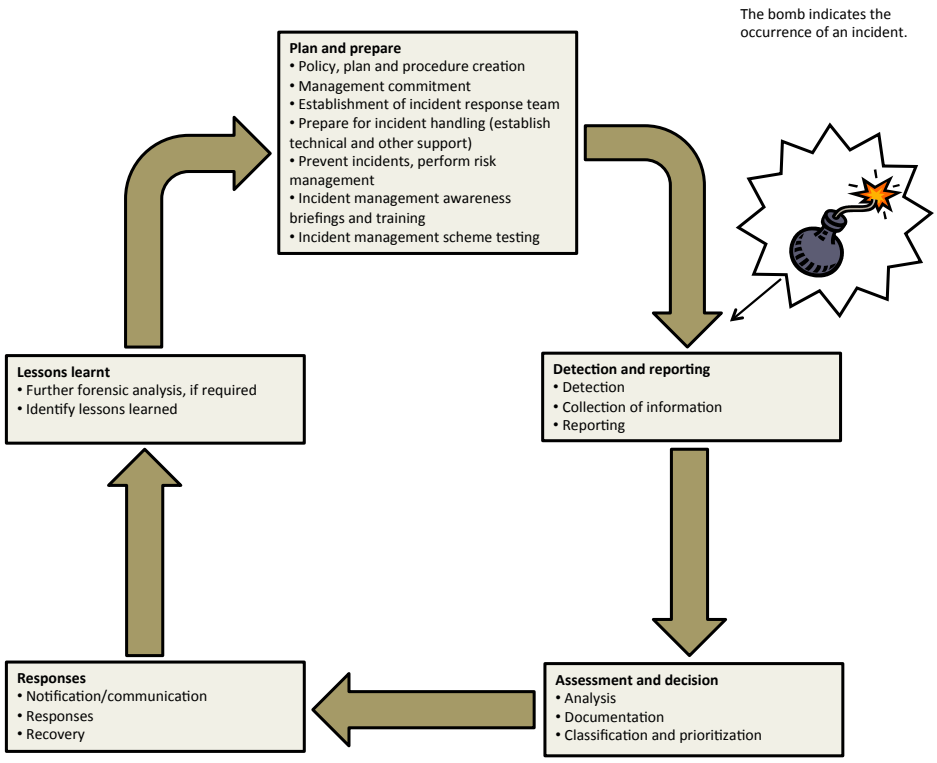

Figure 1: The information security incident management process (ISO/IEC 27035 [1]).

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.

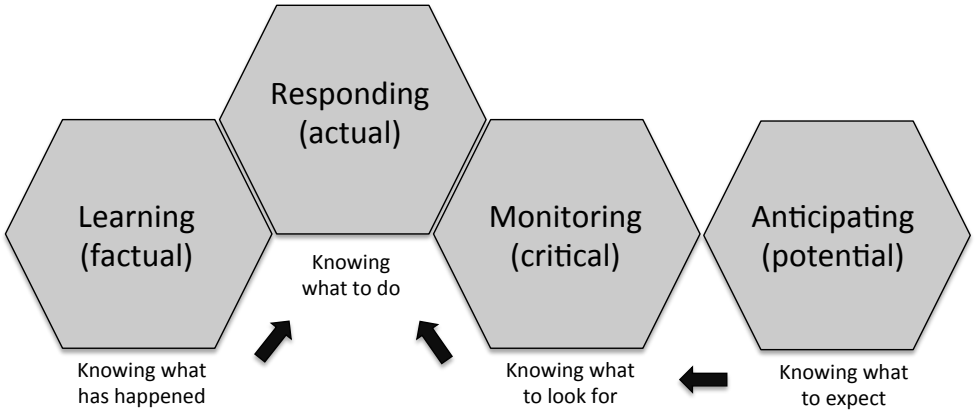

Figure 2: The four basic abilities of resilience [2].

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.

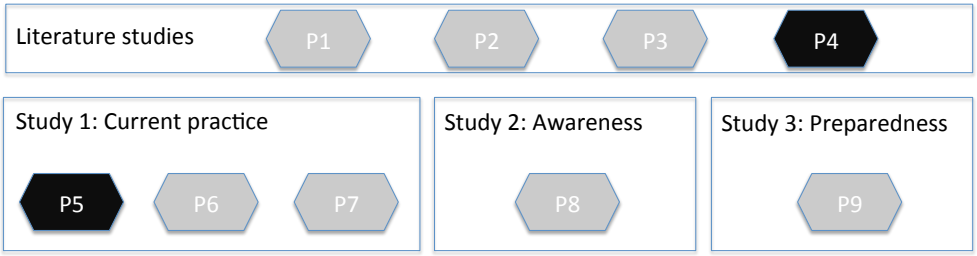

Figure 3: The studies performed and the resulting papers. All papers contribute to both research questions, except from P4 and P5, which address RQ 2 only; thus colored differently than the others.

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

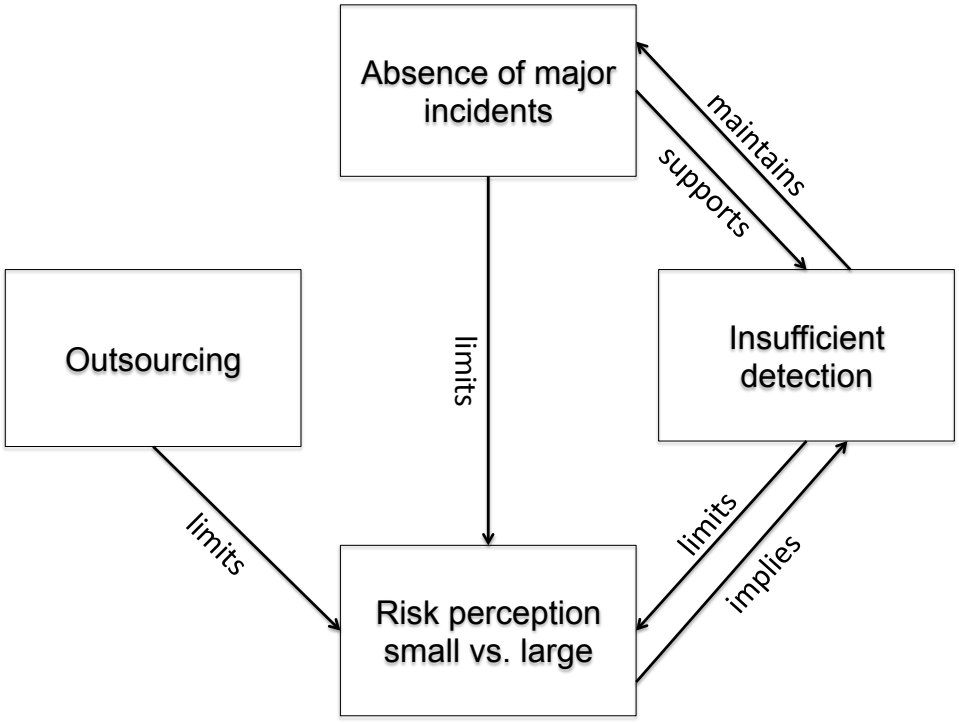

Figure 4: Key findings regarding current incident management practices (RQ1) and how the findings affect each other.

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.

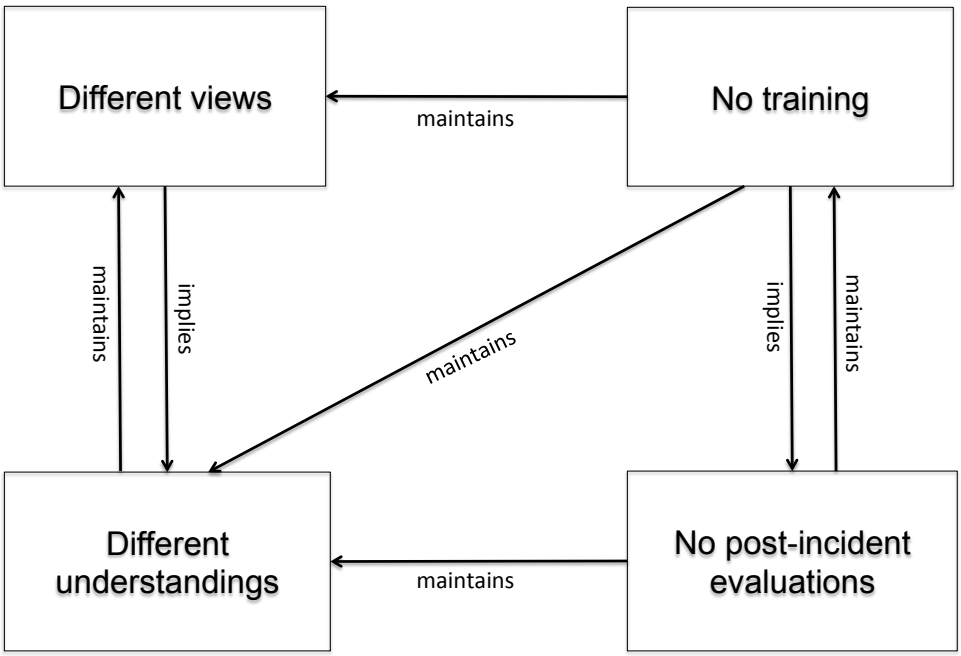

Figure 5: Key findings regarding challenges for improving incident management practices (RQ2) and how the findings affect each other.

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

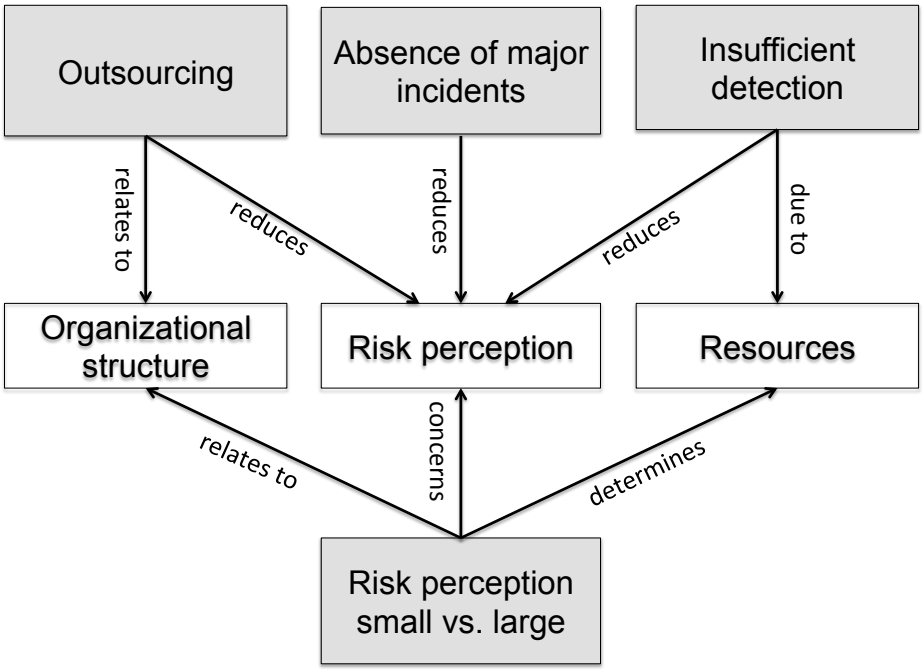

Figure 6: Key findings for RQ 1 relate to the following factors: organizational structure, risk perception, and resources.

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

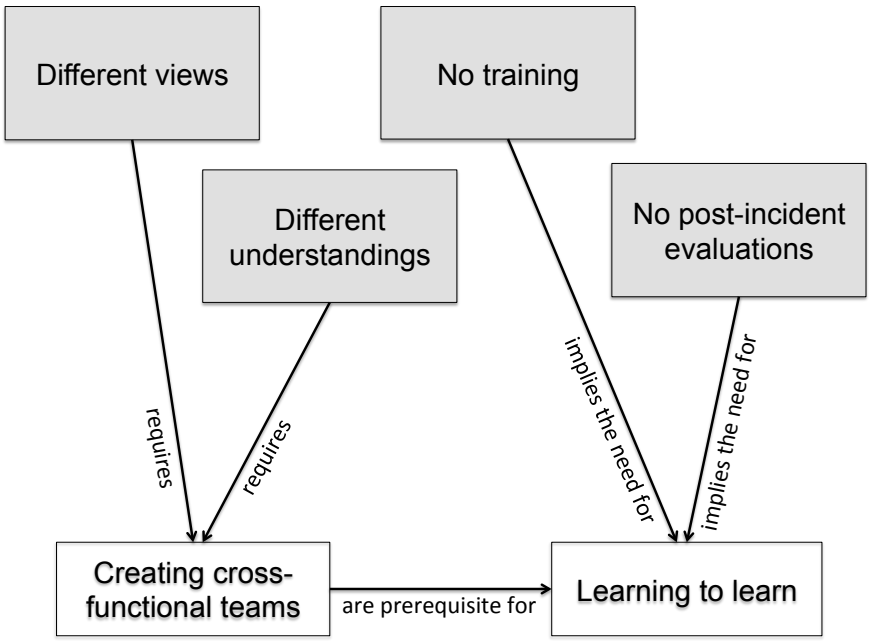

Figure 7: Key findings for RQ 2 sum up to the need for creating cross-functional teams and learning to learn, which are challenges for improving incident management practices.

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

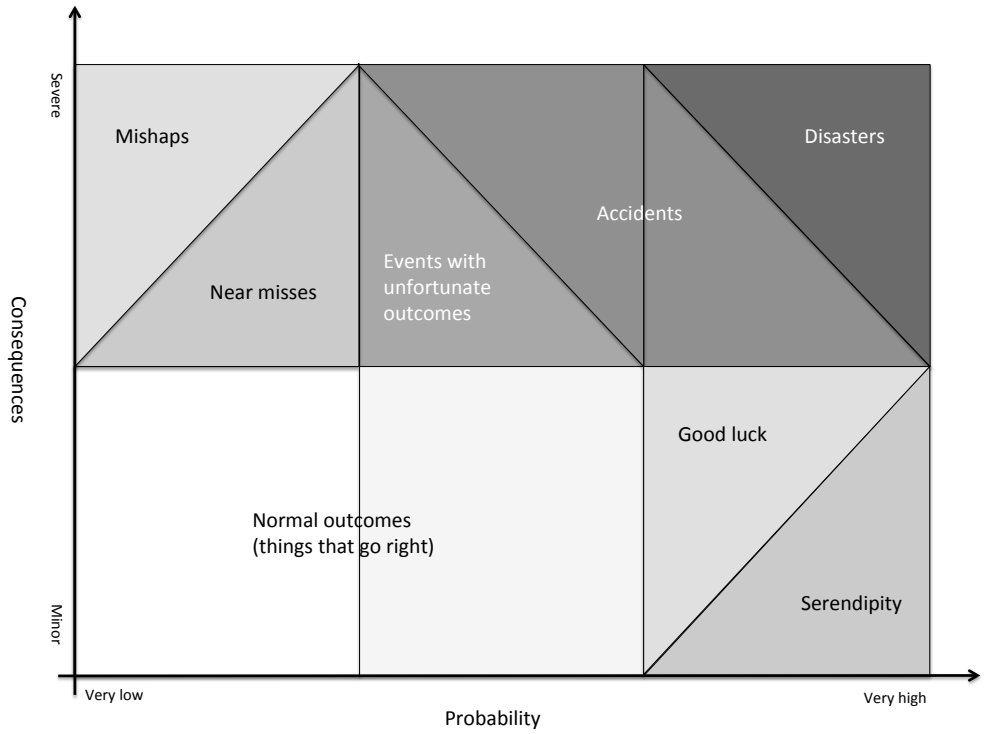

Figure 8: Risk matrix (slightly revised from Hollnagel [2]).

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		