NTNU
Norwegian University of
Science and Technology

The Challenges of Performing IT Security Preparedness Exercises in Organizations

Kine Johnsrud

Master of Science in Communication Technology
Submission date: January 2016
Supervisor: Karin Bernsmed, ITEM
Co-supervisor: Maria B. Line, SINTEF

Norwegian University of Science and Technology
Department of Telematics

Title: The Challenges of Performing IT Security Preparedness Exercises in Organizations

Student: Kine Johnsrud

Problem description:

Information security incidents can occur in any organization, and to be prepared it is important to practice. However, designing practical and functional exercises are not prioritized by the industry, although this would greatly contribute to improved incident management processes.

Earlier research have revealed prominent challenges for organizations on how they perform information security incident management in practice [1], and proposed a number of recommendations. One of the most important recommendations is to perform rehearsals (exercises) to gain experience for the employees. Other recent research has mapped out the challenges of performing tabletop exercises for IT security incidents [2], and how these challenges could affect a real-life incident response process.

In this master's thesis, these findings will be used as a basis to further explore the practical challenges and effects of performing IT security preparedness exercises. The main goal of this thesis is to explore how organizations gain experience from performing information security preparedness exercises.

A suitable basis for discussing the effect and effectiveness of preparedness exercises will be to survey to what extent lessons learned from one exercise are implemented in future exercises, and the challenges that exist in achieving learning from exercises.

This thesis will build upon the aforementioned research studies, consisting of both empirical studies as well as literature research. In order to answer the research questions at hand, new specific information will be gathered from relevant organizations.

[1] C. Hove and M. Tårnes, "Information security incident management – an empirical study of current practice," Master's thesis, NTNU, 2013.

[2] M. B. Line and N. B. Moe, "Understanding collaborative challenges in it security preparedness exercises," in ICT Systems Security and Privacy Protection. Springer International Publishing, 2015.

Responsible professor: Karin Bernsmed, ITEM

Supervisor: Maria Bartnes, SINTEF

Abstract

Organizations can take measures to secure their data to the best of their knowledge, but it is impossible to secure an organization 100 % against attacks and incidents. This calls for the need to handle the incidents as they occur, and to do so successfully one needs to be prepared. That is why it is important to study if, how, and why organizations perform preparedness exercises. In this study the focus was on the challenges and effects of performing information security related preparedness exercises.

The research was conducted as a case study where three Norwegian distribution system operators (DSOs) and two Norwegian preparedness exercise facilitators were interviewed. The study also includes a retrospective on an IT security preparedness exercise the three DSOs performed in the fall of 2014, and 14 of the participants were also interviewed. A background study of relevant material is also included.

The findings from this study indicates that the organizations have improved on some challenges found in earlier studies, but that there is still a way to go. The findings indicate lack of use of definitions from the guidelines, and some lack of proper reporting mechanisms. Organizations have gotten better at collaboration and communication, but there is room for improvement. Performing IT related exercises are challenging due to time and resource restrictions, and technical challenges. Exercises and information security might not be prioritized by the management, and the organizations have some learning difficulties. The most important finding from this thesis is the lack of measured effect from exercises, which makes it hard to put an actual value on performing exercises versus the potential harm of letting be.

Finally, some recommendations for organizations to get better at performing exercises and learning from exercises were provided. The recommendations are: to follow the established standards and guidelines, to set goals and measure them, to perform continual and consecutive exercises, to take actions for improving intra-organization communication and collaboration, to implement an organizational learning framework and apply learning techniques, and lastly; to learn from, or use, external exercise facilitators.

Sammendrag

Organisasjoner kan gjøre tiltak for å sikre sine data etter beste evne, men det er umulig å sikre seg 100 % mot angrep og andre hendelser. Dette skaper behoved for å håndtere hendelser fortløpende, og for å gjøre dette trenger man å være forberedt. Derfor er det viktig å undersøke om, hvordan og hvorfor organisasjoner utfører beredskapsøvelser. I denne studien var fokuset på utfordringene og effektene ved å utføre informasjonssikkerhetsrelaterte beredskapsøvelser.

Forskningen ble gjennomført som en case-studie hvor tre norske kraftselskaper og to norske beredskapsøvelsesfasilitatorer ble intervjuet. Studien inkluderer også et tilbakeblikk på en IT-sikkerhetsøvelse disse tre kraftselskapene utførte høsten 2014, og 14 av deltagerne har også blitt intervjuet. En bakgrunnsstudie av relevant materiale er også inkludert.

Funnene fra denne studien tyder på at kraftselskapene har forbedret seg på noen punkter som ble avdekket i tidligere studier, men at de fortsatt har en vei å gå. Funnene tyder på manglende bruk av definisjoner fra retningslinjene, og noe mangel på gode rapporteringsrutiner. Organisasjonene har blitt bedre på samarbeid og kommunikasjon, men også her er det rom for forbedring. Å utføre IT-relaterte beredskapsøvelser viser seg å være utfordrende grunnet manglende tid og ressurser til overs, og teknologiske utfordringer. Beredskapsøvelser og informasjonssikkerhet blir kanskje ikke prioritert av ledelsen, og organisasjonen møter dermed på noen lærevansker. Det viktigste funnet fra denne avhandlingen er mangelen på målt effekt av øvelser, hvilket gjør det svært vanskelig å sette en reell verdi på det å utføre øvelser i forhold til potensielle skader av å la være.

Til slutt er det gitt noen anbefalinger til organisasjonene for å bli bedre til å utføre beredskapsøvelser og å lære fra øvelser. Disse anbefalingene er: å følge etablerte standarder og retningslinjer, sett etterprøvbare mål og mål disse, utfør beredskapsøvelser jevnlig og kontinuerlig, iverksett tiltak for å forbedre organisasjonens interne kommunikasjon og samarbeid, ta i bruk et organisatorisk læringsrammeverk og anvend læringsteknikker, og til slutt; lær fra, eller bruk, eksterne øvingsfasilitatorer.

Preface

This master's thesis is submitted to the Norwegian University of Science and Technology (NTNU) as the final part of a five-year Master of Science in Communication Technology program at the Department of Telematics (ITEM).

I would like to thank my supervisor Maria Bartnes and responsible professor Karin Bernsmed for valuable guidance and feedback during the course of this project. I would also like to thank all the participants from the electric power industry, and the professional exercise facilitators. I would also like to thank Combitech for the contribution of statistical data.

Trondheim, January 12th, 2016

Kine Johnsrud

Contents

Appendices

List of Figures

List of Tables

List of Acronyms

CERT Computer Emergency Response Team.

DSO Distribution System Operator.

ENISA European Union Agency for Network and Information Security.

HSEEP Homeland Security Exercise and Evaluation Program.

ICS Industrial Control System.

ICT Information and Communications Technology.

IRT Incident Response Team.

ISIM Information Security Incident Management.

ISIRT Information Security Response Team.

ISMS Information Security Management System.

ITEM Department of Telematics.

NIST National Institute of Standards and Technology.

NSD Data Protection Official for Research.

NSM Norwegian National Security Authority.

NTNU Norwegian University of Science and Technology.

NVE Norwegian Water and Energy Directorate.

PST The Norwegian Police Security Service.

SCADA Supervisory Control and Data Acquisition.

Chapter 1 Introduction

"One of the most important parts of incident response is also the most often omitted: learning and improving" – National Institute of Standards and Technology (NIST) [GKK04]

Information security incidents can occur in any organization, and training is imperative in order to be prepared when incidents occur. Statistics from the Norwegian National Security Authority (NSM) shows that there were reported 88 serious incidents in 2014 [Sik14, Sik15], and that there is a large gap between the number of reported incidents and the number of actual incidents – while 5 % of the participating organizations report that they are exposed to hacking, sensor data shows that the correct answer is closer to around 50 %. It is interesting to see if and how organizations learn from exercises and real incidents, as it is a necessary measure to take in order to be better prepared when real incidents occur.

1.1 Motivation

It is important to make the industry see the value in performing exercises. There is a rapid increase in the use of digital solutions in all sectors, and large amounts of sensitive data is stored digitally [TE14]. The number of potential threats and the level of consequence increase accordingly. Organizations today depend and rely on their IT-systems. No matter the amount of security measures taken, no IT-infrastructure will ever be bulletproof. Weakness in information security is the most prevalent reason for data breaches [Mar14]. Therefore, it is vital to know how to respond when security breaches occur. Threat reports show that targeted attacks are on the rise, and critical infrastructure are amongst the most attractive targets [BBF+14]. Research reveals that Distribution System Operators (DSOs) rarely perform information security preparedness exercises [LTJ14], despite the fact that guidelines created by the authorities[1] exists [ulosmN13]. A reason for this can

[1] Norwegian Water and Energy Directorate (NVE)

be the considerable gap between reality and the perception of threat probability and level of consequences.

"By failing to prepare, you are preparing to fail." – Benjamin Franklin

An information security incident management consists of different phases; planning and preparation, detection and reporting, assessment and decision, responses, and lessons learned [ISO11b]. This study focus on the last part of the incident management process – lessons learned. How do organizations gain experience from an information security preparedness exercise? What are the challenges in achieving learning from exercises? To what extentss are lessons learned from one exercise implemented in future exercises? Do processes and policies get updated and improved based on exercises? What about smaller incidents?

Security threats evolve faster than their countermeasures, leaving a gap between the severity of threats and security measures. By performing exercises, learning from exercises, and even learning from smaller incidents, the gap can be closed. To perform preparedness exercises is to lay the groundwork for an organization's personnel in responding to situations out of the ordinary. Information security preparedness exercises leads to better response capabilities to information security incidents due to practical collaborative training [LM15]. It can be argued that improving the exercises leads to strengthened response capabilities.

1.2 Objectives

I aim to draw attention to and increase the awareness around how learning from exercises and learning from smaller incidents make organizations more robust against today's information security threats. The purpose of this thesis is to assess the importance of continually conducting exercises and gain experience from exercises.

Two different approaches is chosen in order to look at the exercise learning experience from different perspectives; from the participants point of view, and the point of view of individuals performing exercises as a service to other organizations seeking external help.

The purpose of this research is to:

- Explore the practical challenges and effects of performing information security preparedness exercises
- Explore how organizations gain experience from performing information security preparedness exercises

- Survey to what extent lessons learned from one exercise are implemented in future exercises, and
- Explore the challenges that exists in achieving learning from exercises.

1.3 Scope and Limitations

We have collected information from three Norwegian DSOs and two experienced exercise facilitators, by conducting textual interviews with some follow-up correspondence. We have also performed an extensive background study of information security incident management, preparedness exercises, organizational learning, and the concept of learning to learn. The areas of incident management, preparedness exercises, and organizational learning are broad and extensive. This thesis focuses on an approach where organizational learning is used to improve an organizations incident management, by means of preparedness exercises. If and how learning is performed, and the effect of said learning, is the top priority of this thesis.

Generalization is not possible due to the number of participants, and the results needs to be regarded in its context – Norwegian DSOs and Norwegian exercise facilitators. We have chosen an in-depth case study as opposed to a quantitative study with volume in number of answers. This is both more doable due to the time restrictions of a master's thesis, and it can also be argued to be the more favorable approach in order to get a deeper understanding of how individuals perceive security, exercising, and learning.

1.4 Outline

In the following chapter, the research method used and why exactly that method is chosen is explained. In Chapter 3 the studied background material is elaborated on, including definitions, information security incident management, planning and preparation, preparedness exercises, organizational learning, and learning to learn. Following is a representation of the case, and the participants in this study in Chapter 4. Chapter 5 presents the results from our interview inquiries, the results are discussed in Chapter 6, and the thesis is concluded in Chapter 7. The interview guides are presented in Appendix A and Appendix B.

Chapter 2 Methodology

In the following, we present how the research method was chosen, and elaborate on the research method used. Further, we explain how data collection was performed.

2.1 Choice of Method

As the goal of this research was to explore the challenges and effects of performing information security preparedness exercises, retrospective information gathered from exercise participants and exercise facilitators after the execution of an exercise is of great relevance. A background study has been performed in order to explore the challenges and recommendations related to performing exercises and learning from exercises found by other researches.

A book on case study research by Robert K. Yin [Yin13] has an overview of criteria that can be used to determine the appropriate research method. The criteria are: 1) form of research question (how, what, why, ..), 2) does the study require control of behavioral events, and 3) does the study focus on contemporary events. Based on this overview, it is evident that this study was best suited as a case study; using multiple organizations to answer one big, in-depth question. This case study is conducted with an extensive background study and qualitative interviews.

2.2 Qualitative Research

Qualitative research is carried out when one wishes to understand meanings, describe, and look at experience, ideas, values and beliefs. Research looking at learning styles and approaches to study, which are described and understood subjectively, will benefit from qualitative research. Conducting interviews is the most common way to perform qualitative research.

This thesis performs qualitative research based on relatively few informants focusing on in-depth information. The information is gathered from the same participants as from a study this thesis builds upon [LM15], with added perspective from two individuals giving another angle on the case – facilitation as opposed to participation.

There are several potential pitfalls with this type of research. Some of these are worth mentioning and keeping in mind when performing such case study. Some of the pitfalls presented by Myers and Newman [MN07] are: artificiality of the interview, lack of trust, lack of time, level of entry, elite bias, hawthorne effects, constructing knowledge, ambiguity of language, and that interviews can go wrong. The challenges encountered during this study is described in Section 2.4 and in Section 6.4.

2.2.1 Background Study

The first step in this research was to study a broad spectrum of background material to gain sufficient knowledge to propose research questions and perform a study. Standards and guidelines for incident management have been studied, as well as standards and procedures for performing preparedness exercises. A study of the concept of organizational learning and learning to learn has also been conducted to better understand what mechanisms an organization uses to learn, and how individuals learn. Related research has been studied, where challenges with incident management, performing exercises and collaboration has been uncovered, and recommendations have been proposed. This background has laid the groundwork for my study of if and how organizations learn from exercises, and what the challenges are.

2.2.2 Interviews

The interview remains the most common method of data gathering in qualitative research. The main objective of qualitative interviews is to see the research topic from the interviewee's perspective and understand how and why they got that particular perspective [CS04]. To meet this objective, qualitative interviews often focus on specific situations and experiences made by the interviewee.

The process of constructing qualitative research interviews can be split into four parts [CS04]: 1) defining the research question, 2) creating the interview guide, 3) recruiting participants, and 4) carrying out the interviews. This is somewhat similar to our process, a major difference however is that the participants were decided before interview questions were created. Due to the nature of how the interviews were carried out, some iteration was also needed. A revised process for constructing and conducting the interviews:

- define the project description
- contact relevant participants
- create interviews based on background studies

– distribute interviews
– interpret the gathered data
– if needed: contact participants for clearance and elaboration

The types of interviews that fit the label of qualitative research is often referred to as "in-depth", "exploratory", "semi-structured", or "un-structured". We performed structured interviews with follow-up questions, and therefore chose to label it as qualitative. The interviewees are encouraged to elaborate and go "off-topic" if necessary. Kvåle defines a qualitative research interview as "an interview, whose purpose is to gather descriptions of the life-world of the interviewee with respect to interpretation of the meaning of the described phenomena" [Kav83]. The goal of any qualitative research interview is to view the research topic from the perspective of the interviewee, and to understand how and why they come to have this particular perspective [CS04].

The interviews in this study were initially performed textually, where the participants received the interview questions by e-mail, and responded by regular mail[1]. No face-to-face interview is conducted due to contributors located outside of reasonable travel distance, and all contact has been by e-mail, telephone and regular mail.

2.3 Participants

Three of the participating organizations are Norwegian DSOs recruited to answer retrospective questions particularly related to a preparedness exercise they all performed in the fall of 2014, on request from the NVE. The exercise was audited by Line and Moe for their research on collaborative challenges in performing IT security exercises [LM15]. We have been able to interview the exercise leader in all three organizations, as well as the exercise participants. The interview guides can be found in Appendix A.

Two other participants were recruited for their interest in information security preparedness exercises, and their employment as facilitators of preparedness exercises for other organizations. They gave another perspective on the challenges of performing exercises, the challenges of making organizations see the value of performing exercises, and the process of evaluating both the exercise in itself and an organizations processes and procedures used during an exercise. The interview questions can be found in Appendix B.

[1] Due to privacy rules set by the Norwegian Data Protection Official for Research (NSD) not allowing anonymous answers to be connected to an e-mail address or IP-address.

2.4 Challenges and Limitations

One of the main challenges of writing a 20-week thesis is the restriction of *time.* All parts of the study from reading up on background material, developing research questions, and creating objectives, to gathering and analyzing data, is affected by restriction of time. It may force the researcher to prioritize, and narrow down the scope. Time is also of the essence when the research requires the researcher to be *reliant on external sources.* External sources have their own priorities, and may push the researchers deadlines for data collection. In an opinion-based study like this, ensuring the *validity of data* can be challenging. Both researcher and interviewee can be tainted by biases.

As participants of this study needs to be anonymous, there is also challenges and limitations of the research due to *confidentiality.* Some of the data collected might be restricted as questions regarding information security are sensitive information for participating organizations. The challenge of obtaining sensitive data to promote research is pointed out by Kotulic et al. [KC04], who recommend focusing on a few selected companies. This can encourage a trusted relationship between the organization and the research, and ease the collection of sensitive data.

Lastly, this is a research of Norwegian companies with Norwegian as work language, and hence the interviews and miscellaneous other contact is performed in Norwegian. There is some challenge related to *translations* between Norwegian and English jargon on the topic of IT, security, preparedness and DSO-specific terms.

Chapter 3 Background

This chapter presents some background information found in the literature. It covers the basic definitions, information security management standards, and how to conduct preparedness exercises. It also discusses the research field of organizational learning, and the important concept of learning to learn. The chapter includes references to and information of related work throughout, and ends with a summary.

3.1 Definitions

This section covers some terms used in this thesis, and terms relevant for the topic at hand. The ISO/IEC 27000 standard [ISO14] presents an overview of relevant definitions, some of them are covered here:

Information security Preservation of confidentiality, integrity, and availability of information. These three concepts are often referred to as the *CIA triad*, as depicted in Figure 3.1.

Information security event Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure controls, or a previously unknown situation that may be security relevant.

Information security incident Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information security incident management Process for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

An **Information Security Management System (ISMS)** consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.

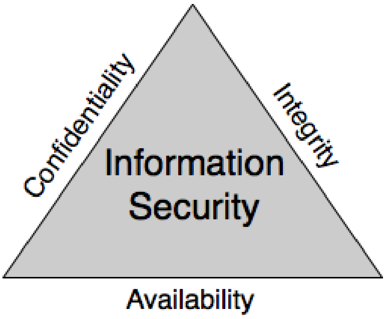

Figure 3.1: The CIA Triad

Information security involves the application and management of appropriate security measures that involves consideration of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing impacts of information security incidents. See information about this term used in this thesis under Section 3.1.2.

A **management system** uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.1.1 IRT and CERT

From ISO/IEC 27035 [ISO11b]: An **Information Security Response Team (ISIRT)** is a team of appropriately skilled and trusted members of the organization that handles information security incidents during their life cycle. Not to be confused by **Computer Emergency Response Team (CERT)**. A CERT mainly focuses on Information and Communications Technology (ICT) incidents. An **Incident Response Team (IRT)** is a team that handles emergency incidents in general, and does not have to be information security specific.

KraftCERT is a CERT that was established in October 2014 by three power companies in Norway after an initiative by NorCERT[1] and the Norwegian Water Resources and Energy Directorate (hereby going by the Norwegian acronym NVE) as a tool to create support for the power industry at large to prevent and handle security incidents. KraftCERT offers services like vulnerability monitoring, threat

[1] NorCERT is a part of NSM that plays a role in preventative work and responses against IT security breaches aimed at vital infrastructure in Norway.

intelligence, detection, incident response, counseling, emergency drills, and training to its members[2].

3.1.2 Information Security and IT Security

IT security is a term that specifies that the security is directly linked to some kind of IT system or network. **Information security** however, is defined as the preservation of confidentiality, integrity, and availability of information in general, and can include incidents like two colleagues talking loudly about confidential information in a public space with bystanders listening in. IT security is therefore a subset of information security, where IT is involved. These two definitions will be used interchangeably in this thesis, as the difference between the two has no relevance for the scope of this project.

3.2 Information Security Incident Management

As long as there is a possibility for information security incidents, there will be need for information security incident management. Both terms are defined in Section 3.1. The ISIM process described in ISO/IEC 27035 [ISO11b] comprise of five phases:

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

The first phase is a continuing, iterative phase that is necessary to offer successful information security incident management. The other four phases are triggered by an actual event, and involve using the established information security management system. The *planning and preparation* phase involves policies, commitment of senior management, management schemes and scheme testing, awareness briefings and training, as well as establishment of an ISIRT (described in Section 3.1). The first phase of the operation that take use of the incident management scheme is the *detection and reporting* phase. It involves detection of an information security event or information security vulnerability, and collection of information and reporting of occurrences related to this. In the *assessment and decision* phase, the information

[2] Information about KraftCERT gathered from the KraftCERT web-page www.kraftcert.no. The CERT is too newly established to have external sources and descriptions.

security event is assessed, and it is decided whether it is an information security incident or not. The *response* phase comprise of forensics analysis and recovery from an information security incident, and when the problem is solved, it is time for the final phase. In *lessons learned* it is time to reflect on the incident, and assess whether the information security incident management scheme worked satisfactorily. Examine whether any changes are needed to existing policies, risk assessment, or the information security management scheme. Potential improvements are then implemented in the new version which then gets included in the next *planning and preparation* phase.

3.2.1 Other ISIM Standards

In this section, a handful of other relevant ISIM standards are mentioned. This is to underscore the high number of respectable guidelines that exist, and that the essence of these guidelines comply with each other.

SANS Incident Handler's Handbook

In SANS[3] Incident Handler's Handbook [Kra11], the incident response team is called CIRT – Computer Incident Response Team. They operate with a six-phase program: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. By and large, it is very similar to the process in ISO/IEC 27035.

NIST SP 800-61 Computer Security Incident Handling Guide

As an answer to the increasing need for incident response capability, NIST released a special publication on computer security incident handling in 2004 [GKK04]. It provides guidelines for incident handling, and for analyzing incident-related data to determine the appropriate incident response.

ENISA – Good Practice Guide for Incident Management

The incident management guide by ENISA[4] is limited to the scope of IT and informations security [eni10]. I.e. incidents that are limited to computers, networks, and the information contained inside this equipment. They choose to differentiate between incident management and incident handling, shown in Figure 3.2. ENISA has also published a "CERT Exercises Handbook" [cer12] containing 22 exercises to help train CERT teams.

[3] SANS Institute is a private U.S company that specializes in information security and cybersecurity training [Kra11].

[4] European Union Agency for Network and Information Security (ENISA) is an agency of the European Union working to improve network and information security i the EU [eni10].

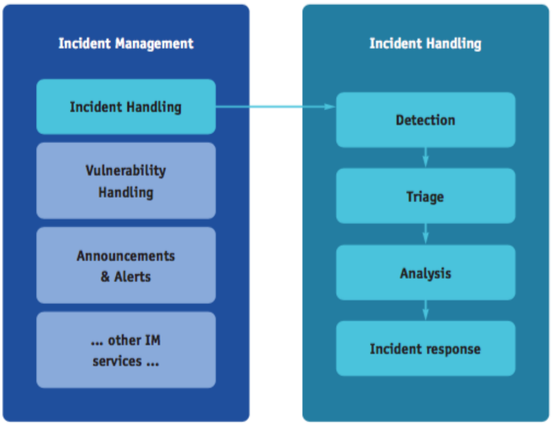

Figure 3.2: Incident management and incident handling clarified [eni10]

3.2.2 Studies of Incident Management in Practice

An empirical study of how organizations perform information security incident management in practice, was conducted in a master's thesis by Cathrine Hove and Marte Tårnes [HT13] in 2013. They performed a case study of organizations by means of qualitative interviews, a document study, and employee surveys. Amongst the prominent challenges and observations were the level of experience, responsibility allocation, and employee involvement. It is stated that by conducting rehearsals addressing various types of incidents, incident handlers will gain experience. They also believe that rehearsals can contribute to revealing grey areas regarding responsibilities, and make incident handlers more suited to determine where incidents originate. Lastly, their research did not show any employee involvement in rehearsals beyond the involvement of incident and crisis handlers, and believe that employees can benefit from being more involved in rehearsals as well.

A bachelor's project executed on assignment from NorSIS[5] explored how incident management is performed in small and medium-sized enterprises [SWF10]. The end product of the project was a guide for incident management targeting this specific audience.They found that half of the participating organizations had incident management policies in place. Most of the organizations had poor training, and little to no implementation of incident management systems. They had unsatisfactory reporting mechanisms, which led to inadequate overview of the number of security events. Most of the organizations performed follow-up after a security event.

[5] The Norwegian Centre for Information Security

3.3 Planning and Preparation

As explained in Section 3.2, the *planning and preparation* phase involves policies, commitment of senior management, management schemes and scheme testing, awareness briefings and training, as well as establishment of an ISIRT. Some studies indicate that this is the phase most often skimped with [LTJ14, MD06], which might lower the execution quality of the following phases of detection, reporting, decision making, and responding.

In a study of planning and preparing performed by Allan McConnell and Lynn Drennan [MD06] four key difficulties in translating planning and preparation ideals to practice were uncovered:

1. Crises and disasters are low probability events, but place large demands on resources, and have to compete against front-line service provision.

2. Contingency planning requires ordering and coherence of possible threats, yet crisis is not amenable to being packaged in such a predictable way.

3. Planning for crisis requires integration and synergy across institutional networks, yet the modern world is characterized by fragmentation across public, private, and voluntary sectors.

4. Robust planning requires active preparation through training and exercises, and such costly activities often produce a level of symbolic readiness which does not reflect operational realities.

These four key difficulties highlight the tension between the “ideals” of crises preparedness and the realities of a real crisis. At the end of this study, they conclude that a conservative tendency in crisis preparedness involve playing down threats, adopting a “can cope” outlook, and being resistant to investing scarce resources in drawing up plans and rehearsing for an event which may never happen. They also conclude that reaching a high level of crisis preparedness is not a “mission impossible” in a practical sense, but that it is certainly very difficult to achieve. This study has a broad scope of types of crises, including nation-wide disasters like hurricanes and terrorist-attacks. However, the concepts of planning and preparation and the challenges involved are the same.

Maria B. Line et. al. [LTJ14] did an interview study and documentation review of six large Norwegian DSOs. This research focused on how planning and preparatory activities for information security incident management performed by organizations depend on successful cooperation between IT systems and ICS[6], and what differences there are between how planning and preparatory activities are performed for IT systems compared to ICS. None of the IT managers or IT security managers reported that they perform regular training exercises where an information security incident creates the basis for the scenario. Reasons given for lack of training: difficult to prioritize, other tasks are given higher priority, training involves a certain cost, real incidents rarely occur, and training might be continuously postponed due to lack of knowledge or experience in performing such exercises. These are the excuses we need to mitigate to make organizations see the value in information security preparedness exercise. This paper concludes that future work should investigate why training for IT security preparedness is more difficult and how knowledge could be transferred from the areas of general emergency preparedness exercises.

3.4 Preparedness Exercises

Preparedness exercises play a huge role in any nations or organizations preparedness program. To be well prepared to respond to any kind of emergency, it is elementary to conduct exercises. For the best possible learning effect, exercises should be performed periodically, with lessons learned from one exercise being implemented in the next.

There are different types of preparedness exercises. The HSEEP [Sec13] has divided exercises into two main categories – discussion-based and operations-based. The following descriptions are retrieved from the HSEEP.

3.4.1 Discussion-based Exercises

Discussion-based exercises include seminars, workshops, tabletop exercises, and games. Discussion-based exercises focus on strategic, policy-oriented issues.

Seminars Provide an overview of authorities, strategies, policies, plans, procedures, protocols, resources, concepts, and ideas. Can be valuable for making major changes to existing plans and procedures.

Workshops Higher participant interaction than in seminars, with focus on achieving or building a product. A workshop should have clearly defined objectives, products, or goals, and should focus on a specific issue.

Table-top exercises Is intended to generate discussions around various issues regarding a simulated, hypothetical emergency. It can be used to rehearse concepts, validate plans and procedures, and enhance general awareness. During

[6] Industrial Control System (ICS) – a general term that engulfs several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems often found in industrial sectors and critical infrastructures (like in the power industry).

a table-top exercise the participants are encouraged to discuss issues in depth, collaboratively examining areas of concern, and solving problems.

Games Is a simulation of events that often requires two or more teams. It can be a competitive environment, using rules, data, and procedures designed to give the illusion of an actual or hypothetical environment. Using games, the consequences of player decisions and actions are explored.

3.4.2 Operations-based Exercises

Operations-based exercises include drills, functional exercises, and full-scale exercises. These can be used to test and validate existing plans, policies, and procedures. They can clarify roles and responsibilities, and identify resource gaps. These require more time and resources than discussion-based exercises do.

Drills A coordinated, supervised activity employed to validate a specific capability or function. Drills are commonly used to validate procedures, provide training on new equipment, or practice on maintaining current skills. Drills can be used to determine if plans can be executed as designed, or to assess whether more training is required. A drill is useful as a stand-alone tool, but a series of drills can also be used to prepare organizations to collaborate in a full-scale exercise.

Functional Exercises Designed to validate and evaluate capabilities and multiple functions. Functional exercises are typically focused on plans, policies, and procedures.

Full-Scale Exercises The most complex and resource-demanding type of exercise. It involves actors from several organizations and domain expertises, and aims to validate all emergency preparedness phases. This is the most life-like training, where you are closest to what an actual emergency incident would be like.

3.4.3 The Exercise Cycle

The HSEEP also presents an exercise methodology, commonly used for planning and conducting individual exercises. The four steps of the exercise cycle is design and development, conduct, evaluation, and improvement planning, as you can see in Figure 3.3. This is similar to the process described in the guide for planning and conducting exercises by the NVE [ulosmN13]. They operate with the four steps; plan, conduct, evaluate, and follow-up. The description of the exercise steps is reproduced from the guide.

In the *planning* phase, the goal is to agree on the overall purpose and goal of the exercise. A planning group is established with representatives from different disciplines, and the organizational assignments are allocated. The exercise scenario

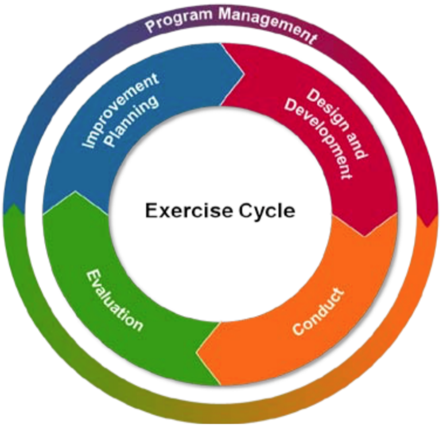

Figure 3.3: The HSEEP Exercise Cycle [Sec13]

is customized for the involved participants and their goal. The exercise should feel relevant and realistic, and should be challenging and give a sense of empowerment.

The *conduction* phase should start with an introductory presentation of the exercise from the exercise leader. The exercise leader leads the exercise, and has the overall responsibility during the exercise. It is desirable he/she stay passive. The person responsible for evaluation should conduct an oral first-impression evaluation shortly after the exercise termination.

The *evaluation* phase is an important and necessary part of an exercise. Experiences can be gathered in an evaluation report, where the focus is success factors, challenges, and points of improvement. The document structure should be as follows; introduction, about the exercise, evaluation, and a follow-up summary.

The *follow-up* phase is about implementing improvement measures identified during the execution of the exercise. When the measures are implemented in the organization and in relevant documentation, it can be useful to conduct a new exercise. The exercise plan overall should also be evaluated, not just the specific scenario.

3.4.4 Norwegian Laws, Regulations and Guides for Emergency Preparedness in the Power Supply Industry

The Norwegian Law of Energy [oe91] together with the Norwegian regulation of power supply emergency preparedness [oe13] provides the overarching framework for organization of the Norwegian power supply. The supervisory responsibility lies with the Norwegian Directorate for Civil Protection[7] and NVE, where the latter has created a supervisory forum that guide and support organizations in preparedness situations. As of 2013 the Norwegian regulation of power supply emergency preparedness includes a demand to perform exercises based on IT security incidents. When Norwegian DSOs refer to “The Preparedness Plan” it is safe to say that they refer to the guide for planning and conducting exercises by the NVE [ulosmN13]. As mentioned, this guide has a similar exercise process as the HSEEP process. This specific guide also contains some examples of DSO specific scenarios in the appendix.

3.4.5 Exercise Facilitators

A facilitator can promote team effectiveness by helping team members learn how to work interdependently in the specific team [Lin15]. It is recommended to include a facilitator to support the team in making joint decisions to develop a shared understanding of who knows what, and to make sure a certain time constraint is upheld during the course of the exercise [LM15]. In the thesis work of M. Bartnes [Lin15] the facilitators had the task of leading their teams through the steps of the exercise, and making sure the discussions were fruitful. The facilitators also had the job of writing down ideas for future improvements regarding procedures and technical measures.

Hackman et al. [HWR$^+$00] specifies a set of process criteria for effectiveness that exercise leaders (i.e. facilitators) can help the participants in. Including the following: 1) *For effort*: Helping participants in minimizing coordination and motivation problems, and building commitment to the group and the group task. 2) *For knowledge and skill*: Helping participants avoid inappropriate weighing different individuals’ ideas and contributions, and helping them learn how to share their expertise to build the group’s repertoire of skills, and 3) *For performance strategies*: Helping members avoid failures in implementing their performance plans, and helping them develop creative new ways of proceeding with the work. There are at three times in a team’s life when participants are likely to be especially open to particular coaching interventions: 1) at the beginning, when a group is just starting to work, it is especially open to interventions that focus on the effort members will apply to their work; 2) at the midpoint, when the group has completed about half of its work, it is especially open to interventions that help members reflect on their performance strategies; and 3) at the end, when the work is finished, learning from their experience, which is the focus of this thesis, and is where the DSO participants are at.

[7] In Norwegian: Direktorat for Samfunnssikkerhet og Beredskap (DSB), www.dsn.no.

3.4.6 Related Work

Maria B. Line and Nils B. Moe presented in 2015 [LM15] a study revealing the collaborative challenges in IT security preparedness exercises. They performed a holistic case study [Yin13] of three distribution service operators (DSOs) performing an IT security preparedness exercise. This is one of the studies this thesis is building on, and the retrospective questions asked to three DSOs about learning from an exercise, is learning from this specific exercise. They argued that the challenges met during an exercise could affect the response process when a real incident occurs, and that by improving the exercises the response capabilities would be strengthened accordingly. The study found the main challenges to be: a) having one goal only, b) enabling self-management and growing team knowledge, c) availability of personnel, d) time management, e) use of existing documentation, and f) involvement of business management.

A qualitative research of computer preparedness exercises was conducted in a specialization project by Ingrid Graffer and Henriette Chiem [GC14]. Based on a background study and semi-structured interview, they came up with a set of recommendations: 1) increase level of collaboration, 2) increase the level of knowledge and competence within the organization, 3) create awareness of the threats related to digital systems, and 4) conduct more computer preparedness exercises. They state that a preparedness exercise will be useless if the participants fail to improve and learn from the exercise, and that these exercises are relatively new to the industry, and to improve them rapidly should be prioritized.

In a study of preparedness exercises initiated by the NVE, a positive attitude towards participating in exercises was found [Gås14]. The study explores preparedness exercises and organizational learning in various industries, including the power industry. It analyses the industry's ability to learn from preparedness exercises initiated by the NVE. The two exercises in question uses incidents related to extreme weather and consequences to critical infrastructure as scenario. These are scenarios the power industry is well accustomed to. The study reveals both encouraging learning factors and inhibiting learning factors. The Encouraging learning factors are; positivity amongst the participants in the organizations, and openness towards learning and possible organizational changes. Cultural values underpin the exercises intention and the majority believes that exercises can affect organizational values positively over time. The inhibiting learning factors include; some lack of quality in the exercise design (according to participants), i.e. dependence on computer systems (not available during exercise). Exercises needs to compete with day-to-day activities, and is therefore secondary.

3.5 Organizational Learning

Organizational learning is viewed as routine-based, history-dependent, and target-oriented. The research of organizational learning examines how organizations develop knowledge and routines to guide their behaviors [LM88]. Learning in organizations take place at the individual level, team level, and organizational level. Organizational learning can be described as a process of individual and shared thought and action in an organizational context, involving cognitive, social, behavioral, and technical elements. [RWH09]. A major theme in organizational learning research is understanding the interplay and interactions between these learning levels [CLW99]. If learning routines are institutionalized and becomes a part of the standard operating procedures (SOPs), lessons can be more systematically exploited despite of employee turnover.

3.5.1 Aspects of Organizational Learning

There are several aspects of this concept that contributes to organizational learning difficulties, explored by Levitt et al. [LM88]. *Competency traps* are especially likely to lead to inadequate adjustments if newer routines are better than old ones. Learning leads to experience that can lead an organization or industry to continue using technologies or a set of procedures that may be far from optimal. An example of this is the qwerty-keyboard optimized for typewriters, but ineffective for use of the electronic keyboards used today. *Superstitious learning* occurs when the experience of learning is compelling, but the connection between actions and outcomes is specified incorrectly. For example, a manager gets promoted based on performance, which produces self-confidence among top executives. This self-confidence is partially superstitious, leading the executives to overestimate their ability to control the risks their organization faces.

There are also aspects of organizational learning that leads to enhanced learning capabilities. One of those is *experimental learning* [RWH09]. Performing preparedness exercises is a form of experimental learning. Experimental learning can lead to cost-reductions as organizations develop expertise and practices to reduce mistakes. The organization speeds up and improves its processes, and is better able to plan for changes and predict incidents and events. No organization can ever claim to be finished with learning, as nicely put by Gorelic (2005, 384) [Gor05]:

> *"If organizational learning is seen as a continuous learning cycle, then an organization can not arrive at a point in time when it declares itself "a learning organization", a noun or an end state. On the other hand, any organization can identify with being in a constant state of learning and declare itself to be practicing organizational learning."*

Level	Process	Inputs/Outcomes
Individual	Intuiting	Experiences, Images, Metaphors
Individual/Group	Interpreting	Language, Cognitive map, Conversation/Dialog
Group/Organization	Integrating	Shared understandings, Mutual adjustment, Interactive systems
Organization	Institutionalizing	Routines, Diagnostic systems, Rules and procedures

Table 3.1: Learning in organizations: Four processes through three levels [CLW99].

3.5.2 The 4I Organizational Learning Framework

An organizational learning framework called the 4I Framework has been developed by Crossan et al. [CLW99] identifying strategic renewal as the underlying phenomenon of interest. They present organizational learning as four related processes – intuiting, interpreting, integrating, and institutionalizing – occurring over three levels; the individual, group, and organizational level. These three learning levels define how organizational learning take place. Intuiting and interpreting happens at the individual level, interpreting and integrating happens at the group level, and integrating and institutionalizing happen at the organizational level (Table 3.1). This section contains information from Crossan et al. [CLW99] unless stated otherwise.

Organizational learning is a dynamic process that not only occurs over time and across levels, but also creates tension between assimilating new learning (feed forward) and exploiting or using what has already been learned (feedback). This kind of "strategic renewal" challenges the institutional norms. This is a particularly useful characteristic as it is expected that lessons learned from security incidents will challenge compliance culture – a key obstacle to the development of effective security strategy [AMS15, TRA10]. Organizational learning as a dynamic process utilizing the 4I Framework is seen in Figure 3.4. This framework employs double-loop learning principles, as explained in Section 3.6.2. A more detailed explanation of the framework is out of scope for this thesis, and reading the original article as well as a proposed improved model by Ahmad et al. [AMS15] is recommended.

3.5.3 Scope, Outcomes and Measures of Organizational Learning

Little is found in the literature about organizational learning specifically from exercises, and specifically on the subject of information security. Organizational learning is often discussed as an all-encompassing and somewhat abstract concept. Measures of outcomes of the organizational learning are generally absent in the research literature as well. The goal of learning needs to be defined in order to measure

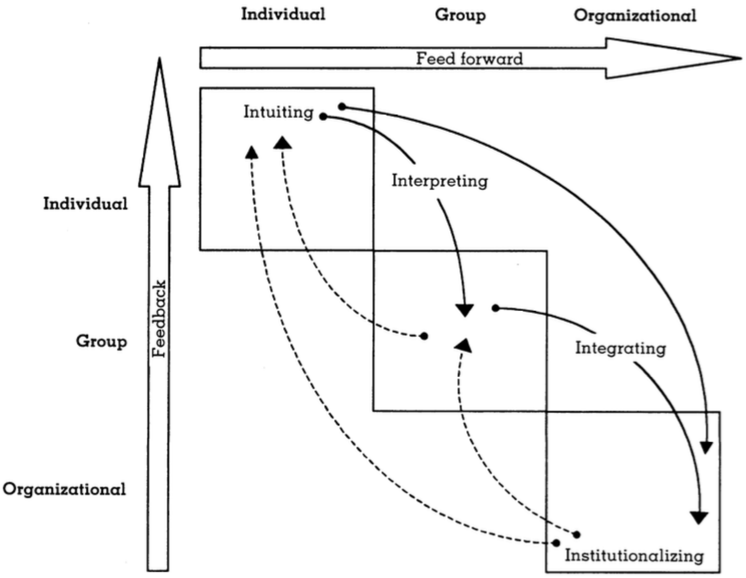

Figure 3.4: The 4I Framework: Organizational learning as a dynamic process. Figure retrieved from Crossan et al. [CLW99].

the impact of learning on improved performance [ESSG98]. Different perceptions of organizational learning influence the definition of organizational learning goals.

3.6 Learning to Learn

> *"The general expectation is that learning procedures will become common when they lead to favorable outcomes and that organizations will become effective at learning when they use learning routines frequently."* – B. Levitt and J. G. March, Organizational Learning [LM88]

Research shows that training for responding to information security incidents is given low priority, and evaluation after training sessions and smaller incidents are not performed [Lin15]. *Learning to learn* would enable organizations to take advantage of exercises and evaluations, and improve their incident response practices. In this research the challenges of improvement of incident management practices were explored, and cross-functional teams and learning to learn were the proposed solution. The discovered challenges and the corresponding solutions are presented in Figure 3.5.

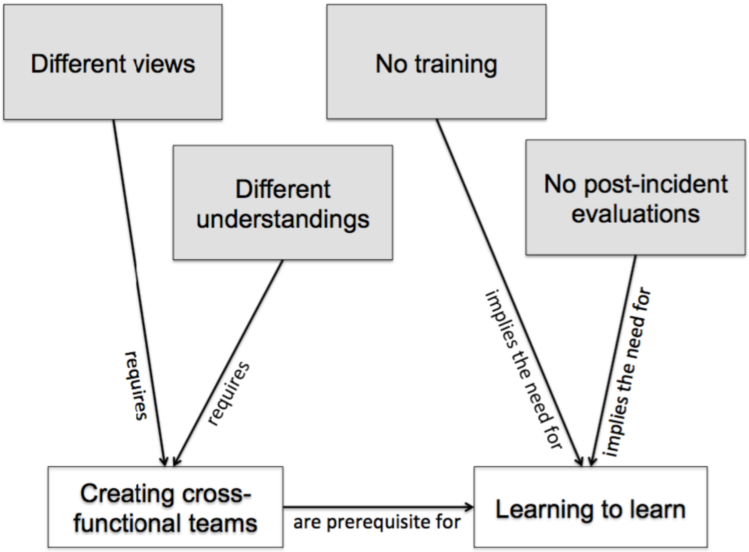

Figure 3.5: Challenges for improving incident management practices – The need for creating cross-functional teams and learning to learn [Lin15]

3.6.1 Challenges with Learning to Learn

Learning from exercises as well as from previous incidents is key for improving incident management practices. Proper handling of small security events and early warnings can prevent extensive security disasters [SM11]. One challenge with learning to learn is *management commitment*. The willingness of management to commit resources to facilitate learning is essential to learn from incidents. Post-incident evaluations and training for incident response is found to not be prioritized due to risk perception being lower than it should be from the level of current threats [Lin15]. A *lack of post-incident evaluations* can also be explained by the lack of major incidents, as organizations do not prioritize learning from smaller incidents [AHR12]. Two main obstacles to organizational learning is found – *threatening* and *embarrassing* issues [AS97]. Information security issues where a computer has been infected due to someone clicking a bad link in an email can be embarrassing, and threatening as the incident can be considered confidential. Hiding these types of incidents can be viewed as *impression management*, and can be put together with *superstitious learning* discussed in Section 3.5.1.

3.6.2 Learning Techniques

This section explains the three learning methods single-loop, double-loop, and triple-loop learning, and how and why they are used in learning to learn for organizations.

Single-loop and Double-loop Learning

Incidents can be complex and messy, increasing the need for learning and complicating the process of effective learning. Organizations need to learn to use the techniques of single-loop and double-loop learning [AS92]. *Single-loop learning* entails changing procedures and practices in response to a problem, in order to avoid the problem from arising in the future. In other words, learning to handle one specific incident. To learn single-loop learning is to answer the question: *"Are we doing things right when solving the incident?"*. *Double-loop learning* involve using experience from occurred incidents to understand their underlying causes, and take action to resolve these causes, and to understand what caused the incident to happen. Learning double-loop learning involves learning how to reflect upon the incident and the underlying organizational action. To learn double-loop learning is to answer the question: *"Are we doing the right things when solving the incident?"*.

To improve the organizational learning from exercises and smaller incidents, double-loop learning is recommended rather than single-loop [Lin15]. Double-loop learning makes the organization understand the underlying causes of problems and initiate actions to solve them. This will ensure a solid and long-lasting improvement. In the next section triple-loop – or deutero-loop – learning is explained, and how this learning method is different from single- and double-loop.

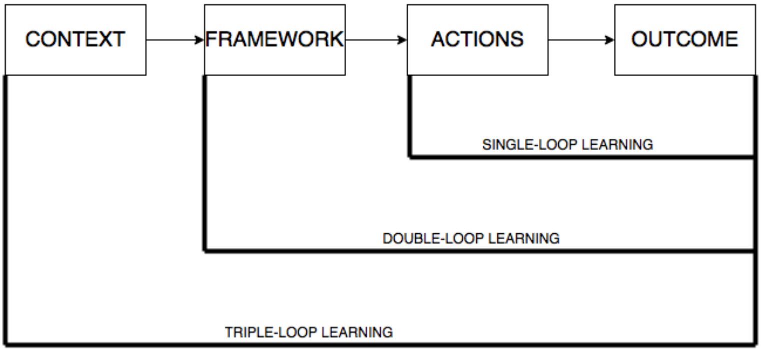

Figure 3.6: The three models of learning as explained by 24reasons [24r08]

Deutero Triple-loop Learning

Deutero triple-loop learning, or transformational learning, involves "learning how to learn" by reflecting on how we learn [24r08]. When you learn a specific technology or process, you simultaneously learn something about the world, how things occur, and you develop habits.

While single-loop learning is about “following the rules” while trying to correct a problem, and double-loop learning can involve “breaking” said rules to ensure that the problems does not re-occur, triple-loop learning is about reflecting on what we believe, how we think, and our values and how they relate to what we do and how.

In Figure 3.6 the three learning methods are visualized; Organizations operate within *context*, *frameworks*, and *actions* in order to produce an *outcome*. The *context* is what organizations do based on history, habits, and organizational strategy. The *frameworks* governs and shape how organizations work with policies, procedures, and constraints. The *actions* are the activities, tasks and behaviors that staff undertake in an organizations processes. And lastly, the *outcome* of an organizations actions are typically what a client/customer experiences, or in our context, the aftermath and consequences of an incident. Where does the learning techniques fit in?

- *Single-loop learning* concerns correcting an unacceptable outcome or result
- *Double-loop learning* concerns improving the framework that governs the actions. Can be systems, procedures, policies, etc.
- *Triple-loop learning* can lead to changes in the overall strategy.

Organizations that only engage in single-loop learning are likely to keep repeating the same mistakes. Organizations that engage in double-loop learning can fix the mistake and work with the framework to address the cause. Triple-loop learning can help an organization to understand more about themselves and others regarding beliefs and perception.

3.7 Summary

The subject of information security incident management and preparedness exercises has risen in popularity in recent years. There are several research articles trying to comprehend the challenges and effects of performing preparedness exercises, and mapping of if and how preparedness exercises are performed in various industries. This can be challenging, as some of the industries that would benefit the most from being prepared for the worst, might not be industries that perform IT security related preparedness exercises yet. We have studied research related to incident management in organizations, preparedness exercises, and research focusing on the power industry particularly.

While studying related work and background material, we have found that research focusing on incident management and preparedness exercises has increased significantly in recent years. However, there is still a long way to go with mapping the actual effect and lessons learned from performing such exercises. The background study tells us that industries still have a hard time grasping the value of performing exercises, and it is therefore often neglected. This is especially a problem within the IT security realm where the development is recent, rapid and overwhelming, and “nothing bad has happened yet”. We hope that this master’s thesis can contribute to revealing the importance and relevance of performing continuous exercises for the power industry and others.

Chapter 4 Case

This study examines three Norwegian Distribution System Operators (DSOs), in addition to acquiring valuable information from two Norwegian preparedness exercise facilitators. The three DSOs are among the ten largest in Norway. The three DSOs are chosen as participants as a continuation of the work done by Line and Moe [LM15], assessing the collaborative challenges in IT security preparedness exercises. This was partly done by auditing an exercise that all three organizations performed, and this exercise is relevant for the questions asked to the participants of this study. The exercise facilitators are key employees in companies working with facilitating preparedness exercises for other clients as a service. A figure of how it all fits together is provided in Figure 4.1: The three DSOs that have participated in the fall 2014 exercise are all interviewed in this study. There is one set of questions asked to the exercise leaders, and one set asked to the exercise participants. Both sets of questions can be found in Appendix A. The two external exercise facilitators are interviewed independently of the exercise and the DSO domain, and the questions asked can be found in Appendix B.

4.1 Distribution System Operators (DSOs)

The three organizations performed an IT security preparedness exercise developed by the Norwegian Water Resources and Energy Directorate (NVE), and the exercises were audited by Line and Moe [LM15] during the fall of 2014. This was the first execution of such an exercise for Organization A and B, while Organization C had performed similar exercises before. In the following, I briefly present the preparedness exercise scenario, the three organizations, and some details of their exercise conduction. The information is from Line and Moe [LM15] unless stated otherwise.

4.1.1 The Fall 2014 Exercise

The scenario of the exercise was, as mentioned, developed and recommended by the NVE. The scenario embodied an information security incident that escalated through

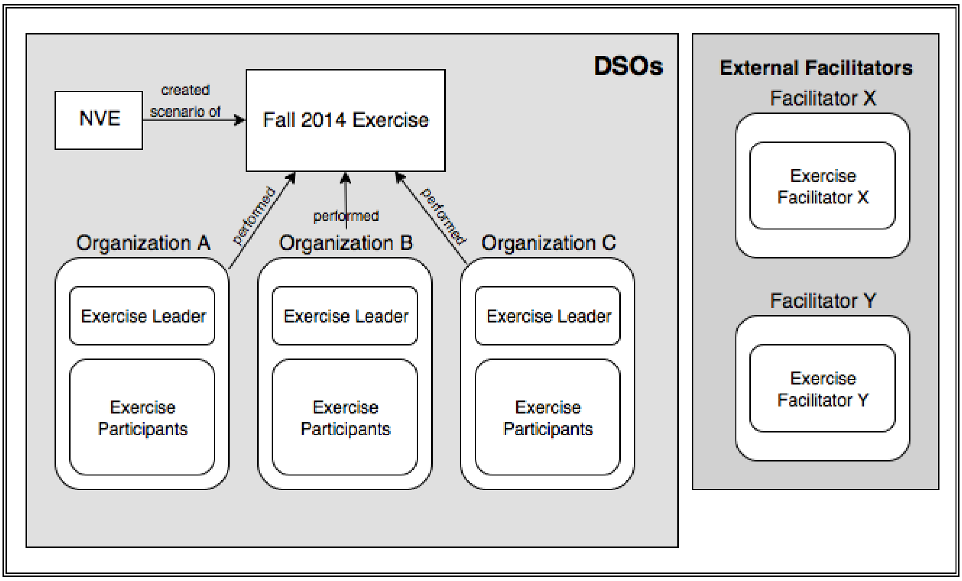

Figure 4.1: An overview of the case material and participants of this study: Three DSOs having performed the same exercise, with their respective exercise leaders and participants, and two external exercise facilitators.

five phases. The exercise itself will hereby be referred to as the fall 2014 exercise or simply "the exercise". The five phases were as follows:

1. Abnormal amounts of information is being sent from the organization's computers.

2. After two weeks, a contractor calls and informs about a discovered vulnerability in the SCADA-system[1], and wishes to patch the system.

3. Three months after the first incident, an area suffers from power outage. The incident is not picked up by the monitoring systems.

4. Customers are calling complaining about power outages in more areas. No alarm is raised by the monitoring systems.

5. Mobile communications and Internet connection is down.

[1] Supervisory Control and Data Acquisition (SCADA) – a system that operates with coded signals over communications channels so as to provide control of remote equipment [DS99].

The phases have a 20-minute time restriction, when this is reached the group is forced on to the next phase. The exercise requires 3 hours in total: 15 minutes of introduction, up to 2 hours of exercise conduction, and 1 hour of presentations.

All three organizations carried out the preparedness exercise according to generally recommended NIST practices [GKK04]. They used the same scenario and had the same main agenda for the exercise, but they differed on the number of and types of participants, and the goal of the exercise.

4.1.2 Organization A

Nine employees participated in the exercise, representing three groups of personnel: IT operations, industrial control systems, and network infrastructure. All but two of the participants had more than 20 years of experience in the business. One of the participants acted as exercise leader when performing the exercise, and is interviewed with the in-depth exercise leader questions. Organization A's goal for the exercise was "Knowledge exchange and process improvement".

4.1.3 Organization B

Three groups of personnel represented: IT, control systems, and control room operations. There were fourteen participants in total, with experiences varying from 1 to more than 20 years. They divided into three groups, with the intention of having all three areas of expertise in each group. One of the participants acted as a part of the exercise leadership when performing the exercise, and is interviewed with the in-depth exercise leader questions. Organization B's goal for the exercise was "Cross-functional self-managing groups".

4.1.4 Organization C

Twelve employees partook in the exercise. Five of the participants were part of an Emergency Management Team and were called into the room when their presence was needed. This was done to create a more realistic feel to the exercise scenario. One of the participants acted as exercise leader when performing the exercise, and is interviewed with the in-depth exercise leader questions. Organization C's goal for the exercise was "Involvement of Emergency Management Team".

4.2 Preparedness Exercise Facilitators

Two information security preparedness exercise facilitators are also included in this study. They are included in order to get an outside perspective of the challenges and effects of performing exercises. They represent two different organizations with different customer bases and different ways of performing the job.

4.2.1 Facilitator X

Facilitator X has 3 years experience as an exercise facilitator, and has conducted six exercises in total. All of the exercises has been related to information security in some degree, always using the CIA triad (confidentiality, integrity, and availability – see Section 3.1) when discussing communication and information handling. One of the exercises was a pure IT security exercise with cybersecurity incidents as the main focus. Facilitator X works for Combitech[2], which has also provided this research with some statistical data on exercise evaluation.

4.2.2 Facilitator Y

Facilitator Y has 5 years of experience working as an exercise facilitator, and has conducted somewhere between 10 and 15 exercises. All exercises have been IT security exercises. Facilitator Y's organizations is one of the largest providers of IT information security services in the Nordic region.

[2] Combitech AS is a Nordic technical consultancy company combining technology, environment and security (www.combitech.com).

Chapter 5
Results

In this chapter the data collected from a total of 19 interview participants is presented; three extensive interviews with the DSO exercise leaders, two extensive interviews with exercise facilitators, and 14 short interviews with DSO exercise participants. The interview questions for the DSO exercise leaders and DSO exercise participants can be found in Appendix A, and the interview questions for the exercise facilitators can be found in Appendix B. At the end of this chapter some exercise evaluation statistics are presented, provided by Combitech.

5.1 DSO Exercise Leaders

5.1.1 Information Security Events and Exercises

The interviewee from *Organization A* acting as exercise leader for the fall 2014 exercise is employed as IT security coordinator for control systems in the organization. The interviewee found it hard to state exactly how often IT security incidents occurs in their organization, as it depends on how you define a security incident. Large unintentional technical incidents on IT-equipment (like in the SCADA system) happen a few times per year, while intentional incidents happens rarely, with many years between each incident. Their system has never detected any hacker activity. Organization A has not performed any new IT related preparedness exercise after the fall 2014 exercise, and state lack of time and low priority as the main reasons.

The interviewee from *Organization B* acted as part of the exercise leadership for the fall 2014 exercise. The number of IT security incidents is confidential information and was therefore not shared in the interview. Organization B has performed one new IT security exercise during the last year. It had a similar outline to the fall 2014 exercise. They have an exercise plan for the next four years using a wide range of exercise types – from table-top exercises, to simulations and operational exercises. They plan to conduct mostly table-top exercises as they are considered to be most efficient and give the desired effect.

The interviewee from *Organization C* acting as exercise leader for the fall 2014 exercise is employed as ICT security manager in the organization. The number of IT security incidents depends again on how you define an incident. The interviewee states that if you define an IT security incident as a breach of rules and procedures, incidents occurs several times a month. Organization C has not performed any IT security preparedness exercises since last fall, but has planned one for this coming December.

5.1.2 Preparedness Plans and Exercises

Organization A uses the authority (NVE) issued "Guidelines to regulations on preventive safety and emergency preparedness in the energy supply" [SSU$^+$13] as a baseline for how they perform preparedness work. They say that procedures might be inspired by various standards, but choose not to mention any specific, as they do not base themselves on any particular framework. They perform exercises in non-IT domains a couple of times a year. They use table-top exercises, as well as operational exercises with acting field workers. They perform exercises aiming to engage management, and technical exercises for checking of redundancy and reserve equipment (drills). The interviewee claims that all exercises provides a certain extra focus on the possibility of real incident occurrence, and that an exercise will sharpen the mindset to be prepared for the unexpected.

Organization B bases their standards and procedures on the ISO/IEC suite, in particular the 22301, 27001, 27005, and 31000 standards [ISO12, ISO13, ISO11a, ISO09]. These are guidelines and frameworks for information security management systems, information security risk management, and business continuity management systems for societal security. They consist of principles, guidelines, and requirements for the aforementioned topics. They perform 2-3 large exercises, and 12 small (2-3 hours) exercises yearly across all domains. Most of these are table-top exercises, a couple of them are simulations, and biannually they perform a live operational exercise. One to two times a year parts of the organization is set into emergency preparedness mode due to extreme weather warnings. This team also contributes to training other employees beyond the regular plan. The interviewee claims that exercises help the communication to flow more freely, and cooperation is performed more smoothly. Emergency alerts and organizing is performed better due to continual exercising.

Organization C uses ISO standards, and the exercises they perform are table-top. The interviewee claims that learning from an exercise has not helped the workflow during a real incident.

5.1.3 Learning from Exercises

Organization A does not have any formalized routines related to improving incident response processes or exercise plans after an exercise, but admit that changes may occur. The participants evaluate an exercise immediately after conduction, and an evaluation report is prepared. The organization claims to adjust and improve procedures based on real incidents, and specifies that this is performed particularly after larger, serious incidents. The exercise leader from Organization A states that it can be challenging to learn from an exercise, as participants return to "normal-operation" mode afterwards and can struggle to bring learning from fictional incidents into the day-to-day operations.

Organization B uses an informal sheet for exercise participants to write down experiences and improvements to processes and routines, ideas for new exercises, et cetera. An exercise is evaluated by the exercise leaders, and by exercise leaders together with participants. Both exercise facilitators and exercise participants contribute with suggestions for new exercises, and the interviewee claims to continually write down new scenarios based on daily routines and real operation events. An exercise is evaluated by means of group meetings and email exchange. A team collaboration software tool will be used in the future. Organization B's internal ICT preparedness plan and other preparedness plans are updated as a reaction to real incidents. Action cards and checklists are updated as a direct result of incidents and exercises. On the question of whether the interviewee has experienced any challenges with learning from an exercise, he responds: "No, there is always something to learn".

After an exercise, *Organization C* evaluates the exercise and establishes measures to be taken. They prepare an exercise report with background information and goals, which gives an overall evaluation and a summary of the most important possible improvements. They have a multi-year exercise plan. The interviewee has not experienced any challenges with learning from exercises. However, they state that they do not perform improvements or adjustments to procedures based on experiences from real incidents.

5.1.4 The Fall 2014 Exercise

In the aftermath of the fall 2014 exercise *Organization A* has adjusted its routines, applied for a membership in KraftCERT, and created an internal IRT. The interviewee does not feel that the organization's incident handling has improved based on the fall 2014 exercise, and states that this has not been measured in any quantifiable manner. The main challenge of performing IT security exercises in this domain is, according to Organization A, a technical and operational difficulty. The SCADA system needs to be operative 24/7, which makes it hard to exercise on the actual online system. Additionally it is challenging to set aside time and gather people in a normal, hectic, day-to-day operation.

Organization B updated parts of their ICT preparedness plan after the exercise, and some action points were added. The interviewee claims that the organization is better at understanding and performing cooperation between ICT and ICS after the exercise, but there is room for even more learning, especially on reporting incidents. Lack of time and hectic workdays are highlighted as the main challenge for performing exercises. All exercises require planning and reservation of time for all participants, else they will be busy doing other tasks that cannot wait while they participate in an exercise. This planning does however gives them the ability to include exactly the wanted personnel. The downside is that no exercises come as a “surprise”. Extreme weather or other incidents will also put any planned exercises on hold, and needs to be taken into account. An interesting observation from the interviewee implying that exercises indeed sharpens the mind: “Last year we went directly from an exercise and into real preparedness due to unexpected extreme weather – top notch preparedness in other words.”

An interest group for industrial control and ICT has been established at *Organization C*, in order to get best practice routines in place. They highlight organizational challenges regarding performing IT security exercises in their domain, where different departments and businesses have responsibility for different systems and infrastructure in the organization.

5.2 DSO Exercise participants

Following is the results from the short interview sent to all DSO exercise participants. From Organization A 6 out of 9 responded, from Organization B 3 out of 14 responded, and the number from Organization C was 5 out of 12. They were asked questions directly related to the fall 2014 exercise (interview questions can be found in Appendix A).

5.2.1 Organization A

When asked whether there have been any changes to routines or tasks after the exercise, the participants are evenly split answering either yes or no. Those answering yes can tell of improved reporting procedures and inter-organization cooperation, KraftCERT membership, a security project initiated by internal communication distributor, and general changes and increased focus on the topic of information security.

All except one has not participated in any new exercise with focus on IT and security. One person is working with the internal communication distributor and performs regular exercises on security incidents in conjunction with this.

There is a general agreement amongst the participants that it is hard to measure if incidents have been more effectively handled due to this exercise. Some say that it might have a marginal effect, and that participants will be more aware of ICT security in general. One mentions that the internal IT groupings work more closely than before, and that this is an effect of both this exercise, the KraftCERT membership, and the establishment of an internal IRT.

Challenges related to conducting IT security exercises in this specific domain is time, unavailability of correct personnel, that the participants cannot tamper with the ICT-systems involved, and the challenge of making the exercises realistic enough; they can "only" perform table-top exercises as down-time on the IT systems is not acceptable.

There is a general agreement that the fall 2014 exercise has improved the organization's ability to handle IT security incidents, to some degree. Again they mention that this is hard to measure. One states that the point of an exercise like this is to drill the existing routines, and to have specific roles, routines and processes in order to avoid chaos when a real incident occur. A reporting procedure has been put in place in order to shorten the response time when an incident is reported, and the newly established IRT contributes to better cooperation between the three internal IT groupings. One states that performing exercises is always good, as it puts emphasis on routines and procedures related to preparedness.

More than half of the participants state that there is increased information exchange and cooperation across the organization after this exercise. There is also an agreement that this is not a direct consequence of the exercise, but of the organization's generally increased IT security focus, the newly established IRT, and the security project of the internal communication distributor.

5.2.2 Organization B

Two participants declare that there has not been any changes to routines or work tasks after the exercise, and one speaks of increased focus on attitude change related to information security, creating better relations and information flow across the departments in the organization.

Two of the participants have participated in more IT related exercises. None of the exercises were similar to the fall 2014 exercise, but smaller, repetitive exercises over email in conjunction with the National Cyber Security Awareness Month. This maintains focus and motivates.

There is unanimous agreement that the exercise has contributed to more effective incident handling this last year. One points out that the exercise is only a small part of the perspective-changing work making it hard to isolate its first-hand effect, but that incidents has definitely been more effectively handled during the last year.

An activity packed workday means that it is difficult to reserve the resources necessary to perform exercises. Security is often a topic of discussion, but little worked on. One states that his work as SCADA administrator provides challenges related to security on a daily basis, and on many levels.

There is some uncertainty around whether this exercise has changed the organization's ability to handle IT security incidents, as the exercise is now a year old. One says that the exercise surprisingly posed as a forum where many participants experienced epiphanies, the discussion was flowing freely between the participants across the organization, and generated many new train of thoughts that the company may take use of.

All participants agree that the exercise has lead to increased information exchange and cooperation across the organization. One states that the exercise has contributed to achieve mutual understanding of the respective departments predicaments and challenges. This is important for holistic security work and to avoid widespread self-centering.

5.2.3 Organization C

Two of the participants mentions the creation of an interest group for ICT for cooperation between the ICT department and the ICS department as newly formed routines after the exercise. The other three claims that no change has been made.

This organization has not performed any new IT and security related exercises since last fall. They are however running an ICT security campaign on their intra-net to raise awareness amongst employees.

There is discord in the answers to whether incidents are better handled due to experiences from the exercise. Two say no, three say yes or maybe. They point out increased focus on ICT security, and especially focus on the issues raised in the exercise. There is also mentioned that they have not experienced any large incidents since then, and therefore no way of measuring the exercises effect on handling real incidents.

As with the other organizations, time, prioritization, and technical difficulties are the most prominent challenges with performing IT security exercises. One states that IT exercises need to compete with the important tasks of power generation and distribution, and handling of injured personnel, which are tasks of great importance for the organization. The importance of 100 % up-time of the SCADA system is mentioned here as well, making other exercises than theoretical table-top exercises impossible.

There is general agreement that the exercise has had a positive effect on the organization's preparedness plan. They highlight KraftCERT membership, teamwork and cooperation, and increased awareness around IT security issues as positive effects. One comments on the value of getting to know the employees working with adjoining problems in various sister organizations. Two states that the exercise has lead to better information exchange and cooperation across the organizations, especially regarding power sensitive information.

5.3 Preparedness Exercise Facilitators

Two professional preparedness exercise facilitators have been interviewed, and the results of these interviews are presented in this section. The questions asked kan be found in Appendix B.

5.3.1 Exercise Standards and Challenges

Standards and Guidelines

When working with building an organization's IT security preparedness, Facilitator Y's firm uses the framework that their own IRT is based on. This framework is primarily based on NIST [GKK04] and FIRST [fir], but is increasingly influenced by own experiences. ENISA [eni10] and FIRST can be viewed as an inspiring foundation for developing exercises, as the development of exercises is to a small degree based on standards. Facilitator X mentions a range of standards and guidelines used in their line of work. A range of ISO/IEC standards[1] and NIST standards[2], in addition to laws and guidelines specific for various sectors in the Norwegian industry[3].

[1] ISO/IEC 270xx: Information Security Management Systems Family of Standards [ISO14, ISO13, ISO11a], ISO/IEC 22301: Societal security – Business continuity management systems — Requirements [ISO12], and ISO/IEC 31000: Risk management - Principles and guidelines [ISO09].

[2] NIST SP 800-53: Recommended Security Controls for Federal Information Systems [NIS03], NIST SP 800-115: Technical Guide to Information Security Testing and Assessment [SFS08], NIST SP 800-34: Contingency Planning Guide for Federal Information Systems [SBWP$^+$10], and SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities [GNB$^+$06]

[3] Norwegian laws and regulations concerning security (sikkerhetsloven), electronic communication (ekomloven), privacy (personopplysningsloven), health preparedness (helseberedskapsloven) etc. [For01, Sam14, ob01, oo01]

Challenges with Creating and Performing Exercises

It is challenging to avoid making the exercises too complicated, and develop good scenarios that reach the correct goals, states Facilitator Y. Organizations can have trouble expressing what they want to achieve, making it a challenging task. Having a clear exercise goal, keeping to time constraints and budget constraints are challenges mentioned by Facilitator X. Both facilitators express the importance of planning the evaluation method early on, and claims that it is beneficial to ask the same evaluation questions before and after an exercise in order to measure differences in perceived preparedness. An example of this kind of measurement is shown in Section 5.4.

Challenges with Information Security Exercises

The challenge of making an IT-related exercise technically viable, realistic and feasible is mentioned by both Facilitators. The need for dedicated exercise equipment to avoid spreading business confidential information on the Internet is also mentioned by Facilitator X, as well as avoiding the management's perception that "It will be fixed by the IT department", and actually involve and activate the entire business in a realistic manner.

Challenges with Making an Organization See the Benefit of Exercising

Facilitator X claims that businesses regard information security as an assignment for the IT department, and hence does not realize it is a management responsibility – or that information security or cyber security incidents can evolve to cover the entire business. Facilitator X do not feel that any specific work domains are worse than others, but that the businesses maturity level concerning IT and incident management is relevant. Facilitator Y states that there are challenges to making organizations see the benefit of exercising, but that it is not a prioritization for their business to make it otherwise, and therefore cannot mention any challenges in specific.

5.3.2 Learning from Exercises

Post-Exercise Work

Facilitator Y is to a small degree participating in performing changes in an organization as a result of an exercise. They can be asked to make updates to the organization's framework, or conduct various kinds of training. Facilitator X is generally more involved in realizing measures identified during and after an exercise. To what degree this happens depends on the scope and goal of the exercise, but the facilitator is usually involved in the after work. Changes can include updating documentation, conducting theme specific training, conducting table-top exercises to test the updated documentation, procurement, facilitation and training in use of new preparedness equipment and material, and help to narrow down the amount of business information that is publicly available.

Facilitator X performs debriefs immediately after exercise and creates a summarized evaluation report. The customer can then evaluate the evaluation report, and commit to implementing identified improvements. Facilitator Y also writes a report to the customer with suggestions for improvements, and in organizations where they perform consecutive exercises they can see evidence of the suggestions being considered and might be added to their framework.

Exercise Evaluation

Facilitator X performs evaluations before, during, and after an exercise, where participants fill out three questionnaires each. They occasionally use "observers" that are assigned to observe and report to the facilitating exercise leaders and provide suggestive counsel if the participants reaches a stand-still during the exercise. They also sometimes use "moles" with the purpose to assist with suggestions if the participants reaches a stand-still, provide continuing feedback to exercise leaders regarding adjustments of exercise pace, give continuing and closing evaluation of the organization's ability to handle a crisis, and identify possible improvements. They facilitate an oral debrief immediately after an exercise with the exercise participants, followed by a debrief internally in the facilitation organization identifying other aspects of the clients actions during the exercise, and improvements for future exercises. An evaluation report is delivered about a week after, covering a short description of the exercise, summary of feedback and input from participants, comparison of exercise with earlier exercise(s), and a prioritized list of improvements based on "quick wins/low hanging fruits" first, followed by usefulness and realization probability.

Metrics

No specific metrics are established by Facilitator Y. The importance of establishing goals before making the exercise is emphasized, and they admit that goals could have been used more actively to evaluate the exercise afterwards. Questionnaires with scale from 0 to 5 are used by Facilitator X, in addition to some free-text fields for further expression. A questionnaire is handed out three times – before, during, and after an exercise (see Section 5.4).

Experiences from Exercises

Facilitator Y uses experiences from previous exercises to improve their own exercise framework. Facilitator X claims that using experiences from an exercise is necessary in order to develop the organization's readiness level and competence. This can include conducting smaller intermediate exercises to work on specific aspects of incident management. This can mean that the consecutive exercise focuses on further identifying improvements from the previous exercise, to test if the participants can use their acquired knowledge and experiences in a new and unexpected exercise context. In addition, improvements to the exercise concept itself are identified, so that the exercises and its measures will be continually improved.

Organizational Improvement Challenges

Management commitment, budget constraints, and contradictory interests within the company, are pointed out as challenges by Facilitator X. Facilitator Y mentions the lack of willingness to change, the need of sponsors, seeing the need for change, economic sensibility, and having the right resources available; people and technology. The biggest challenge according to Facilitator X is to get an organization to change its normal, consensus-based thinking, where everyone is supposed to agree with the others opinions.

5.4 Exercise Evaluation Statistics

This section presents exercise evaluation statistics provided by Combitech – a Nordic technical consultancy company combining technology, environment and security. Combitech is the company where Facilitator X works, and this is an example result of the evaluation sheet they provide the participants before, during, and after an exercise.

The questions being asked are split into two parts of 5 and 8 questions respectively. The first set of questions is being asked both before and after an exercise, in order to compare how each individual measures their own progress before and after the exercise. The results from the questions asked after the previous exercise is also included in order to compare against previous results. The questions are rated from 1 through 6, with 6 being the highest score. 0 means not applicable. The questions are as follows (translated from Norwegian):

1. I feel well prepared in my role to deal with and assist during an emergency
2. I have read and familiarized myself with the emergency preparedness plan
3. I have read and familiarized myself with the alert sheet[4]
4. I know what role and tasks I have in the emergency team
5. I know who I am deputy to, and who is my deputy[5]

The results from these questions are represented in Table 5.1.

[4] Norwegian: varslingsskjema

[5] Norwegian: stedfortreder

Question #	**After last ex.**	**Before this ex.**	**After this ex.**	**Change**
1	3.6	3.7	4.2	+0.6
2	5.5	4.9	5.6	+0.1
3	5.4	5.4	5.7	+0.3
4	4.8	5.0	4.9	+0.1
5	5.4	5.0	5.3	-0.1

Table 5.1: The answers to questions 1 through 5, asked after the preceding exercise, before the current exercise, and after the current exercise. The scale is from 1 to 6.

The second set of questions deals with the conduction of the exercise itself, which also includes the results from the previous exercise for comparison. The same scale from 1 to 6 is used. The questions are as follows (translated from Norwegian):

1. I experienced that the alert quickly assembled the emergency team
2. I experienced that the emergency team quickly distributed and organized the assignments at hand
3. I experienced the changing of roles to function effectively and informative
4. I experienced my situational awareness during the exercise as good – I felt that I handled the situation quickly
5. I felt on top of the situation as it changed during the course of the exercise
6. I experienced a good flow of information during the exercise
7. I experienced the organization to support the emergency team well
8. I experienced that the preparedness plan and available sheets were helpful for my role in the emergency team

The results from these questions are represented in Table 5.2.

Question #	**After last exercise**	**Weighted average**	**Change**
1	2.4	3.6	+1.2
2	4.2	4.5	+0.3
3	2.9	3.6	+0.7
4	4.8	4.4	-0.4
5	4.4	4.6	+0.2
6	2.7	3.8	+1.1
7	4.2	3.8	-0.4
8	4.0	4.9	+0.9

Table 5.2: The answers to questions 1 through 8, asked after the preceding exercise, and during current exercise. The weighted average is of the evaluations performed during the current exercise. The scale is from 1 to 6.

Chapter 6
Discussion

In this chapter, the findings from Chapter 5 are discussed in relation to the studied background material and the thesis's research questions. The most prominent findings from this research are presented in the first two sections, followed by a revisit to the research objectives of this thesis. This is followed by a section presenting recommendations on how to accommodate the challenges found, and the chapter ends with a section discussing the limitations of this kind of study.

6.1 Prominent Observations from Findings

In this section, the most prominent observations from the interviews are presented. At the start of the section a list of challenges and effects are provided to summarize, followed by sections elaborating on the findings.

6.1.1 Challenges and Effects Summarized

To get an overview of the challenges and effects that were discovered during this research, a simplified list is provided. This is both to provide a synopsis of the results, but also to highlight the existence of both negatives and positives. Some findings are put under both categories as they are improved, but not yet perfected.

Challenges:

- Lack of definitions
- Lacking reporting mechanisms
- Management prioritization
- Learning difficulties
- Time restrictions
- Technical challenges
- Communication

- Collaboration
- Hard to measure effect

Effects:

- Increased security awareness
- Increased communication and collaboration
- Better reporting mechanisms
- Creation of interest groups
- Memberships of KraftCERT
- Perceived better preparedness

6.1.2 Definitions and Reporting

All three DSOs have some problems with using a clear definition of what a security incident is, and are therefore vague when describing the number of incidents occurred the previous year. This is despite the fact that the same organizations claim to use standards and guidelines that define information security incidents [ISO14]. The lack of consistency in incident reports and clear definitions might be a cause of why some participants state that their organization still has some way to go regarding reporting of incidents. It also underpins the statistics from NSM showing that there is a substantial gap between the number of reported incidents and the number of actual incidents [Sik14, Sik15].

6.1.3 Exercise Challenges

There has been little IT security related exercise activity in the organizations the last year. Lack of time and prioritization are pointed out as main obstacles. The low priority concurs with earlier research [Lin15]. Power supply companies are highly operational organizations that need to be prepared for incidents related to HSE (Health, Security, Environment) and infrastructure breaches due to extreme weather, and arguing the importance of performing additional exercises within other domains can be challenging. The list of challenges mentioned are long; technical difficulties, operational difficulties, time restrictions, availability of resources, organizational challenges, and prioritization. One can argue that if you solve the challenge of management prioritization, the other challenges will be diminished.

The technical difficulty of not being able to exercise using the live SCADA system is a DSO specific obstacle, and narrows down the span of available exercise methods. Table-top exercises are most frequently used, and Organization B states that table-top exercises are efficient, doable, and achieves the desired effect. The relationship between cost and effect plays an important role in getting management commitment.

It is also practically more feasible as it does not require use of live computer systems. However, a disadvantage of making technical table-top exercises is making it realistic and technically viable.

6.1.4 Exercise Learning Challenges

The DSOs have no formalized routines for improving incident response processes or exercise plans after an exercise. The exercise in itself is evaluated, but there are no routines for evaluation of the plans and processes the exercise is performed upon. Changes are made after larger incidents, but there is no evidence of improvements performed after smaller exercises. This concurs with earlier research [Lin15] where the reason for lack of post-incident evaluation was due to risk perception being lower than it should be from the level of current threats. This is a classic example of single-loop learning [AS92]. This is an indication of lack of good framework for revision of routines based on exercises and smaller incidents. It is also an indication of lack of organizational learning maturity, and the organizations could benefit from applied learning techniques and organizational learning frameworks.

6.1.5 Measure of Effect

Many participants, across all DSOs, have reported that it is hard to measure the actual effect of the exercise, and no quantifiable measure has been established. This is in compliance with the absence of research material measuring the outcomes and effects of organizational learning. A quantifiable measure of the effect of performing exercises can be used as a metric to convince management of exercise prioritization. The establishment of learning goals is needed in order to measure the effect of learning on improved performance [ESSG98]. Facilitator X uses evaluations before, during, and after an exercise, and therefore have numbers to show to when advocating the effect and importance of performing exercises. This indicates a distinction between professional exercise facilitators and regular organizations, where the facilitators are more dependent on showing results in order to keep selling their services.

6.1.6 Perceived Positive Effects and Actions Taken

Despite the lack of quantifiable effect measurements, there is a range of perceived positive effects identified by the participants. There is mention of better cooperation and communication across departments of the organizations, especially between ICS and ICT. The importance of successful cooperation between ICS and ICT was explored by recent research of six Norwegian DSOs [LTJ14]. Participants have also reported increased security focus and awareness, improved reporting procedures, and perceived better preparedness. When no other measurable metrics are used, the individual perception of increased experience, knowledge and preparedness is the closest one gets to measure the effect. Actions taken are memberships in KraftCERT, establishment of internal IRT, and establishment of interest group for collaboration between ICS and ICT.

6.1.7 Organizational Learning Challenges

Lack of Communication and Collaboration

Despite the fact that some participants report better communication and collaboration across the organization, the diversity of the answers indicates that there is still some way to go. The split in answers indicates some lack of communication internally in the organization, which leads the participants to occasionally have totally different views of the state of things. While some say that the organization is working actively with information security and performs various measures and attitude-changing work, others in the same organization reports to no action at all. Recent research has also identified different views and different understandings as challenges for improvement of incident management practices [Lin15]. The proposed solution for achieving learning to learn was creating cross-functional teams, which Organization C in my study has done.

Lack of Management Commitment or Willingness to Change

Varying maturity of organizational learning can be found in this study, and this can indicate a varying degree of management commitment. Management commitment is one of the main challenges with learning to learn, and is crucial for performing successful changes to an organization [PL00]. Facilitator X reports of management responses like "it will be fixed by the IT department", which indicates a certain lack of perceived management responsibility and involvement when it comes to information security exercises and incidents.

Management can also suffer from competency traps or superstitious learning. Competency traps can lead to unwillingness to change. Learning leads to experience on a certain type of process or framework, and the organization can want to continue using this process or framework even though it is not best practice. Strategic renewals that challenge the institutional norms is a useful characteristic of an organizational learning framework as it will often challenge an organization's compliance culture, which is often a key obstacle to the development of an effective security strategy [AMS15, TRA10]. Superstitious learning can occur amongst management, as self-confidence can lead an individual to overestimate their ability to, for example, assess the organization's level of security and level of preparedness. The challenge of making an organization see the value of performing information security preparedness exercises, as stated by Facilitator X:

> *"Get an organization to change its normal, consensus-based thinking, where everyone is supposed to agree with everyone else."*

6.2 The Research Objectives Revisited

In this section we will revisit the objectives of this study, and how they are answered based on the findings from the interviews and with knowledge from the background study.

Explore the practical challenges and effects of performing information security preparedness exercises

The practical challenges of performing information security preparedness exercises have proven to be many. In this work domain, technical and operational difficulties are of import. The SCADA system needs to be operational 100 % of the time, making it hard to perform exercises using the live and operational systems. This limits the ability to perform closer to real-life exercises, and the issue of making exercises realistic enough is mentioned. The lack of time and resources are prominent challenges as well. The challenge of setting aside time and gathering people in a hectic day-to-day operation is highlighted. Prioritization is also emphasized as a challenge. Other daily tasks are seen as more important, and exercises are postponed or neglected. Time and resource constrains can be seen as a cause of lack of prioritization.

The practical effects of performing information security preparedness exercises are hard to measure, and are often expressed as feelings and opinions. Many participants report back on better cooperation and communication inside the organization, increased focus on information security, attitude changes related to information security knowledge, and achievement of mutual understandings across departments within the organization. Tangible signs of organizational development are establishments of IRTs and interest groups, and becoming members of an official CERT. The effects are caused by performing exercises, in addition to other information security and IT security specific work.

Explore how organizations gain experience from performing information security preparedness exercises

It is necessary to distinguish between experiences gained by the individual, and experience gained by the organization. The individual experiences learning of handling new and unknown types of emergencies, and should attain knowledge of IT, security, and the organizations emergency policies, processes, and routines. As a participant put it, performing exercises "sharpens the mind", and gives a sense of being better prepared. This type of experimental learning potentially speeds up the processes, and makes an organization able to plan for changes and predict incidents and events better than before [RWH09]. The gain in experience is not measured in any quantifiable way after the fall 2014 exercise, and is based on perceptions, opinions, history, and earlier studies.

Survey to what extent lessons learned from one exercise are implemented in future exercises

To what extent this is performed varies greatly between the DSO organizations and the exercise facilitators. As previous research supports, there is little to no learning from exercises or small incidents implemented in future exercises or frameworks in the case of DSOs. Changes to existing frameworks are reported to happen after large incidents, but no formalized routines are in place for updating the exercise material after an exercise. That does not mean that changes do not occur, but there is no guarantee that it will. The exercise facilitators however, have robust mechanisms in place. Facilitators use experience from exercises to improve their own exercise frameworks, in addition to using experiences from an exercise to develop and improve consecutive exercises to train on the identified improvement possibilities. This shows an healthy implementation of double-loop learning.

Explore the challenges that exists in achieving learning from exercises

There are some challenges directly influencing learning achievement, and other challenges that have an indirect effect on learning achievement. A direct challenge of achieving learning on the individual level is; returning to normal-mode operations directly after an exercise, struggling to bring learning from the fictional incident into the day-to-day operations. It is simply challenging to bring the experiences and learning from a fictional exercise into the daily work, that can be two quite separated experiences. On an organizational level, a challenge is revealed by the fact that exercise frameworks are not necessarily updated based on the results of an exercise. This leaves the experiences and learning from an exercise inside the minds of the participating individuals, and can in theory be forgotten on an organizational level. This is an example of single-loop learning where the problem is fixed, but the cause is not investigated. For an organization to achieve learning, actions must be taken based on experiences, and double-loop and triple-loop learning needs to be applied.

6.3 Recommendations

This section presents our recommendations for these organizations to get better at performing exercises, learning to learn, and measure the actual effect of performing said exercises. These recommendations are based on observations of challenges and positive effects from this research, and experiences and best practices found in the background material. We believe these recommendations to be useful also for organizations of other domains and sizes.

1. **Follow the established standards and guidelines.** One thing is implementing standards and guidelines for show, or due to rules and regulations, another is to actually implement them and follow them. The standards that exist are consistent and well made, and using them will lead to consistency in operations, both inside an organization and across multiple organizations. Doing this might enable an organization to:

    a) Use a clear definition of security incidents and events, across the organization

    b) Perform better and more consistent reporting, as it is better defined

    c) Follow procedures for making changes and improvements due to thorough incident handling processes

2. **Set goals and measure them.** When performing exercises, setting various goals and measuring the achievement of said goals before, during, and after an exercise, provides valuable data. This data can enable an organization to:

    a) Make it easier to evaluate what works and what does not, in terms of exercising

    b) Use data to present the cost-benefit of performing exercises to management, which may lead to increased management commitment and prioritization

    c) Collected data may give a realistic view on the organizations state regarding a specific topic (for example information security), and that view may cause management to take action

3. **Perform continual and consecutive exercises.** Research indicates that to get the most benefit from the cost, one needs to exercise continually, learn from previous exercises, and evolve the exercises based on experience. This is what's called double-loop learning. This may lead an organization to:

    a) Stop performing single exercises, costing resources and having little to no effect

    b) Perform double-loop learning and evolve as a learning organization

    c) Ensure solid and long-lasting improvements when the organization underlying causes of problems and initiate actions to solve them

    d) Get increasingly better effect of consecutive exercises as organizational and individual learning improves

4. **Take actions for improving communication and collaboration.** A goal should be that all employees have the same informed perception of the organization's current state and situation, in relation to security threats and a range of other areas. Conducting awareness campaigns on various topics can do this. More openness and collaboration can lead to:

    a) A more unified organization where employees have the same perception of situations

    b) A more informed employee base will also be a more knowledgeable employee base

    c) Better communication and collaboration can lead to improved employee involvement

    d) Exchange of knowledge, information and experiences between employees is value to the organization

5. **Implement an organizational learning framework and apply learning techniques:**

    a) Performing preparedness exercises is a form of experimental learning, and can lead to cost-reductions as organizations develop expertise and practices to reduce mistakes [RWH09]

    b) Implementing the 4I Framework can create tension between assimilating new learning and exploiting what has already been learned, and this type of strategic renewal is a useful characteristic as it is expected that lessons learned from security incidents will challenge an organizations compliance culture [AMS15, TRA10]

    c) Advancing from single-loop learning to double-loop learning is a great step in the way of taking actions to change systems, procedures and policies based on experiences [AS92, Lin15]. An advanced learning organization may advance further to triple-loop learning and use information to help the organization understand more about themselves and other regarding perceptions and beliefs [24r08].

6. **Learn from, or use, external exercise facilitators.** Information collected in this research indicate that the external exercise facilitators are more experienced at performing exercises, and have a more robust framework around the conduction of an exercise. They can also provide an outside-view of an organizations performance, and provide valuable feedback. As a provider of preparedness exercise services an external exercise facilitator will also often have mechanisms in place in order to measure the effect of said exercise, in order to sell the service to potential clients.

6.4 Limitations

Finally, we will discuss some limitations related to the study that is presented in this thesis. In case studies, one of the main challenges is to ensure validity of the collected and presented data.

External Validity

There are some potential pitfalls and weaknesses with performing qualitative case studies. As the study includes a small number of participants, there is no way of concluding with a statistical generalization based on this study alone [Yin13]. However, if several similar studies reach the same conclusions, some generalization is possible. Results from this study align with earlier studies [LM15, Lin15, HT13, GC14, SWF10, Gås14].

Construct Validity

When performing qualitative interviews, there is always the potential of biases. The knowledge of information security and incident management vary amongst interviewees, and may taint the provided answers. Some of the questions asked are opinion-based, and many factors can play in how they are answered. The textual conduction of the interviews restricting two-way communication increased the challenge of having uncommunicative or over-communicative interviewees [CS04]. There is also the challenge of performing a neutral analysis of the material, as the interpretation of the qualitative data is based on researchers background.

Chapter 7 Conclusion

7.1 Summary

The purpose of this thesis was to get two different perspectives, the DSOs and the facilitators, on the effects and challenges of performing information security exercises, and how organizations learn from exercises and other experiences. This has been done by conducting five main interviews and 14 small interviews. Three Norwegian DSOs and two Norwegian exercise facilitators have contributed to the main interviews, and 14 exercise participants from the DSOs organizations. The study of the DSOs are based on previous research looking at the collaboration during an exercise of fall 2014, performed in these organizations [LM15]. The two exercise facilitators were interviewed to get a professional view and an outside-perspective of the challenges and routines involved in performing exercises for other organizations.

The main findings of this study show that the organizations involved are improving on the topics of performing IT related exercises, and having an increased organizational focus and awareness of information security. However, there is still a long way to go. Guidelines and standards are in place, but are not necessarily followed. Reporting mechanisms are still not that well established, as also pointed out by earlier research [HT13]. Many participants reports that inter-organizational communication and collaboration has improved, but there are lots of room for improvement. The challenge of communication and collaboration was the main focus of the research this thesis is based upon [LM15]. Challenges with performing exercises are dominated by availability of time, resources, and personnel, which are challenges that can be interpreted as lack of management commitment. The technical challenge of performing exercises for DSOs were also prominent, as their industry-specific IT systems needs to be operational 24/7 and can therefore not be used when performing exercises.

One of the findings that is of great relevance for the objectives in this thesis, is the lack of measuring the exercise learning effect. Apart from one of the experienced facilitators, none of the organizations report to measuring the effect of performing exercises in any quantifiable way. Not only does this give this thesis less hard facts to work with, but it does not provide the organizations any visuals on the cost-effect ratio of their exercise performances. The most important finding from this thesis is the lack of measured effect from exercises, which makes it hard to put an actual value on performing exercises versus the potential harm of letting be.

By evaluating the challenges revealed by the 19 interviews, a set of recommendations has been developed. The recommendations for the DSO participants are:

1. Follow the established standards and guidelines,
2. Set goals and measure them,
3. Perform continual and consecutive exercises,
4. Take actions for improving intra-organization communication and collaboration,
5. Implement an organizational learning framework and apply learning techniques, and
6. Learn from, or use, external exercise facilitators.

7.2 Future Work

This study has revealed similar exercise and learning challenges as previous research [LM15, HT13, Lin15, GC14], using the same type of organizations as research object. It would be enriching to ask the same set of questions to organizations operating in completely different domains, and draw lines between the similarities and differences in the challenges met. A larger interview study with more interviewees and follow-up interviews could be valuable. Getting a larger set of data points to work with, and the potential of doing follow-up interviews, provides the possibility of performing a more in-depth analysis of why the interviewee has those specific opinions.

Based on the results presented in this thesis, and with more time and resources, a larger project aiming to measure the actual effect of performing exercises could be conducted. Of the background literature read for this thesis, no such studies were found. This should be highly interesting for future researchers wanting organizations to get more robust and prepared for emergency, both inside IT and in other fields. A study like this could involve creating measurable goals, creating and performing an (information security) preparedness exercise in a number of organizations, provide participants with measurable questionnaires, and collect and analyze the data.

References

[24r08] 24reasons. Single, double and triple loop learning. *Youtube, retrieved: 12. Nov 2015*, Aug 2008.

[AHR12] Atif Ahmad, Justin Hadgkiss, and Anthonie B Ruighaver. Incident response teams–challenges in supporting the organisational security function. *Computers & Security*, 31(5):643–652, 2012.

[AMS15] Atif Ahmad, Sean B Maynard, and Graeme Shanks. A case analysis of information systems and security incident responses. *International Journal of Information Management*, 35(6):717–723, 2015.

[AS92] Chris Argyris and Donald A Schön. *On organizational learning.* Blackwell Cambridge, MA, 1992.

[AS97] Ch Argyris and Donald A Schön. Organizational learning: A theory of action perspective. *Reis*, pages 345–348, 1997.

[BBF+14] D Batchelder, J Blackbird, D Felstead, P Henry, J Jones, and A Kulkarni. Microsoft Security Intelligence Report, 2014.

[cer12] ENISA - CERT Exercises Handbook. *European Network and Informaton Security Agency*, November 2012.

[CLW99] Mary M Crossan, Henry W Lane, and Roderick E White. An organizational learning framework: From intuition to institution. *Academy of management review*, 24(3):522–537, 1999.

[CS04] Catherine Cassell and Gillian Symon. *Essential guide to qualitative methods in organizational research.* Sage, 2004.

[DS99] Axel Daneels and Wayne Salter. What is SCADA? 1999.

[eni10] ENISA - Good Practice Guide for Incident Management. *European Network and Informaton Security Agency*, 2010.

[ESSG98] Mark Easterby-Smith, Robin Snell, and Silvia Gherardi. Organizational learning: diverging communities of practice? *Management learning*, 29(3):259–272, 1998.

[fir] FIRST – Forum of Incident Response and Security Teams. https://www.first.org/about. Accessed: 2015-12-10.

[For01] Forsvarsdepartementet. Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). https://lovdata.no/dokument/NL/lov/1998-03-20-10, 2001. Accessed: 2015-12-02.

[Gås14] Stian Gåsland. Gjør øvelse mester? om læringsfaktorer i beredskapsøvelser initiert av nve. *Institutt for Statsvitenskap, Det Samfunnsvitenskapelige Fakultet, Universitetet i Oslo*, 2014.

[GC14] Ingrid Graffer and Henriette Victoria Chiem. Computer Preparedness Exercises. *Institutt for telematikk*, 2014.

[GKK04] Tim Grance, Karen Kent, and Brian Kim. Special Publication 800-61: Computer Security Incident Handling Guide. *Recommendations of the National Institute of Standards and Technology (NIST)*, January 2004.

[GNB+06] Timothy Grance, Tamara Nolan, Kristin Burke, Rich Dudley, Gregory White, and Travis Good. SP 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. *National Institute of Standards & Technology*, 2006.

[Gor05] Carol Gorelick. Organizational learning vs the learning organization: a conversation with a practitioner. *The Learning Organization*, 12(4):383–388, 2005.

[HT13] Cathrine Hove and Marte Tårnes. Information security incident management: an empirical study of current practice. *Institutt for telematikk*, 2013.

[HWR+00] J Richard Hackman, Ruth Wageman, Thomas M Ruddy, Charles R Ray, C Cooper, and EA Locke. Team effectiveness in theory and practice. *Industrial and organizational psychology: Theory and practice*, 2000.

[ISO09] ISO/IEC. ISO/IEC 31000:2009 Risk management - Principles and guidelines. *International Organization for Standardization*, 2009.

[ISO11a] ISO/IEC. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. *International Organization for Standardization*, 2011.

[ISO11b] ISO/IEC. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management. *International Organization for Standardization*, 2011.

[ISO12] ISO/IEC. ISO/IEC 22301:2012 Societal security – Business continuity management systems — Requirements. *International Organization for Standardization*, 2012.

[ISO13] ISO/IEC. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. *International Organization for Standardization*, 2013.

[ISO14] ISO/IEC. ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary. *International Standard*, 2014.

[Kav83] S Kavale. The qualitative research interview: a phenomenological and a hermeneutic model of understanding. *Journal of Phenomenological Psychology*, 14(1983):171–196, 1983.

[KC04] Andrew G Kotulic and Jan Guynes Clark. Why there aren't more information security research studies. *Information & Management*, 41(5):597–607, 2004.

[Kra11] Patrick Kral. SANS - The Incident Handlers Handbook. *SANS Institute*, December 2011.

[Lin15] Maria Bartnes Line. *Understanding Information Security Incident Management Practices: A Case Study in the Electic Power Industry.* PhD thesis, Norwegian University of Science and Technology, April 2015.

[LM88] Barbara Levitt and James G March. Organizational learning. *Annual review of sociology*, pages 319–340, 1988.

[LM15] 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.

[LTJ14] Maria B Line, Inger Anne Tøndel, and Martin Gilje Jaatun. Information security incident management: Planning for failure. In *IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on*, pages 47–61. IEEE, 2014.

[Mar14] Louis Marinos. ENISA Threat Landscape 2014 – Overview of current and emerging cyber-threats. *ENISA Threat Landscape 2014*, 2014.

[MD06] Allan McConnell and Lynn Drennan. Mission impossible? planning and preparing for crisis. *Journal of Contingencies and Crisis management*, 14(2):59–70, 2006.

[MN07] Michael D Myers and Michael Newman. The qualitative interview in IS research: Examining the craft. *Information and organization*, 17(1):2–26, 2007.

[NIS03] SP NIST. NIST SP 800-53: Recommended Security Controls for Federal Information. *National Institute of Standards and Technology*, 2003.

[ob01] Justis og beredskapsdepartementet. Lov om behandling av personopplysninger (personopplysningsloven). https://lovdata.no/dokument/NL/lov/2000-04-14-31, 2001. Accessed: 2015-12-02.

[oe91] Olje og energidepartementet. Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven). https://lovdata.no/dokument/NL/lov/1990-06-29-50, 1991. Accessed: 2015-12-03.

[oe13] Olje og energidepartementet. Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften). https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157, 2013. Accessed: 2015-12-03.

[oo01] Helse og omsorgsdepartementet. Lov om helsemessig og sosial beredskap (helseberedskapsloven). https://lovdata.no/dokument/NL/lov/2000-06-23-56, 2001. Accessed: 2015-12-02.

[PL00] Micha Popper and Raanan Lipshitz. Organizational learning mechanisms, culture, and feasibility. *Management learning*, 31(2):181–196, 2000.

[RWH09] Lyndsay Rashman, Erin Withers, and Jean Hartley. Organizational learning and knowledge in public service organizations: A systematic review of the literature. *International Journal of Management Reviews*, 11(4):463–494, 2009.

[Sam14] Samferdselsdepartementet. Lov om elektronisk kommunikasjon (ekomloven). https://lovdata.no/dokument/NL/lov/2003-07-04-83, 2014. Accessed: 2015-12-02.

[SBWP+10] Marianne Swansen, Pauline Bowen, Amy Wohl Philips, Dean Gallup, and David Lynes. NIST SP 800-34: Contingency Planning Guide for Federal Information Systems. *National Institute of Standards and Technology*, 2010.

[Sec13] Homeland Security. Homeland Security Exercise and Ecaluation Program (HSEEP). *Homeland Security*, April 2013.

[SFS08] Keith Stouffer, Joe Falco, and Karen Scarfone. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment. *National Institute of Standards and Technology*, 2008.

[Sik14] Næringslivets Sikkerhetsråd. Mørketallsundersøkelsen – informasjonssikkerhet, personvern og datakriminalitet. *Mørketallsundersøkelsen 2014*, 2014.

[Sik15] Nasjonal Sikkerhetsmyndiget. NSM Risiko 2015. *NSM Risiko 2015*, 2015.

[SM11] Frederick Scholl and Michael Mangold. Proactive incident response. *The Information Systems Security Association Journal*, Feb 2011.

[SSU+13] Truls Sønsteby, Frank Skapalen, Helge Ulsberg, Roger Steen, et al. Beredskapsforskriften: Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen. *Norges Vassdrags- og Energidirektorat*, July 2013.

[SWF10] Lars Arne Sand, Gaute Bjørklund Wangen, and Anders Sand Frogner. Hendelseshåndtering i små og mellomstore bedrifter. *Avdeling for informatikk og medieteknikk, Høgskolen i Gjøvik*, 2010.

[TE14] Kripos Taktisk Etterforskningsavdeling. Den Organiserte Kriminaliteten i Norge - Trender og Utfordringer. *Kripos*, 2013-2014.

[TRA10] Terence CC Tan, Anthonie B Ruighaver, and Atif Ahmad. Information security governance: when compliance becomes more important than security. In *Security and Privacy–Silver Linings in the Cloud*, pages 55–67. Springer, 2010.

[ulosmN13] Norconsult under ledelse og samarbeid med NVE. Øvelser - En veiledning i planlegging og gjennomføring av øvelser i NVE. *Norges Vassdrags- og Energidirektorat*, 2013.

[Yin13] Robert K Yin. *Case study research: Design and methods.* Sage publications, 2013.

Appendix A
Interviews of the Power Industry

In this section we present the interview questions asked the three DSO's. The former is the questions asked to the representative responsible for the execution of the exercise, and the latter is the questions asked to the exercise participants. The questions are presented in Norwegian, as was the original language of the interviews, and an English translation is provided as well.

A.1 Questions for the Representative Responsible for the Exercise

A.1.1 In Norwegian (Original Language)

Informasjon om bedriftens generelle beredskapsplan

1. Hvilke standarder og prosedyrer benyttes i deres beredskapsarbeid? (ISO/IEC, NIST, SANS, ENISA etc.)
2. Hvor ofte utføres øvelser med andre scenarioer enn IT-sikkerhet?
   a) Hvilken type øvelse brukes? (skrivebordsøvelser, simuleringer, etc.)
3. Har erfaring fra en øvelse hjulpet i en reell hendelse?
   a) Hvis ja, på hvilken måte?

   Læring fra øvelse

4. Hva gjøres i etterkant av en øvelse?
   a) Har dere rutiner for forbedring av prosedyrer for hendelseshåndetring basert på en øvelse?

   b) Har dere rutiner for forbedring av videre øvingsopplegg basert på en øvelse?

5. Hvordan evaluerer dere en øvelse?

6. Gjøres forbedringer/justeringer av prosedyrer basert på læring fra relle hendelser?

   a) Hvis ja, hvordan?

7. Har du opplevd noen utfordringer med å oppnå læring fra en øvelse?

   a) Hvis ja, hvordan?

IT-sikkerhet

8. Hvor ofte forekommer IT-sikkerhetshendelser i din bedrift?

9. Har det blitt utført noen ny øvelse knyttet til IT-sikkerhet etter NVE-øvelsen høsten 2014?

   a) Hvis ja: Hvordan var denne øvelsen lagt opp sammenlignet med den forrige?
   b) Hvis nei: Hvorfor ikke?

Om NVE-øvelsen

10. Hva ble gjort i etterkant av NVE's øvelse høsten 2014?

    a) Har noen nye rutiner blitt iverksatt?

11. Har dere i løpet av det siste året opplevd at hendelser har blitt mer effektivt håndtert som følge av at dere gjennomførte en øvelse i fjor høst?

12. Er det noen spesifikke utfordringer knyttet til å utføre IT-sikkerhetsøvelser i det domenet du jobber i? Hvorfor, hvorfor ikke?

A.1.2 English Translation

Information about the company's overall preparedness plan

1. What standards and procedures are used in your preparedness work? (ISO/IEC, NIST, SANS, ENISA etc.)

2. How often do you perform exercises with other scenarios than IT-security?

   a) What types of exercises are used? (table-top, simulations etc.)

3. Has experience from one exercise helped the solving of a real incident?

   a) If yes, in what way?

Learning from exercises

4. What is being done in the aftermath of an exercise?

   a) Do you have routines for improving procedures for incident management based on an exercise?
   b) Do you have routines for improvement of further training programs based on an exercise?

5. How do you evaluate an exercise?

6. Do you make improvements / adjustments of procedures based on lessons learned from real events?

   a) If yes, how?

7. Have you experienced any challenges in achieving learning from an exercise?

   a) If yes, how?

IT-security

8. How often does IT security incidents occur in your company?

9. Has there been conducted any new exercises related to IT security after the NVE-exercise of fall 2014?

   a) If yes How was this exercise performed compared with the previous one?
   b) If no: Why not?

The NVE Exercise

10. What was done on the wake of the NVE exercise in fall 2014?

    a) Has any new procedures been implemented?

11. Have you during the last year experienced the events have been more effectively managed as a result of that you conducted an exercise last fall?

12. Are there any specific challenges to perform IT security exercises in the domain you work in? Why, why not?

A.2 Questions for the Exercise Participants

A.2.1 In Norwegian (Original Language)

Hei!

Mitt navn er Kine Johnsrud, og jeg skriver masteroppgave for NTNU som omhandler evaluering og læring av IT-sikkerhetsøvelser. I fjor høst utførte dere en IT-sikkerhetsøvelse basert på et scenario fra NVE, og Maria var med som observatør ifbm sitt doktorgradsarbeid. Jeg håper du kan ta deg tid til å svare på 7 spørsmål som omhandler etterarbeidet etter denne øvelsen.

Om NVE-øvelsen

1. Opplevde du endringer i rutiner eller arbeidsoppgaver i etterkant av øvelsen høsten 2014?
   a) Hvis ja, hvilke?
2. Har det blitt utført flere øvelser med fokus på IT og sikkerhet?
3. Har dere i løpet av det siste året opplevd at hendelser har blitt mer effektivt håndtert som følge av at dere gjennomførte en øvelse i fjor høst?
4. Er det noen spesifikke utfordringer knyttet til å utføre IT-sikkerhetsøvelser i det domenet du jobber i?
   a) Hvorfor, hvorfor ikke?

   Vurdering av øvelsen

5. På hvilken måte har øvelsen endret organisasjonens evne til å håndtere IT-sikkerhetshendelser?
6. Har øvelsen ført til økt informasjonsutveksling og samarbeid på tvers av organisasjonen?
7. Har du diskutert øvelsen med kollegaer i etterkant?

A.2.2 English Translation

Hi!

My name is Kine Johnsrud, and I am writing a master's thesis for NTNU concerning evaluation and learning from IT security preparedness exercises. Last fall you performed an IT security preparedness exercise based on a scenario made by NVE, and Maria was present as an observer in conjunction with her doctorate. I hope you can take your time to answer 7 questions that concerns the supplementary work of this exercise.

The NVE Exercise

1. Did you experience changes in procedures or tasks after the exercise in fall 2014?
   a) If yes, which?
2. Has it been performed any additional exercises with focus on IT and security after the fact?
3. Have you during the last year experienced that events have been more effectively managed as a result of that you conducted an exercise last fall?
4. Are there any specific challenges to perform IT security exercises in the domain you work in?
   a) Why, why not?

   Evaluation of the exercise

5. In what way has the exercise changed the organization's ability to manage IT security incidents?
6. Has the exercise led to increased information sharing and collaboration across the organization?
7. Have you discussed the exercise with your colleagues in the aftermath?

Appendix B Interviews of the Exercise Facilitators

In this section we present the interview questions asked the two exercise facilitators. The questions are presented in Norwegian, as was the original language for the interviews, and an English translation is provided as well.

B.1 Questions for the Exercise Facilitators

B.1.1 In Norwegian (Original Language)

Hei! Jeg skriver masteroppgave for NTNU som omhandler læringseffekten ved, og utføringen av, beredskapsøvelser for IT-sikkerhet i bedrifter. I den forbindelse håper jeg at du kan svare på et sett spørsmål rettet mot det å være øvingsleder, og erfaringer knyttet til dette. Er det noe du føler jeg mangler å ha spurt om eller andre ting du lurer på, så er det bare å si ifra.

Innledende faktaspørsmål

1. Hvor mange år har du jobbet med øvingsfasilitering (som øvingsleder)?

2. Cirka hvor mange øvelser har du vært med å arrangere?

   a) Hvor mange av disse har omhandlet informasjonssikkerhet?

3. Hvilke standarder og prosedyrer benyttes i ditt arbeid? (ISO/IEC, NIST, SANS, ENISA, etc.)

4. I hvilken grad er du med på å gjennomføre endringer i bedriften i etterkant av en øvelse?

   a) Hva slags endringer kan det være snakk om?

Generelt om øvelser

5. Kan du si noe om utfordringer ved å utføre øvelser generelt?
6. Kan du nevne noen spesifikke utfordringer med å utføre informasjonssikkerhetsøvelser?
7. Er det noen spesielle utfordringer knyttet til å få kunder til å se nytteverdien av en informasjonssikkerhetsøvelse?

    a) Hvis ja, er det noen bransjer som stikker seg ut?

Læring fra øvelser

8. Hvordan evalueres en øvelse?

    a) Hva slags metoder brukes?

    b) Hvilke "metrics" brukes?

9. Lages det noen statistiske data på dette jeg kunne fått tilgang til? (evt. en offisiell uttalelse om hvor snittet ligger)
10. Hva blir gjort i etterkant av en øvelse?

    a) Brukes erfaringen fra en øvelse som grunnlag for neste øvelse? Hvis ja, hvordan?

11. Utfordringer ved læring fra øvelse:

    a) Hva kan være utfordringen med å forbedre en øvelse?

    b) Hva kan være utfordringen med å forbedre hendelshåndteringsprosessen til en bedrift?

    c) Andre utfordringer?

B.1.2 English Translation

Hi! I am writing a master's thesis for NTNU concerning the learning effect of, and execution of, preparedness exercises for IT security in organizations. In that regard, I hope that you can answer a set of questions aimed at being an exercise leader, and experiences related to this. If there's anything you feel I haven't asked or anything else you are wondering about, let me know

Introductory facts

1. How many years have you worked as an exercise leader / exercise facilitator?
2. How many exercises have you executed?
    a) How many of these have been related to information security?
3. What standards and procedures are used in your work? (ISO/IEC, NIST, SANS, ENISA, etc.)
4. To what extent are you involved in implementing changes in the company in the aftermath of an exercise?
    a) What kind of changes can this be?

About exercises

5. Can you say anything about the challenges of performing exercises in general?
6. Can you mention any specific challenges of perform IT security exercises in specific?
7. Are there any particular challenges related to getting customers to see the usefulness of an information security exercise?
    a) If yes, are there any industries that sticks out?

Learning from Exercises

8. How is an exercise evaluated?
    a) What kind of methods are used?
    b) What kind of metrics are used?
9. Are there any statistical data on this that I can get access to?
10. What is done in the aftermath of an exercise?
    a) Are experiences from one exercise used as a basis for making the next exercise? If yes, how?
11. Challenges with learning from exercises:
    a) What can be challenging with learning from an exercise?
    b) What can be challenging with improving the incident management process of an organization?
    c) Other challenges?