NTNU – Trondheim
Norwegian University of
Science and Technology

Information Security Incident Management

An Empirical Study of Current Practice

Cathrine Hove
Marte Tårnes

Master of Science in Communication Technology
Submission date: June 2013
Supervisor: Karin Bernsmed, ITEM
Co-supervisor: Maria Line, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem Description

In recent years, an increasing number of information security incidents have been reported. Typical incidents include both general and single-purpose attacks caused by malware, in addition to minor errors with severe consequences. Hence, organizations need to be prepared to handle incidents caused by both known and unknown vulnerabilities. Several well-established standards and guidelines addressing incident management exist. A number of factors are involved in determining how successfully organizations respond to information security incidents.

The main research question of this thesis is as follows:

- How do organizations perform information security incident management in practice?

The main research question is further divided into sub-questions. A solid basis for discussing the main research question will be established by answering the following questions:

- What plans and procedures for information security incident management are established in organizations?
- To what extent are existing standards/guidelines adopted in plans for information security incident management?
- To what extent have previous information security incidents been handled in accordance with predetermined plans?

In order to answer the research questions, information on incident management in various organizations as well as about actual incidents will be gathered. Experiences from a variety of incidents will be systematized and a study of incident handling processes will be performed.

Students:	Cathrine Hove and Marte Tårnes
Assignment given:	21. January, 2013
Supervisor:	Maria B. Line
Responsible professor:	Karin Bernsmed

Abstract

An increasing use of digital solutions suggests that organizations today are more exposed to attacks than before. Recent reports show that attacks get more advanced and that attackers choose their targets more wisely. Despite preventive measures being implemented, incidents occur occasionally. This calls for effective and efficient information security incident management. Several standards and guidelines addressing incident management exist. However, few studies of current practices have been conducted. In this thesis an empirical study was conducted where organizations' incident management practices were studied. The research was conducted as a case study of three large Norwegian organizations, where the data collection methods were interviews and document studies. Our findings show that the organizations were relatively compliant with standards and guidelines for incident management, but that there was still room for improvements. We found communication, information dissemination, employee involvement, experience and allocation of responsibilities to be important factors to an effective and efficient incident management process. Finally, we contribute with recommendations for performing successful information security incident management. We recommend organizations to use standards and guidelines as a basis for incident management, conduct regular rehearsals, utilize employees as part of the sensor network in incident detection and to conduct awareness campaigns for employees.

Sammendrag

En økende bruk av digitale løsninger tyder på at virksomheter i dag er mer utsatt for angrep enn før. Rapporter viser at angrep blir stadig mer avanserte og at angripere velger sine mål med omhu. Hendelser forekommer til tross for implementering av forebyggende tiltak. Dette setter krav til en effektiv hendelseshåndtering. Det finnes flere standarder og retningslinjer som omhandler hendelseshåndtering, men det har blitt gjennomført få praktiske studier av virksomheters hendelseshåndtering. I denne masteroppgaven ble en empirisk studie utført for å kartlegge virksomheters hendelseshåndtering. Studien ble gjennomført som et case studie av tre store norske virksomheter hvor datainnsamlingsmetodene var intervjuer og dokumentstudier. Våre funn viser at virksomhetene var relativt kompatible med standarder og retningslinjer for hendelseshåndtering, men at det fremdeles var rom for forbedringer. Vi fant at kommunikasjon, distribusjon av informasjon, involvering av ansatte, erfaring og fordeling av ansvar var viktige faktorer for en effektiv hendelseshåndtering. Vi bidrar med anbefalinger for å utføre en vellykket hendelseshåndteringsprosess. Noen av våre anbefalte tiltak er å bruke standarder og retningslinjer som et grunnlag for hendelseshåndteringsprosessen, utføre øvelser, benytte ansatte som en del av sensornettverket for å detektere hendelser og utføre holdningsskapende kampanjer for de ansatte.

Preface

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

We would like to thank our supervisor Maria B. Line and our professor Karin Bernsmed for valuable comments and guidance throughout this work. Their contributions have been invaluable. We would also like to thank all participating organizations and all the interviewees who took the time to participate in the case study.

Trondheim, June 6th, 2013

Cathrine Hove and Marte Tårnes

Contents

List of Figures

List of Tables

Acronyms

AFP Australian Federal Police

CERT Computer Emergency Response Team

CIM Critical Incident Management

CIRT Computer Incident Response Team

CSIRC Computer Security Incident Response Capability

CSIRT Computer Security Incident Response Team

DDoS Distributed Denial of Service

ENISA European Network and Information Security Agency

HSE Health Safety and Environment

ICT Information and Communications Technology

IDP Intrusion Detection and Prevention

IDPS Intrusion Detection and Prevention System

IDS Intrusion Detection System

IEC International Electrotechnical Commission

IRISS Irish Reporting & Information Security Service

IRT Incident Response Team

ISIRT Information Security Incident Response Team

ISMS Information Security Management System

ISO International Organization for Standardization

IT Information Technology

ITIL Information Technology Infrastructure Library

NCIS National Criminal Intelligence Service

NHTCU National High Tech Crime Unit

NIST National Institute of Standards and Technology

NorCERT Norwegian Computer Emergency Response Team

NorSIS Norwegian Centre for Information Security

NSM Norwegian National Security Authority

PCeU Police Central e-Crime Unit

PoC Point of Contact

ROI Return On Investment

SLA Service Level Agreement

SME Small and Medium-sized Enterprise

USB Universal Serial Bus

USSS United States Secret Service

Chapter 1

Introduction

The occurrence of computer security incidents have been a known issue ever since the introduction of the PC. However, in recent years there has been an increased focus on information security incidents. Several major incidents have received attention in the media and drawn attention to the topic.

It is interesting to study how organizations perform incident management in practice. How organizations prepare for and handle information security incidents, comply with standards and learn from mistakes are of interest. We wanted to assess how various factors contribute to the efficiency and effectiveness of organizations' incident management. By identifying how these factors affect successful incident management, we hoped to find improvements to incident management practice for relevant organizations.

1.1   Why We Need Incident Management

Modern society shows an increasing use of digital solutions. Today, digital solutions are vital to most organizations' day-to-day operations and large amounts of sensitive data are stored digitally [1]. As the value and sensitivity of information increases, the number of potential threats increase accordingly. This suggests that organizations today are more exposed to attacks than before. This section discusses the current threat landscape and the need for plans in situations where systems have not been sufficiently secure.

Organizations are increasingly using and depending on information technology in their operations. Attacks get more advanced and attackers choose their targets more strategically. A significant challenge arises when new and severe security threats evolve faster than corresponding measures. This leads to an increasing gap between threats and security measures in organizations. To avoid severe consequences such as disclosure of sensitive information, this gap must be closed.

Despite organizations' implementation of information security policies and controls, it is inevitable that new vulnerabilities and information security incidents occur occasionally. Thus, it is essential that organizations have a structured and planned approach to detect, report, assess, respond to and learn from information security incidents [2]. Preventive actions are not sufficient and an incident management capability is therefore necessary.

> "Everybody should do what they can to protect themselves from being attacked, but the sad truth is that the most important thing you should plan and prepare for is how to behave when the attacker has succeeded"

> – Roar Thon, Senior Adviser NSM

The information security threat landscape is continuously changing and new types of security-related incidents emerge frequently [3].

NSM NorCERT[1] has registered a 30% increase in cases each year for the past few years. They have seen an increase in cases of all impact levels. In addition they believe that there is a large number of incidents not reported or discovered [6]. These findings are supported by Kripos[2], that reports ICT related crime to be expanding [1]. There is a large increase in targeted espionage operations directed towards Norwegian industry [8]. Attacks are mainly driven by Return On Investment (ROI), thus targets are chosen based on potential profit. Other incidents not necessarily motivated by money are strategic targets and domestic political monitoring as seen in China and Syria [9].

---

[1]NSM is the Norwegian National Security Authority and is a cross-sectional professional and supervisory authority within the protective security services in Norway [4]. NorCERT is the Norwegian Computer Emergency Response Team and is part of NSM. NorCERT coordinates preventive work and responses against IT security breaches aimed at vital infrastructure in Norway [5]

[2]Kripos is the National Criminal Intelligence Service (NCIS) in Norway and it is the unit for combating organized and other serious crime [7].

NSM states that the security condition in Norway for 2012 is not satisfactory [10]. This seems to be a continuing trend and the security condition for 2011 was summarized in the following way [11]:

> "The **values** we want to protect increase in amount, the **threats** are increasing, new **vulnerabilities** are constantly discovered, but **measures** to reduce these vulnerabilities are not developed at the same rate in addition to being inadequate."

Additionally, there is an increasing number of vulnerabilities discovered on smart phones and tablets, which represents a relatively new part of the threat landscape. There exist persistent vulnerabilities in organizations with classified information and these exist mainly due to lack of understanding of risks [8].

In 2012 NorCERT handled a large amount of serious cases related to espionage against Norwegian high-technology organizations [6]. In a recent report PST[3] expressed concerns related to Norwegian research and education environments being exploited to strengthen other nations' defences [12].

Many of the current threats cannot be stopped by antivirus software. Attacks are increasingly becoming targeted to specific organizations in addition to becoming more advanced. Delay in updates and patches of computers is a big problem for many organizations [13]. NSM has observed a change in attacks from random and opportunistic attacks to advanced and focused attacks on specific targets of high economic or social value. In addition to technical means, attackers use social engineering[4] to obtain sensitive information or to obtain access to systems [11]. Another trend is attacks that compromise legitimate websites and infect all users that visit them [8]. Such attacks are called water-holing. They are particularly difficult to protect against as these exploit websites that users are normally allowed to visit.

There is great diversification in type of attackers. Attackers can belong to foreign intelligence, traditional military, global businesses, terrorist organizations, hacker groups or they can operate individually [10]. Criminals are organized in new ways, and various participants contribute with services, making attacks possible [1]. It is even possible to buy attacks like

---

[3]The Norwegian Police Security Service

[4]Social engineering involves manipulating people into performing certain actions such as disclosing sensitive information.

Distributed Denial of Service (DDoS) attacks or spam distribution [13]. Attacks can also come from the inside, either from an insider or by social engineering, and many organizations do not focus on this threat [8]. This expands the group of possible attackers, in practice it includes everyone.

Several publications and recent reports highlight the need for incident management by pointing out deficiencies in organizations' information security. PST states that information security is given low priority in Norwegian government and private institutions [14]. This is supported by NSM that states that organizations seem to lack the ability and/or will to prioritize ICT-security [15]. Incident handling is often not prioritized and the severity of attacks are often not understood [13]. Management's knowledge of information security is often insufficient, which is unfortunate as this is key to commitment of the rest of the organization [6]. Systems for reporting security incidents to the management rarely exist and NSM almost always discover that incidents have occurred or are occurring when they perform inspections [11]. Many organizations have inadequate contingency plans related to information security. Organizations also omit to conduct rehearsals related to preventive security and omit to rehearse their contingency plans [8].

Several trends described here are not unique to Norway. Verizon Enterprise's RISK team published a report in cooperation with the United States Secret Service (USSS), the Dutch National High Tech Crime Unit (NHTCU), the Australian Federal Police (AFP), the Irish Reporting & Information Security Service (IRISS) and the Police Central e-Crime Unit (PCeU) of the London Metropolitan Police [16]. The report discusses data breaches in 2011 in 36 different countries. 855 incidents were analysed. It shows that 96% of the (reported) attacks were not particularly advanced. It also shows that 85% of the breaches took weeks or more to discover and that 92% of incidents were discovered by a third party. 86% of the breaches were caused by organized crime. Based on the cases reported to the involved organizations, 2011 seems to be the year with the second highest number of data losses since 2004. The results of this report indicate that the overall international security condition is not satisfactory.

This shows a complex threat landscape with a large variety of attackers and with organizations that are not sufficiently prepared. It is not realistic to believe that all incidents can be prevented. In addition, it is not economically feasible. Hence, it is evident that organizations need plans

and procedures to handle incidents *when* they occur. The existence of an incident response capability in an organization can assist them in rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited and restoring computing services [3].

1.2 Objectives

We aimed to draw attention to and increase awareness around incident management. By investigating how various organizations perform incident management, what plans and procedures are developed and to what extent these plans and procedures comply with standards, we also hoped to find potential improvements.

The main research question of this thesis is:

- How do organizations perform information security incident management in practice?

This research question is further divided into the following sub-questions:

- What plans and procedures for information security incident management are established in organizations?

- To what extent are existing standards/guidelines adopted in plans for information security incident management?

- To what extent have previous information security incidents been handled in accordance with predetermined plans?

1.3 Scope and Limitations

We collected information about three large Norwegian organizations' incident management processes by conducting qualitative interviews, document studies and a survey. We did not include any small or medium sized organizations, as we wanted to study large organizations since they are particularly exposed to targeted attacks and espionage. As we only included three organizations in our study, generalization was not possible. The reason for not including more organizations in our research was the time restrictions for this thesis.

1.4   Outline

Chapter 2 discusses the research method used for this study. Chapter 3
presents a background on information security incident management. It
explains what incident management is and provides a review of relevant
standards and guidelines. In chapter 4 the three organizations in the case
study are presented. The findings from the case study are presented in
chapter 5. Chapter 6 discusses the findings presented in chapter 5 and
compares these with the literature presented in chapter 3. Chapter 7 pro-
vides a conclusion of the findings as well as suggestions for future work. In
Appendix A the information sheet given to the participating organizations
can be found. Appendix B contains the interview guide used as a basis for
the collection of empirical data in this study. In Appendix C, the employee
survey is included. All of the appendices are written in Norwegian.

Chapter 2

Method

This section describes the research method for this thesis as well as reasons for the choices made. Further, ethical considerations and challenges are discussed.

2.1 Choice of Method

Figure 2.1 shows an overview of various research methods and three criteria that can be used to determine the appropriate research method. The criteria are: form of research question, whether the study requires control of behavioural events and if the study focuses on contemporary events. The defined research question for this study, as presented in section 1.2, is a so-called "how" question. As the goal of our study was to reveal current practices in organizations, we did not need control over behavioural events. This study's focus was mainly contemporary events. Some past events such as incidents that have occurred were relevant, but the main focus was on current practices. Based on this, case study emerged as the most suitable method for this study, as highlighted in the figure.

A case study is applicable to real-world organizations, which is what we wanted to study. An advantage is that it can deal with various kinds of evidence, such as documents, archival records, interviews and artefacts.

METHOD	(1) Form of Research question	(2) Requires Control of Behavioural Events?	(3) Focuses on Contemporary Events?
Experiment	how, why?	yes	yes
Survey	who, what, where, how many, how much?	no	yes
Archival Analysis	who, what, where, how many, how much?	no	yes/no
History	how, why?	no	no
Case Study	how, why?	no	yes

Figure 2.1: Choice of Research Method, modified from [17]

2.2 Qualitative research

A qualitative research method based on relatively few informants was used for this thesis. Unlike a quantitative approach where the use of questionnaires to gather information from a large number of participants is common, we wanted in-depth information from selected organizations. The qualitative research method enabled us to perform a rich and detailed analysis.

The use of a quantitative method would have made statistical generalization possible, but it would have been more difficult to gather in-depth information. A survey may be easier to ignore, than a request for a face-to-face interview and a quantitative approach may not have given answers from the type of organizations we wanted. It may additionally be easier to get sincere answers in a face-to-face interview. In an interview the possibility to explain the questions is there. This is not the case for a survey, and it can be difficult to construct unambiguous questions that provides sufficient data for the analysis.

Further, we used an inductive research approach which is defined as follows [18]:

Inductive research: The objective is to infer theories and patterns from observed data. Also called *theory-building* research.

In inductive research, researchers perform field studies followed by deriving theories from observations. This method is a contrast to deductive research where a theory is developed initially, followed by observations to evaluate it [19].

2.3   Case Study

This section describes case study as the chosen research method for this thesis. The content is derived from [17] where Yin defines a case study in the following way:

Case Study: An empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context.

The case study inquiry relies on multiple sources of evidence and benefits from the prior development of theoretical propositions to guide data collection and analysis.

The research process is illustrated in figure 2.2. As the figure shows, the process in linear, but iterative. This means that one can go back to previous phases if needed. The Plan phase consisted of identifying research questions and deciding to use case study as the research method for this study. The Design phase is about getting from initial questions to conclusions or answers. It is the logic that links the data to be collected to the initial questions of the study.

Yin presents tactics to maximize the quality of empirical research. He recommends to use multiple sources of evidence and to have key informants review a draft of the report. Both of these tactics were used in this study.

The choice between a single- and multiple-case belongs to the Design phase. Multiple-case is usually preferred and was chosen as the method for this study. Additionally each case may be embedded or holistic. An embedded case has more than one unit of analysis. The design for this study is a
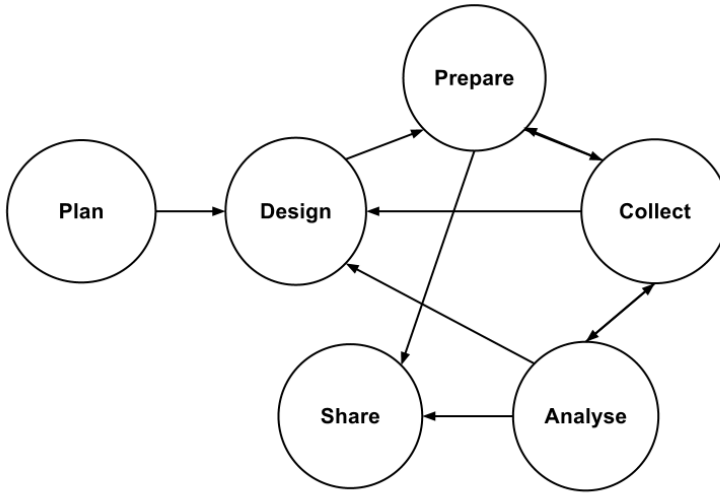
Figure 2.2: Case Study Research Process [17]

mix. It is a multiple-case study where one case has three embedded units of analysis and two cases are holistic. The design of our study is illustrated in figure 2.3.

The Preparation phase was very important as we did not have experience with the case study research method. The main activities performed in this phase were acquiring desired skills to become case study investigators and preparing for the specific case studies. It is considered difficult to obtain these skills as procedures are not routinised. It is advised to prepare to ask good questions, be a good "listener", be adaptive and flexible, have a firm grasp of the issues being studied and be unbiased by preconceived notions. We have performed a background study in order to get a thorough understanding of the issues in the study. Relevant background information is discussed in chapter 3 and the background study itself is briefly discussed in section 2.3.1.

Interviews, documents and surveys were chosen as the sources of information in the Collection phase. The use of multiple sources of evidence is consistent with the definition of a case study, which is presented in the beginning of this section. The interview is seen as being one of the most important sources of information in a case study. Documentary information is likely to be relevant in any case study. These data collection methods
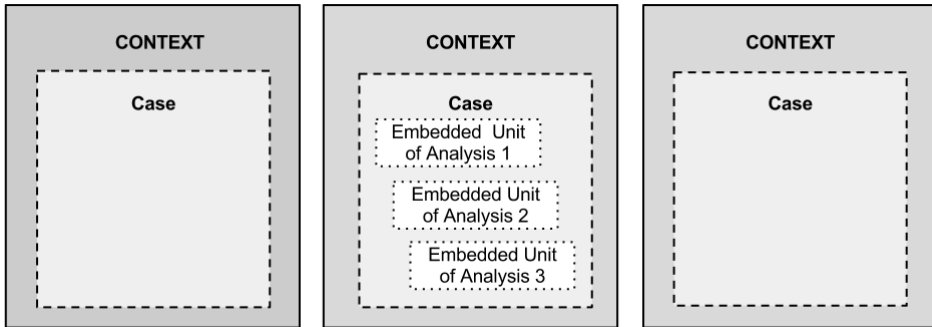
Figure 2.3: Case Study Design, modified from [17]

are described and discussed in sections 2.3.2, 2.3.3 and 2.3.4.

The Analyse phase is described in section 2.3.5.

The Share phase consisted of preparing, writing and editing this report. Choices such as to anonymize identities of individuals and individual organizations were part of this phase. This choice is further discussed in section 2.5. It was a choice that was made as part of the preparation of the study and this illustrates the arrow from Prepare directly to Share, and shows that the case study process is not purely linear.

2.3.1 Background Study

The first step in our research was a background study of incident management. We studied relevant literature such as standards and best practice guidelines to acquire sufficient knowledge. We focused on some of the well-established and internationally accepted ISO/IEC standards and documentation from the National Institute of Standards and Technology (NIST) in addition to a few other guidelines. As part of the background study we reviewed related work. The background study was used to guide the data collection. It was also used in the data analysis, by comparing standards and previously developed theory to the findings of this study. This is consistent with the definition of a case study, as presented in the beginning of section 2.3.

To gain additional knowledge and to get a realistic perspective on incident

management, we attended two conferences addressing information security: one arranged by the Norwegian National Security Authority (NSM)[1] and one arranged by The Norwegian Computer Society[2].

2.3.2   Qualitative Interviews

We chose to perform qualitative interviews as part of our research as they are a well-known and powerful tool for information collection in qualitative research [20]. The main objective of qualitative interviews is to see the research topic from the interviewees' perspective and understand why and how they got that particular perspective [21]. To meet this objective, qualitative interviews are driven by open questions, a low degree of structure and often focus on specific situations and experiences made by the interviewee.

We used what is referred to in literature as semi-structured interviews [21]. To ensure we got all necessary information we used an interview guide. The interview guide worked as an incomplete script and states the main goals for our research as well as the main research questions and topics for the interview. The interview guide can be found in Appendix B (in Norwegian).

Questions were not asked in any pre-defined order during interviews. This enabled us to ask follow-up questions and ask for elaborations on certain topics. When using semi-structured interviews, interviewees can be seen as being participants in the research, rather than objects only answering pre-defined questions.

The interviews were performed face-to-face and voice recorded. We believe that conducting interviews face-to-face helped build trust with interviewees and thus gave better and more elaborative answers. It also gave us the opportunity to explain and elaborate questions that were unclear. As we recorded all of the interviews we could focus on listening and thus ask valuable follow-up questions instead of being distracted by writing down answers. Additionally, we could listen to the recordings several times as needed and clarify things that were unclear later. Challenges related to qualitative interviews are discussed in section 2.6.

---

[1]NSMs sikkerhetskonferanse 2013
[2]Sikkerhet & Sårbarhet 2013

2.3.3 Document Study

In case studies, documents are often used to verify or to question data obtained from other data collecting methods. To complement information gathered from interviews we studied relevant academic literature, standards and organization-specific documents such as policies and plans. This enabled us to compare standards, plans and current practice of incident management in the participating organizations.

When using documents in research one should be aware of possible bias and other elements that could compromise reliability [19]. In our case study we looked at both public and confidential documents. We believe that by signing confidentiality agreements we were presented with authentic documents from the participating organizations. Nevertheless, we kept in mind that information could be outdated, not applicable or incorrect.

2.3.4 Employee Surveys

By studying documents and performing detailed interviews we got a thorough knowledge about routines related to incident handling. We found it interesting to examine how well these routines were established among the employees in the various organizations. To accomplish this we developed five main questions. These were asked to randomly selected employees who did not necessarily have any specific IT knowledge. The questions can be found in Appendix C (in Norwegian).

2.3.5 Qualitative Data Analysis

As discussed in section 2.2 we have chosen a qualitative and inductive research method. For the data analysis we used a "general inductive approach", as described by David R. Thomas [22]. He presents a systematic set of procedures for analysing qualitative data and explains a straightforward approach for deriving findings guided by research questions. We found this approach to be less complicated and more suitable than other approaches to qualitative data analysis such as grounded theory, phenomenology and ethnography research approaches [23].

Inductive analysis is often guided by predefined research objectives. The use of research questions as guidance in data analysis undoubtedly sets

constraints on the number of possible interpretations and outcomes as it
draws attention to specific aspects of the data. However, using the general
inductive approach rather than a stricter and more structured methodology,
enabled findings to emerge from themes inherent in the raw data despite
the pre-set research questions. Also, by using this approach, findings were
not restricted by the method used.

The main purposes of an inductive research approach are [22]:

- to condense raw textual data into a brief, summary format;

- to establish clear links between the evaluation or research objectives
  and the summary findings derived from the raw data and

- to develop a framework of the underlying structure of experiences or
  processes that are evident in the raw data.

The first one is fulfilled in chapter 5 where data from each individual case
are summarized. The last two are fulfilled in chapter 6.

In chapter 6, findings both directly linked to the research questions and
findings that emerged independently from the data are discussed. This is
compliant with the general inductive approach [22]:

> *"Although the findings are influenced by the evaluation objec-*
> *tives or questions outlined by the researcher, the findings arise*
> *directly from the analysis of the raw data, not from a priori*
> *expectations or models."*

As a first step in our analysis we perused the data and identified themes and
categories that we found related to the research questions. The process from
raw data to main findings and a conclusion can be outlined as follows:

1. Detailed readings of the qualitative data

2. Identifying specific themes that captured core messages given by par-
   ticipants.

3. Grouped themes into broader categories.

4. Primary findings are represented as a framework of themes.

To verify credibility of our findings we sent summaries of the interviews to
the participants. They were thereby given the opportunity to challenge our

interpretations and comment on whether our findings were in compliance with their personal experience.

2.4   Participants

The participating organizations in this study are all large Norwegian organizations. Their core activities belong to sectors identified by organizations such as NSM to be especially exposed to attacks. Additionally, a study from Gjøvik University College [24] found large organizations to be better at establishing information security policies, defining information security incidents, conducting rehearsals based on their incident management plans and facilitating anonymous reporting. This could indicate that they are experienced and well equipped to handle information security incidents. We found it interesting to examine how such assumed experienced organizations perform incident management and what challenges they face. Additionally, the participating organizations have quite different organizational structures, which we believed could lead to interesting findings.

2.5   Ethical Considerations

The main ethical concern related to our research was the potentially confidential information revealed during interviews. It is unlikely that organizations want details about their information security practices to be publicly known. Another important consideration was the privacy of the interviewees. Since a voice recorder was used during interviews, participants could potentially be identified later by voice recognition. To make sure that the participants knew exactly what they participated in, they were given information about how collected data was handled through a statement of consent. They were also given the right to withdraw from the study at any given time. This project was reported to the Norwegian Social Science Data services. The information sheet, including the statement of consent can be found in Appendix A (in Norwegian).

As we got insight into confidential documents, we had to sign confidentiality statements beforehand.

The term anonymization means that any information that could directly identify individuals or individual organizations is deleted and that any infor-

mation that indirectly could identify individuals or individual organizations is deleted or changed. No individuals or individual organizations are recognizable in this report. Participating organizations were given pseudonyms. All relations between individuals and individual organizations and results were anonymized at the end of the study, and only available to the students and partly the supervisors during the study. At the end of the study all recordings were deleted.

2.6   Challenges

This case study relied on qualitative information and it was challenging and time consuming to report all findings correctly. Furthermore, as the interviews were conducted in Norwegian, correct translation enhanced this challenge. Additionally, this type of research provides little basis for statistical generalization. [17]

For quantitative data there exist clear conventions for analysis, but there are fewer guidelines for analysing qualitative data. As Allen S. Lee pointed out in [25], "[...] the analyst faced with a bank of qualitative data has very few guidelines for protection against self delusion".

As most of the information collection was based on interviews, the challenges with this approach had to be considered. We had little or no experience in preparing and conducting qualitative interviews. We therefore tried to identify challenges and prepare the questions beforehand. Michael D. Myers and Michael Newman discussed potential challenges with qualitative interviews in [20]. They mentioned the artificiality of qualitative interviews where one interrogates a stranger that does not know or trust you. The lack of trust may cause the interviewee to withhold information that could be of value to the study. As an attempt to mitigate trust issues the procedure of handling data (anonymization) was presented and the fact that the project had been reported to the Norwegian Social Science Data Services was highlighted.

Problems could arise if too little time is assigned for interviews. Time constraints could cause questions to be rushed leading to interviewees giving inaccurate information or leaving out important information. To avoid time limitations being a problem, we assigned more time than estimated for each interview. We used the interview guide with predefined questions and topics

as well as correcting any misunderstandings during the interview to avoid ambiguous questions.

When relying on qualitative interviews for information, one has to consider potential interviewee bias as for instance incident management knowledge vary greatly among employees in an organization. In addition, Myers and Newman mentioned the possibility for interviewees to construct knowledge to appear knowledgeable and rational. By giving interviewees enough time to answer questions and carry out interviews as a dialogue, we hope to have avoided these problems.

One challenge of using qualitative data is that the interpretation of information is somewhat based on researchers' background. Both are master students in communication technology with specialization in information security. As students with similar backgrounds and limited experience we believe that choosing an inductive qualitative research approach gave less bias in our results since we did not aim at proving a specific theory, but rather aimed at starting our information collection with open minds. Our similar backgrounds could have led to limitations when analysing data due to a potentially narrow perspective. However, this was somewhat mitigated by discussions with our supervisor.

A challenge related to empirical research is that it relies on other people. We experienced that it was at times difficult to make contact with people and this led to at times slower progress than desired.

Chapter 3

Background

This chapter presents relevant background information with regard to incident management. An overview of incident management, relevant standards and guidelines as well as related research is presented.

3.1 Incident Management Overview

This section provides an overview of common concepts and terms used in incident management.

3.1.1 Definitions

In information security incident management there are a few terms that need to be defined clearly. Two such terms are information or computer security *incidents*[1] and information or computer security *events*. It is important to recognize these as two terms of different meaning. The standard ISO/IEC 27000[2] [26] specifies the following definitions:

---

[1] In this report the terms "information security incident", "computer security incident", "ICT security incident", "security incident" and "incident" are used interchangeably.

[2] ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

Information security: Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

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

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

Information Security Incident Response Team (ISIRT): Team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle.

The guidelines NIST Special Publication (SP) 800-61: Computer Security Incident Handling Guide [3] specifies the following definitions:

Event: An event is an observable occurrence in a system or network.

Adverse event: Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Computer security incident: A violation or imminent threat of violation[3] of computer security policies, acceptable use policies, or standard security practices.

NorCERT specifies the following definitions [6]:

Computer Security Incident Response Team (CSIRT): A central tool with the task of protecting important infrastructure. The team must consist of security specialists and they must handle and responds to incidents. Additionally, they need to create awareness and educators.

Computer Emergency Response Team (CERT): A trademark that can only be used after approval by Carnegie Mellon University. Is in practice the same as a CSIRT.

---

[3]An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur.

The definition of an adverse event from NIST [3] is quite similar to the definition of an information security event from ISO/IEC [26]. The definitions of incidents are also quite similar. These definitions are the ones that will be used in this report. ISIRT, CSIRT and CERT define similar types of teams. In this report the term IRT is used to denote such a team.

3.1.2 What is Incident Management

Incident management is a collective term that comprises all activities associated with managing security incidents. Incident management is not restricted to incident handling alone, but includes activities for the entire incident lifecycle; from planning, training and raising awareness to detecting, responding and learning from incidents.

Various guidelines and standards describe best practice and suggest activities for effective and efficient incident management. It is important to note that incident response requires a substantial amount of planning and resources. Two of the most important parts of incident management are the existence of guidelines for communication and prioritization of incidents as well as the use of an evaluation process to gain experience from previous incidents. [3]

As part of an incident management capability, organizations should have an incident management policy, a plan and procedures, all of which should be tailored to the specific organization's needs. Additionally, it is important to have a planned approach to reporting of vulnerabilities that have not yet been exploited. [2]

Incident management is not purely an IT related issue as information security incidents threaten an organization as a whole. Having a well-planned and tailored incident management capability is therefore important for organizations in order to protect information. Incident management seeks to both prevent, contain and resolve incidents, in addition to perform post-learning. ENISA states the following about incident management [27]:

> "Incident management is an important tool of overall governance and to have it, in whatever form or shape, is a necessity."

3.1.3   Incident Response Team

Having an Incident Response Team (IRT) will aid organizations in responding to incidents more effectively and efficiently, in addition to providing a structured approach for learning from previous incidents.

As the various definitions in section 3.1.1 indicate, an incident response team is "a team that responds to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution of them" [28]. The team structure, members, tasks and responsibilities may vary depending on organizations' resources and needs.

NIST recommends having one person in charge of incident response, taking the role as team manager. The team manager should act as a liaison to senior management and ensure that the team has the necessary resources, personnel and skills. It is recommended that team members have diverse backgrounds so they can handle different incidents that occur. The team manager should assess the situation and assign responsibility for incidents to the most appropriate team member. [3]

Usually teams consist of highly technically skilled persons, and teams should have at least one member with expertise in each major technological category. Good problem solving skills and communication skills are essential to the team as effective incident response requires collaboration and coordination within the team and throughout the organization. [3]

The structure of the team may vary. The number and frequency of incidents as well as team responsibilities should guide organizations' choice of team structure. However, whenever justified the ISO/IEC 27035 standard[4] recommends having a permanent team. [2]

Participating in a community of teams will be beneficial for teams due to collaboration on standards and procedures as well as information and resource sharing. To minimize the frequency of incidents and to mitigate negative impact caused by them, most IRTs do not only provide reactive services, but may also have other responsibilities, such as intrusion detection, advisory distribution, education and raising awareness within the organization. [3]

---

[4]ISO/IEC 27035 Information technology - Security techniques - Information security incident management

3.2 Standards and Guidelines

This section gives an introduction to the most relevant and widely implemented standards and guidelines for information security incident management.

3.2.1 The ISO/IEC 27001 Standard

This standard provides a model for establishing, implementing, operating, reviewing, maintaining and improving an Information Security Management System (ISMS). It states that management shall provide evidence of its commitment to the ISMS. This section presents clauses relevant to incident management that are directly retrieved from the standard [29].

4.2.2 Implement and operate the ISMS
The organization should do the following.

h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents.

This clause specifies that organizations should be able to detect and handle security incidents.

4.2.3 Monitor and review the ISMS
The organization shall do the following.

a) Execute monitoring and reviewing procedures and other controls to:

   2) promptly identify attempted and successful security breaches and incidents;

   4) help detect security events and thereby prevent security incidents by the use of indicators;

   5) determine whether the actions taken to resolve a breach of security were effective.

b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.

4.3.3 Control of records
Records shall be kept of the performance of the process as outlined in
4.2 and of all occurrences of significant security incidents related to the
ISMS

Common for all clauses in this standard is that they only specify that things
should be done, and not *how* they should be done. The ISO/IEC 27002
standard[5] provides a code of practice for information security management
and the ISO/IEC 27035 standard provides guidelines for the establishment
of information security incident management. These standards are further
described in sections 3.2.2 and 3.2.3 and can be used as aids to fulfil the
clauses presented in the ISO/IEC 27001 standard.

3.2.2   The ISO/IEC 27002 Standard

This standard represents a code of practice for information security man-
agement and establishes guidelines for initiating, implementing, maintain-
ing and improving information security management in an organization.
The standard is intended to be a starting point for developing organiza-
tion specific guidelines and contains 11 security control clauses that out-
line various security objectives and provide implementation guidance. It is
emphasized that organizations should initially identify and establish their
security requirements and then choose which of the security controls to
implement.

This section presents clauses from the standard that are relevant to incident
management. They are retrieved from [30].

13.1 Reporting information security events and weaknesses
The objective is to ensure that all significant information security events
and weaknesses are reported such that corrective actions can be made in
time. Reporting procedures and employee awareness are important success
factors and it should be required to report any events or weaknesses to the
point of contact as quickly as possible.

13.1.1 Reporting information security events
Control: Information security events should be reported through appropri-
ate management channels as quickly as possible.

---

[5]ISO/IEC 27002 Information technology - Security techniques - Code of practice for
information security management

Implementation guidance: A point of contact and a formal event reporting procedure should be established and employees should be made aware of these. The reporting procedure should include the following.

a) suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed.

b) information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event.

c) the correct behaviour to be undertaken in case of an information security event.

d) reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches.

13.1.2 Reporting security weaknesses
Control: All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Implementation guidance: There should exist an easy, accessible and available reporting mechanism for employees, contractors and third party users. Weaknesses should be reported as quickly as possible to either management or the service provider and not attempted to be proven.

13.2 Management of information security incidents and improvements
The objective is to ensure that the management of security incidents follows a consistent and effective approach where responsibilities and procedures are in place to handle incidents once they have been reported. Procedures should be in place for continual improvement of management processes. When necessary to collect evidence, this should be done in compliance with legal requirements.

13.2.1 Responsibilities and procedures
Control: Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.

Implementation guidance: In addition to reporting, monitoring should be

used to discover incidents. When implementing incident management procedures organizations should consider the following.

a) procedures should be established to handle different types of information security incidents, including:

   1) information system failures and loss of service.

   2) malicious code.

   3) denial of service.

   4) errors resulting from incomplete or inaccurate business data.

   5) breaches of confidentiality and integrity.

   6) misuse of information systems.

b) in addition to normal contingency plans, the procedures should also cover:

   1) analysis and identification of the cause of the incident.

   2) containment.

   3) planning and implementation of corrective action to prevent recurrence, if necessary.

   4) communication with those affected by or involved with recovery from the incident.

   5) reporting the action to the appropriate authority.

c) audit trails and similar evidence should be collected and secured, as appropriate, for:

   1) internal problem analysis.

   2) use as forensic evidence in relation to potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation.

   3) negotiating for compensation from software and service suppliers.

d) action to recover from security breaches and correct system failures should be carefully controlled. The procedures should ensure that:

   1) only certain identified and authorized personnel are allowed access to live systems and data.

2) all emergency actions taken are documented in detail.

3) emergency action is reported to management and reviewed in an orderly manner.

4) the integrity of business systems and controls is confirmed with minimal delay.

13.2.2 Learning from information security incidents
Control: There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Implementation guidance: By monitoring incidents, reoccurring and high impact incidents can be identified and need for additional controls can be evaluated.

13.2.3 Collection of evidence
Control: Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Implementation guidance: The rules of evidence involve admissibility and weight of evidence, that is whether or not evidence can be used in court and the quality and completeness of the evidence. To achieve admissibility and weight of evidence, organizations should ensure their systems comply with standards and that controls used to protect evidence are complete and consistent.

3.2.3 The ISO/IEC 27035 Standard

This section gives an introduction to the ISO 27035 standard and the content is, unless specified otherwise, derived from [2].

Implementing this standard will aid organizations in dealing with information security incidents properly and mitigate both direct and indirect adverse business impact. This standard provides an extensive and structured approach to incident management by presenting five phases with recommended activities for large and medium-sized organizations.

One of the standard's objectives is to provide guidelines to aid organizations in meeting the requirements specified in the ISO/IEC 27001 standard. The

ISO/IEC 27035 standard is a supplement to the implementation guidelines relevant to incident management that are presented in the ISO/IEC 27002 standard.

Plan and Prepare   This phase is by far the most extensive phase and involves many activities. Individual organizations have to ensure that their use of resources are proportional to their needs. Each organization should formulate an incident management policy that reviews current vulnerabilities, states the need for an incident management scheme and identifies benefits for the organization. Security and risk management policies should be reviewed and updated regularly. The standard highlights the importance of ensuring commitment from senior management in the security incident management policy to ensure the organization's commitment to resources and maintenance of an incident management capability.

One of the main activities in the plan and prepare phase is to make a detailed incident management scheme. The scheme should include reporting forms (preferably electronic) and a classification scale for grading incidents.

Another important activity in this phase is the establishment of the Information Security Incident Response Team (ISIRT). Organizations should establish and implement required mechanisms of support for their incident management scheme to operate efficiently during this phase. This includes technical tools such as Intrusion Detection Systems (IDSs) and log monitoring systems as well as relationships and connections to other organizations.

All personnel should be familiar with the incident management scheme, when it becomes operational and be able to recognize its benefits. Users' awareness and participation is essential for the success of a structured incident management approach. It is recommended that an appropriate awareness and training program is developed and repeated regularly as personnel change over time.

The entire incident management scheme should be tested to verify that the scheme and the ISIRT work in complex and real situations. After going through this phase, organizations should be fully prepared to manage security events, incidents and vulnerabilities.

Detection and Reporting   The first operational phase of an incident management scheme involves detection, collection of information and re-

porting of occurrences of security events, incidents and vulnerabilities either discovered by humans or automated systems. It is important to preserve information about vulnerabilities and incidents in a database operated and maintained by the ISIRT. Organizations should implement security monitoring systems, Intrusion Detection System/Intrusion Detection and Prevention (IDS/IDP) and antivirus programs to aid the detection of security events, incidents and vulnerabilities. Logs from various entities should be analysed and registrations of incidents should be made in an Incident Tracking System.

It is the person first notified about an event that is responsible for starting the activities involved in this phase. There are several ways a security event or incident can be detected and thus all employees should be aware of and have access to the guidelines for reporting. There should be clear procedures to follow for people involved in handling an incident. All relevant information should be passed to the Point of Contact (PoC) and the responsible ISIRT member. It is recommended that one of the ISIRT members is appointed the responsibility for incoming reports and for making assessments about further actions. A reporting form should be specified to ensure that all necessary and relevant information is preserved and that there is consistency in the information gathered.

Assessment and Decision   This phase includes assessment of information regarding security events and decisions about whether events should be treated as incidents. The assessment and decision phase also includes assessment of information received regarding vulnerabilities and decisions of how to handle these in accordance with previously agreed actions.

The PoC should use a predefined classification scale to make an assessment of security events, whether they are incidents or false alarms and what impact they may have on the organization's core services, information and affected assets. The initial assessment made by the PoC should be verified by an ISIRT member. The ISIRT makes decisions about how the incident should be handled, by whom and in what priority. To be able to respond to security incidents in an efficient and effective way, a prioritization process should be conducted based on the level of adverse business impact and the required effort to solve them. All information pertaining to an incident should be recorded in the database by the ISIRT. A main activity for the ISIRT is to allocate responsibilities for incident management actions and provide thorough and structured procedures for people involved.

Responses   The third operational phase presents guidelines and activities for organizations to use when responding to security incidents. The response should be in accordance with the actions agreed in the previous phase. This phase also involves responding to vulnerabilities reported either internally or by external parties. As a first step, the ISIRT has to determine whether the incident is under control, and then initiate appropriate actions. For situations out of control, escalation to crisis handling might be necessary. Otherwise, response activities including recovery, proper documentation and communication to relevant parties can be started.

The ISIRT should consider which internal and possibly external resources to utilize for optimal incident response. It is important that every action conducted by the ISIRT in this phase is logged properly and that guidelines are used to ensure thorough documentation. Logging will aid in analysing how effective and efficient the incident response process was as well as ensuring that any possible evidence is not compromised. It is the ISIRT's responsibility to make sure affected assets become operational again and that they are not vulnerable to the same attacks. Once an incident has been handled, the case should be closed formally by the ISIRT and recorded in the database.

Lessons Learned   The final phase starts after an incident has been resolved and/or closed and focuses on analysing whether the organization's incident management scheme worked successfully. During this phase improvements are identified and implemented. One of the main activities is reviewing how effective the entire incident management process was in responding to, assessing and recovering from the incident. Shortcomings and improvements in policies, procedures, security control implementations, reporting formats and risk assessments should be identified during this phase. Improvements may be implemented immediately or incorporated into future plans. The ISIRT should make sure improvements are made to the entire system and not only the affected parts.

The lessons learned phase has many iterative activities. An essential post-incident activity is documenting incidents properly as well as ensuring that the incident trend analysis is accurate. Sharing experiences with trusted communities and partners should be done on a regular basis, regardless of whether incidents occur internally. Reviews, trend analysis and testing should be performed frequently to improve the incident management scheme over time.

3.2.4 The ITIL Framework

Information Technology Infrastructure Library (ITIL) is a framework and a source of good practice for service management, that is aligned with the ISO/IEC 27000 standard. This section gives a brief introduction to the ITIL framework, focusing on the parts related to incident management and the content is, unless specified otherwise, derived from [31]. The definitions presented in this section are directly retrieved from [31].

To describe service management, the ITIL framework uses the following definitions:

Service: A service is a means of delivering value to customers by facilitating outcomes that customers want to achieve without the ownership of specific costs and risks.

Service Management: Service management is a set of specialized organizational capabilities for providing value to customers in the form of services.

The specialized organizational capabilities include the processes, activities, functions and roles that a service provider uses in delivering services. The ITIL framework is generic and is meant to be useful for any type of organization. It describes a set of functions and processes that can be implemented in order to be able to perform service management. The terms function and process are defined in the following ways:

Function: A team or group of people and the tools they use to carry out one or more processes or activities.

Process: A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may define policies, standards, guidelines, activities and work instructions if they are needed.

This section describes processes and functions related to incident management.

Availability Management   Availability management is essential for an organization and is primarily a proactive process. In addition to activities such as preparing and maintaining an availability plan and monitoring

availability levels, this process includes assisting investigation and resolution of availability related incidents and problems. The latter is a reactive part of availability management. This process is related to other processes including IT service continuity, information security, event, incident and problem management.

IT Service Continuity Management   This process is concerned with key systems in the event of a failure. The purpose of the process is to ensure that IT resources, systems and services can be restored within agreed timescales in the event of a major incident. The process is related to availability and information security management.

Information Security Management   This process is concerned with enforcing the security policy. The system in place for this is the ISMS. The security policy in an organization is something everyone should have access to and be aware of. Information security management is related to availability, incident, problem and IT service continuity management.

The Service Desk   The service desk is a function. One of the processes the service desk carries out is incident management. The service desk should be the single point of contact for IT users in an organization. This means that if users wish to log incidents or report events they should contact the service desk. The service desk is the owner of incidents throughout their lifecycle, regardless of who is working on the incident. They should be trained to obtain the skills needed in order to perform incident management as effectively and efficiently as possible.

Incident Management   This is the process for dealing with incidents. An incident is defined as being an unplanned interruption or reduction in quality of an IT service. An incident can also be the failure of a configuration item that has not yet impacted service. Hence, incident management includes both incidents where service has been disrupted or where service has not yet been disrupted. Each organization should have its own definition of a major incident. Large organizations may have dedicated teams available 24/7 to handle major incidents.
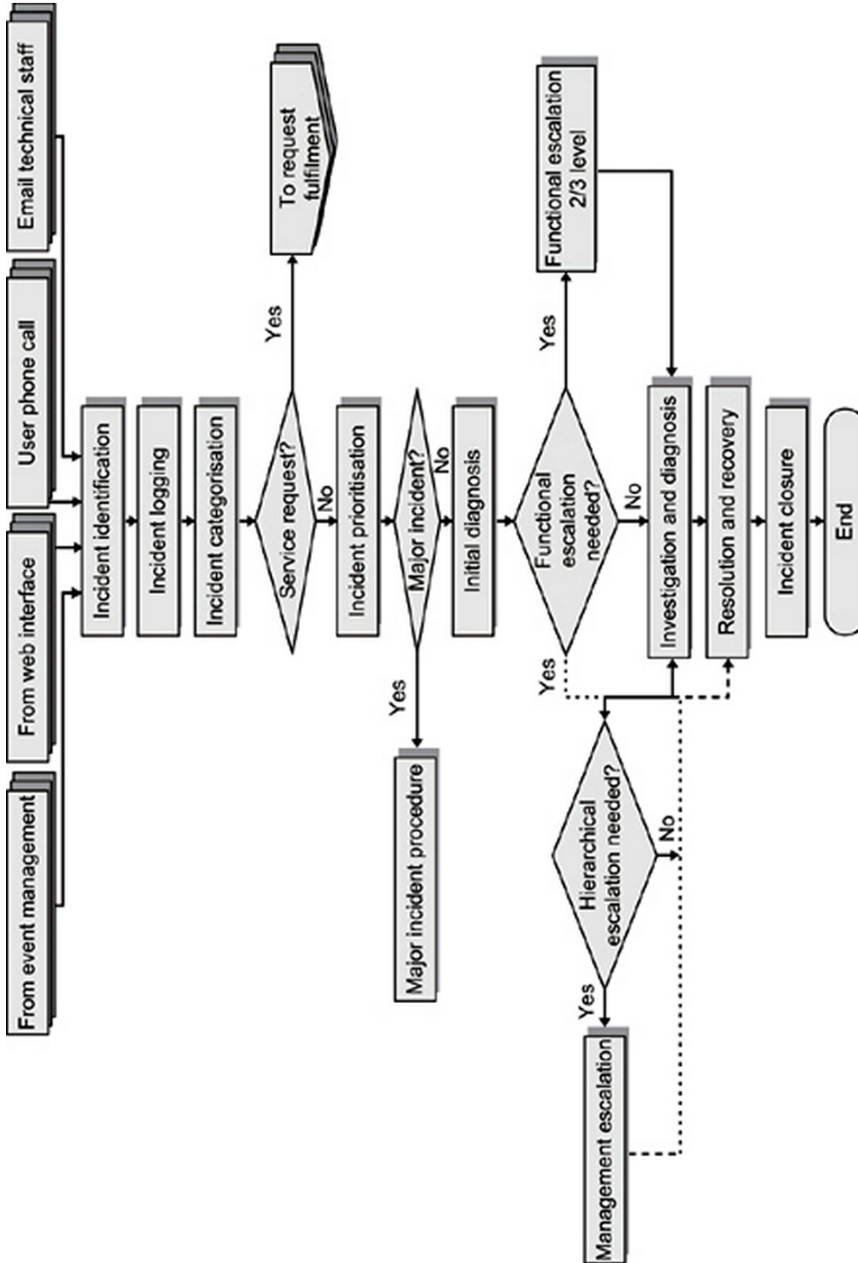
Figure 3.1: Incident Management Process [31]

In the incident management process resources are allocated to minimize and mitigate the impact of incidents and service unavailability in line with business priorities. The main objectives are to restore service as quickly as possible in addition to limit adverse impact on business operations. Incident handling may reveal areas that are in need of improvement. Organizations can adopt incident models, which are methods for handling groups of similar incidents.

The incident management process flow is illustrated in figure 3.1. The figure shows that incident reports can come from various sources. The incident reported needs to be identified, logged, categorized and prioritized. Accurate categorization is important as areas of the infrastructure where incidents occur can be highlighted. An example of an incident priority coding system can be seen in figure 3.2.

		Impact		
		High	Medium	Low
Urgency	High	Priority 1	Priority 2	Priority 3
	Medium	Priority 2	Priority 3	Priority 4
	Low	Priority 3	Priority 4	Priority 5

Figure 3.2: Incident Priority Coding System [31]

If the incident turns out to be major, the major incident process is initiated. The incident handling may also need to be escalated. Functional escalation is when the service desk is not able to resolve the incident or when they have not been able to resolve it within the target resolution time. Hierarchical escalation is when the profile of a specific incident within the IT organization and also within business areas needs to be raised. All incidents need to be investigated and diagnosed in order to subsequently be resolved and closed. The incident management process is closely related to the problem management process.
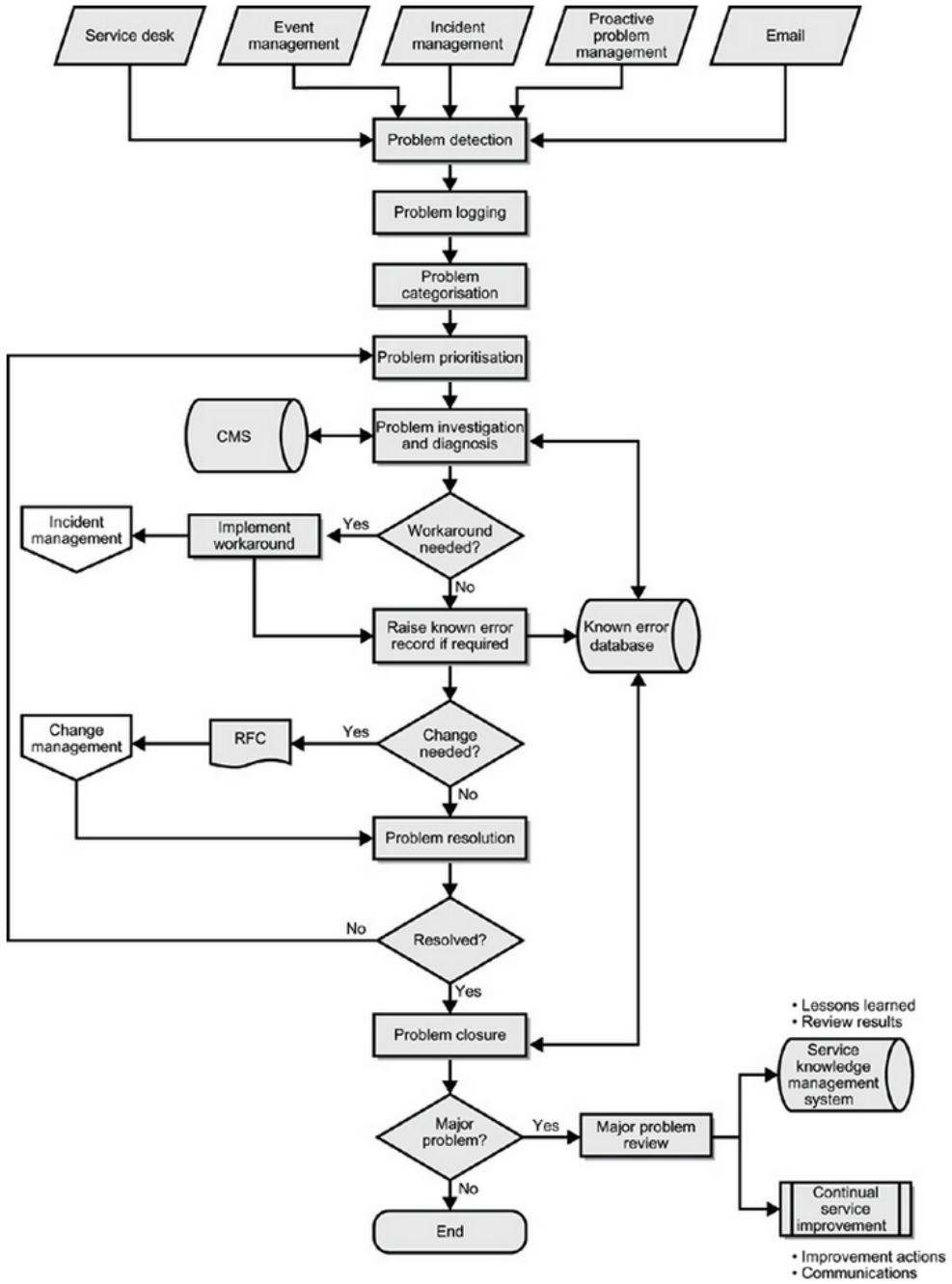
Figure 3.3: Problem Management Process [31]

Problem Management   The problem management process concerns analysis of the root cause as well as resolving problems. A problem is defined as being the cause of one or more incidents. The process is both proactive and reactive and seeks to prevent problems and incidents as well as reduce the impact of those that cannot be prevented. The problem management process is illustrated in figure 3.3.

The figure shows the various inputs to the process. It is important to log all details of the problem. All problems need to be categorized and prioritized. They should be prioritized in the same way as incidents, e.g. as in figure 3.2. During investigation and diagnosis the root cause of the problem should be discovered. The problem needs to be resolved as soon as a permanent fix is available and subsequently closed. If the problem is major, a major problem review must be conducted.

Event Management   The event management process handles normal messages and detects, escalates and reacts to exceptions. An event can be informational, a warning or an exception. The event management process is similar to the incident management process and should ideally be automated. Some events are triggers for the incident management process.

3.2.5   NIST Special Publication 800-61

This subsection gives an introduction to the guideline NIST SP 800-61 and the content is, unless specified otherwise, derived from [3]. This publication aims to assist organizations in mitigating risks from computer security incidents by providing guidelines on how to respond to incidents effectively and efficiently.

One of the first considerations for a Computer Security Incident Response Capability (CSIRC) should be to agree on a definition of the term incident. This guideline's definitions of events and incidents are included in section 3.1.1 of this report.

NIST SP 800-61 describes the four phases of incident response; preparation, detection and analysis, containment, eradication and recovery and post-incident activity. The phases and the relationship between them are illustrated in figure 3.4.
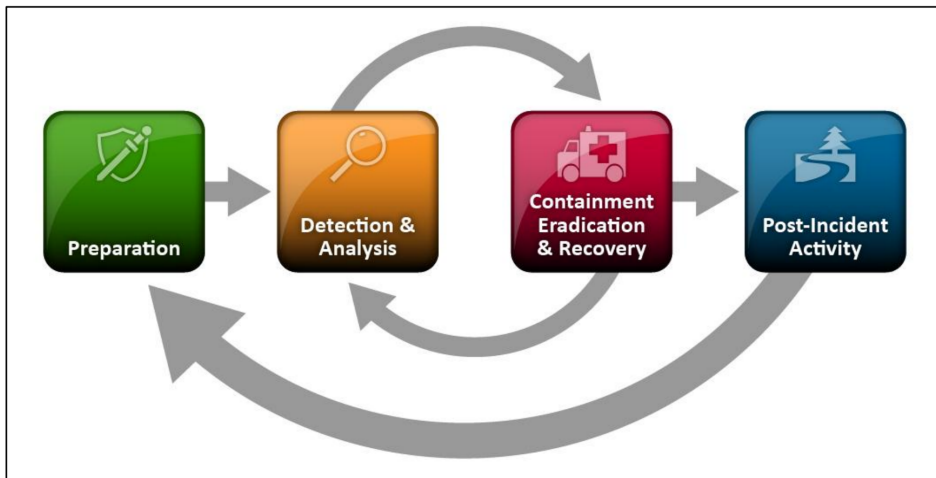
Figure 3.4: Incident Response Life Cycle [3]

Preparation This phase includes establishing an incident response capability as well as preventing incidents. The latter is not typically part of the IRT's tasks, but it is fundamental to the success of the organization's incident response. If a large number of incidents occur, it may overwhelm the IRT. To prepare for incidents, the incident handlers should have tools and resources such as contact information, incident reporting mechanisms, issue tracking system, digital forensic workstations[6] and digital forensic software.

Detection and Analysis Organizations should prepare to handle any type of incident. A classification of incidents can be used as a basis for incident handling. The guideline focuses on all kinds of incidents and does not address specific incident categories. A challenge related to incident handling is to detect the incident and determine the potential impact the incident may have. The actual detection may be the hardest part of incident handling. The guideline defines two types of signs of incidents; precursors and indicators, with indicators being the most common. These are defined in the following way: "A *precursor* is a sign that an incident may occur in the future. An *indicator* is a sign that an incident may have occurred or may be occurring now." Common sources for precursors and indicators are Intrusion Detection and Prevention Systems (IDPSs), antivirus and antispam

---

[6]A digital forensic workstation is specially designed for acquiring and analysing data. It usually contains a set of removable hard drives that can be used for evidence storage.

software, third-party monitoring services, logs, people and information on new vulnerabilities and exploits.

A challenging part of this phase is the analysis, i.e. to determine which indicators and precursors are legitimate, if they are really related to an incident and what has actually happened. When the team believes an incident has occurred they should try to determine the scope. All steps taken should be documented and timestamped. It is important to note that any such documentation can be used in court. The IRT should maintain a database containing information about incidents, such as status, indicators, related incidents and actions taken by the incident handlers. It is important to prioritize incidents and to handle them accordingly. Factors that can be used as a basis for prioritization include the functional impact of the incident, the information impact of the incident and recovery from the incident. When the prioritization is performed, the IRT should notify the appropriate people. It is important to have procedures regarding who these people should be.

Containment, Eradication and Recovery   Containment is obviously an important part of incident handling. The existence of strategies and procedures for containment is helpful. These strategies and procedures are different for different types of incidents. Gathering and handling of evidence are part of this phase. For some incidents eradication is necessary and it is sometimes conducted during recovery. Eradication can include deleting malware and disabling breached user accounts. Recovery consists of restoring systems to normal operations and in some cases eliminating vulnerabilities that could cause similar incidents. The guideline does not offer specific recommendations for eradication and recovery as these are often OS specific.

Post-Incident Activity   Learning and improving are two of the most important parts of incident response. It is recommended to hold a lessons learned meeting after each major incident and periodically after minor incidents. One meeting could potentially cover several incidents. Lessons learned meetings should generally focus on revealing shortcomings as well as what was successful. The desired result is that the organization will be better equipped for the next incident. Often, incident response policies and procedures are updated. Areas these meetings should focus on are how well the staff performed, whether documented procedures were followed, if procedures were adequate and how information sharing with other organizations could be improved. To prevent similar incidents in the future,

potential corrective actions and potential additional tools and resources should be reviewed. Both people involved in the incident(s) in question and people needed for future cooperation should be included in these meetings. A follow-up report that provides a reference that can be used when handling similar future incidents should be created. Other post-incident activities include the use of collected data for risk assessment, measurement processes to determine the success of the incident response team and audits of incident response programs.

3.2.6 ENISA - Good Practice Guide for Incident Management

This guide is developed by the European Network and Information Security Agency (ENISA) and provides a description of good practices for security incident management. The content is, unless specified otherwise, derived from [27]. The focus of this guide is IT and information security incidents. It specifically addresses the incident handling part of incident management. The incident management and incident handling processes are illustrated in figure 3.5. The incident handling process has four major components, as shown in the figure.

Detection: The CERT can receive incident reports from various sources. This guide recommends to use e-mail as a communication channel as people prefer this. Additionally, it recommends to use monitoring systems in addition to reports sent by others. Detection includes registration of incident reports in an incident handling system. This stage is a good place to implement pre-filtering mechanism for incident reports. The registration process could include the use of an incident report form.

Triage: This stage consists of the three phases verification, initial classification and assignment. During these phases the following questions should be answered:

- Is it really an IT security incident?
- What is the impact?
- Is there collateral damage?
- How many people do you need to handle this incident?
- Which incident handler should be appointed to the incident?
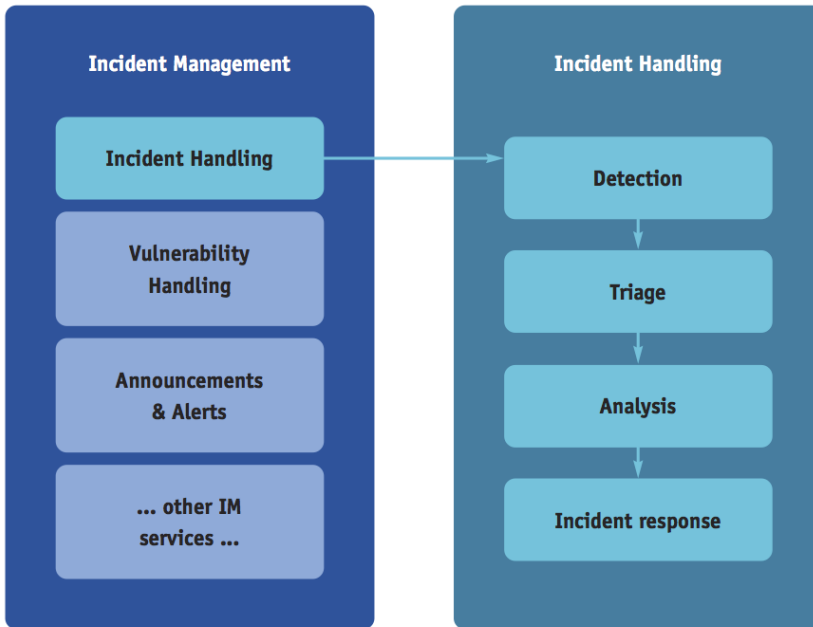
Figure 3.5: Incident Management and Incident Handling [27]

The verification phase seeks to answer the first question. It is however recommended to respond to and archive all reports, even those not defined as information security incidents. They may include information relevant to other incidents or potentially lead to an incident. After an incident report has been verified the incident should be initially classified according to a classification schema. The last part of the triage component is to assign the incident to an incident handler.

Analysis and Incident response: These components are illustrated by figure 3.6. The cycle may need to be iterated several times. To perform *data analysis* there should be collected as much data as possible. Prior to the collection, all involved parties should be notified. Sources for data collection could be an incident reporter, monitoring systems, a referring database and relevant log files. The collected data should be used to try to determine the source of the incident. Prior to the data analysis, decisions about what data to analyse and in what order must be made. During the analysis, people will often exchange ideas and observations as well as draw conclusions. This belongs to the *resolution research*. It is recommended to advise team

members to write down any observations that can be discussed in review meetings. The *action proposed* part consists of preparing a set of tasks for each party involved. The *action performed* should be monitored, where possible. The main goal for all actions is the *eradication and recovery*.
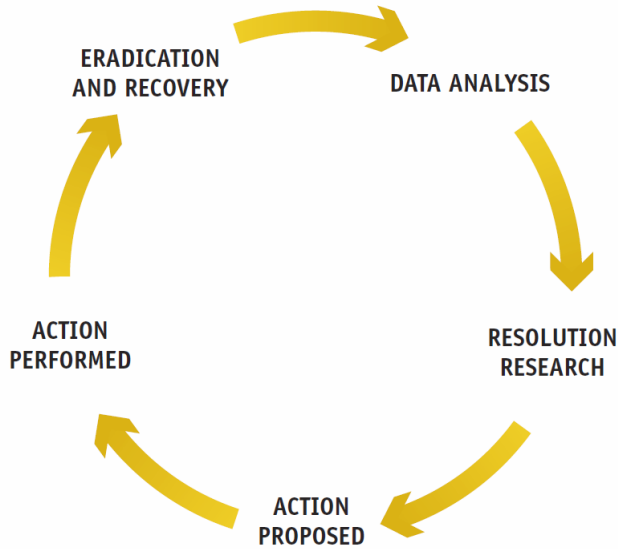
Figure 3.6: Incident Resolution Cycle [27]

When you have left the incident resolution cycle, there are still tasks to perform. The incident needs to be closed properly. Each involved party needs to be informed that the incident is resolved. The classification of the incident should be revisited and a final classification should be performed. The classification could have been revisited during the resolution cycle as well. It is recommended to have a taxonomy and to classify incidents in accordance with it.

After an incident has been resolved or closed a post-analysis should be performed in order to learn from the incident. It is also recommended not to analyse all incidents, but only the most characteristic and complex ones and those that include new attack vectors.

Incidents should be reported to the management. In addition to specific issues, the daily operations should be reported, including costs, positive results, plans and risks. This will save time and resources in situations where you need the management's operational or financial support and

quick decisions.

3.2.7   NorSIS - Guideline for Incident Management

The Norwegian Centre for Information Security (NorSIS) has in cooperation with a group of students[7] developed a guideline for incident management, published in 2010 [32]. The aim of this guideline is to give a thorough description of why and how organizations should plan for security incident management, conduct business impact analysis and explain various measures to improve information security in organizations. This guideline is specifically developed for Small and Medium-sized Enterprises (SMEs) and may thus not be extensive enough for large organizations. The content in this section is, unless specified otherwise, derived from [32].

Incident Management Policy   An incident management policy should form the basis for developing new incident management plans in organizations. A solid policy should state an organization's objectives for incident management and include a statement ensuring commitment from senior management. Any relevant laws, standards and regulations should be included. It is essential that the policy has requirements for performing regular risk assessments, business impact analysis, tests and training. The guideline recommends to include the assignment of roles and responsibilities in the incident management policy.

Business Impact Analysis   NorSIS recommends organizations to conduct a business impact analysis to identify which services are of significant value and needs to be secured. Risk assessments and the identification of possible consequences of security incidents are part of this process. The guideline emphasizes the importance of knowing risks and potential threats.

Preventive Measures   One of the most cost effective ways to perform incident management is implementing preventive measures. Listed as minimum requirements are antivirus, logs, firewalls, backups, alarms, locks, regular reviews of the threat landscape, and reporting systems for employees. Other proposed measures include encryption of data and wireless networks.

---

[7]The students did a survey on incident management in Norwegian SMEs [24]

Recovery Strategies The guideline recommends having a recovery strategy to quickly re-establish business operations after an incident. Suggestions include backup and emergency solutions. Routines and plans should be in place to handle recovery efficiently.

Incident Management Plan Organizations should use previous assessments and proposed incident scenarios to develop an incident management plan. It is recommended that individual plans addressing different scenarios are developed. Each incident management plan should include type of incident, what triggered the incident, roles and responsibilities, guidelines for communication and notifications, maximum response time, check-list of tasks during incident response and post-incident activities.

Training To reduce costs caused by security incidents, NorSIS suggests training employees in correct use of equipment and making sure routines for incident response are well known.

Plan Maintenance The guideline recommends organizations to conduct annual reviews of their incident management plans. To ensure a solid and up-to-date incident management plan, changes should be made based on experience from previous incidents.

Outsourcing When organizations decide to outsource services, they should evaluate and agree on incident management procedures. It is the organization outsourcing that is responsible for securing information properly and for making sure sufficient plans for incident management exist. An agreement should define responsibilities and state expected quality of services.

3.2.8 SANS: Incident Handler's Handbook

This section gives an introduction to SANS' Incident Handler's Handbook and the content is, unless specified otherwise, derived from [33]. The purpose of this document is to provide sufficient information for IT professionals and managers to create incident response policies, standards and teams for their organization. Six phases of incident management are described and recommended to be followed in sequence as each phase builds on the previous one.

Preparation   This is the most crucial phase as it determines how well the incident response team will be able to respond to security incidents. During this phase, several key elements should be implemented to avoid potential problems while responding to security incidents.

Organizations should develop a policy stating the organization's principles, rules and practices. After the establishment of a security policy, organizations should develop a response plan with a prioritization of incidents based on organizational impact. Having this prioritization scheme could aid in obtaining necessary resources for incident management by ensuring commitment from senior management as they will better understand risk and business impact. It is also recommended to have a communication plan so the response process is not delayed by uncertainty of whom to contact in unexpected situations. These plans should also state when it is appropriate to contact law enforcement.

Documenting incidents is beneficial for organizations. A thorough documentation is useful for lessons learned and might also serve as evidence if an incident is considered a criminal act. The establishment of a Computer Incident Response Team (CIRT) is part of the preparation phase. It is vital that also their activities are documented properly.

Identification   The first step of this phase is identification of security events by detecting deviations from "normal" operations within the organization. This is followed by a decision of whether the event is categorized as an incident. Organizations should implement various tools to gather documentation about events, such that incidents and patterns can be identified. Examples of such tools include IDSs, firewalls and log files. Typically, incidents are reported to the CIRT that decides the scope of the incidents and how to move forward.

Containment   In this phase organizations try to limit the damage and prevent further damage caused by security incidents. It is recommended to isolate compromised systems to avoid escalation. An easy measure could be to disconnect affected parts of the system.

Several steps are necessary for a successful incident response. The first step is called short-term containment and is concerned with limiting the damage by implementing short-term but effective measures. The second step is concerned with ensuring proper back-up of information before system resources can be restored. The final step is called long-term containment

and involves removing alternations made by an attacker, installing security patches and limiting further escalation of the incident.

Eradication Affected assets and systems are restored during this phase. To avoid similar incidents in the future, defences should be improved. Continuous documentation is important in this phase to ensure that proper steps were taken in previous phases in addition to determine the overall impact on the organization. It is recommended that all affected systems are scanned with anti-malware software to ensure that all potential latent malware is removed.

Recovery Activities in this phase include bringing affected systems back into operation and preventing future incidents caused by the same problem as previous incidents. Other activities are testing, monitoring and validating systems to ensure they are not reinfected.

Lessons Learned The final phase's main objectives are to learn from incidents to improve the CIRT's performance and to provide material to aid in future incident responses. An important activity is to hold a post-incident meeting that summarizes the incident management process. This phase evaluates an organization's incident management procedures and identifies areas of improvement.

3.2.9 Summary

The standards and guidelines have a number of similarities and have chosen to divide the incident management process into several phases. Most of them describe a preparation phase, where an incident management capability is built. All of the standards and guidelines have phases for detection, analysis and incident responses, but the structure of these phases varies. All of them highlight lessons learned activities, even though not all describe a separate phase for this. It is worth noting that the guidelines presented are developed by single organizations, whereas the ISO/IEC standards are developed by groups of experts from all over the world. The development and approval of the ISO/IEC standards are extensive processes with many contributors and should therefore be widely accepted.

3.3   Related Work

In recent years the amount of available academic literature addressing inci-
dent management has increased along with an overall interest for the topic.
Despite the amount of available literature there is limited knowledge about
how organizations perform incident management in practice and thus an in-
teresting topic for research. We studied related research papers and surveys
and some of them are briefly discussed in this section.

Eugene H. Spafford presented in 2003 [34] the first large internet worm
and discussed what happened during the years after this large incident,
which occurred in 1988. The worm led to the CERT at Carnegie-Mellon
University being established. The three flaws this worm exploited were
trust relationships, buffer overflows and poor default configuration. The
author claimed that these flaws have not been removed but rather worsened.
The author also questioned the CERT model. He claimed that incident
response is uncoordinated and of minimal effectiveness. Lastly he predicted
that he could either in 2013 or 2018 write a paper about 2003 as the time
were we did not know how bad it was going to get. This work is quite
different from our thesis, but it is interesting that he points to lack of
lessons learned and predicts that the situation in the time of this writing
has not improved.

In a study from 2005 [35], a survey of Norwegian companies and public in-
stitutions was conducted where routines for information security incidents,
how theory and practice differed as well as potential differences between
organizations in public and private sectors were examined. The survey
showed that statistical material about incidents were inaccurate due to
lack of implemented routines, lack of training and weak definitions of se-
curity incidents in general. Public institutions were found to have greater
shortcomings in reporting, training and statistics than private ones. A lack
of documentation and use of metrics when outsourcing IT systems were
also revealed. Of all the participating organizations only 50% followed in-
ternational standards for information security. Further, the study disclosed
a gap between incident management theory and practice in terms of how
organizations handle information security incidents. Even though private
organizations were found to have overall better incident management, there
were still room for improvements, especially regarding reporting, training
and statistics.

In 2007 Werlinger et al. [36] conducted an exploratory study using interviews and questionnaires. The purpose of the study was to investigate what tasks security practitioners perform during security incidents, what skills and tools are necessary and what strategies are required in order to deal with security incidents. They grouped tasks into the main stages detection, analysis and response. They identified pattern recognition, hypothesis generation and cooperation as needed skills. Two identified strategies in incident response were isolation and simulation.

Werlinger et al. [37] conducted in 2009 16 semi-structured interviews with IT security practitioners from seven types of organizations. Their research focused on diagnostic work performed in response to security incidents as well as the tools used in this process. Their findings showed that a great deal of tacit knowledge is used in the diagnostic work. In addition to relying on tools, the employees used their own technical knowledge as well as their knowledge of the organization and its systems to handle incidents. The findings also showed that intensive diagnostic work was needed to be able to respond to security incidents. This research differentiates from our research in the sense that it focuses mainly on diagnostic work and the tools used instead of the entire incident management process. Additionally there is no comparison to existing standards and guidelines in the analysis of the data.

In 2010, a group of students at Gjøvik University College conducted a survey of incident management policies, implementations, training and routines in Norwegian SMEs [24]. They performed interviews and questionnaires and concluded that there was still room for improvement regarding incident management in Norwegian SMEs. Having a chief of information security was shown to be beneficial. The organizations that had a chief of information security tended to have better plans for incident management and in addition they used their plans more often. Their research indicates overall insufficient plans for incident management among Norwegian SMEs, and poor quality in existing plans. Finally, in cooperation with NorSIS the students proposed a guideline for incident management customized for SMEs. A summary of this guideline was presented in section 3.2.7. Since then, both new standards and guidelines addressing incident management have been published. It is thus interesting to study how organizations perform incident management and how these standards and guidelines are adopted in current plans and procedures for incident management.

An ongoing study by Maria B. Line [38] investigates, by conducting a case

study, current practice for information security incident management in the power industry. Six large organizations are studied. Preliminary results show that plans for incident management are not widely established in the participating organizations. She found that most of the organizations perform regular meetings to evaluate incidents. It was evident that it is the ICT staff's responsibility to handle information security incidents and that there is not a close cooperation between the ICT staff and power automation staff.

Incident response teams are of utmost importance to incident management. We therefore found research related to IRTs' tasks, structure and responsibilities interesting. As described in section 3.2, several standards and guidelines address establishment and running of IRTs and a few studies also look at how IRTs operate in practice. In 2003, Killcrece et al. [39] studied the current state of practice for IRTs and found several shortcomings for teams in general such as lack of tools, training and experienced personnel. However, during the past decade new standards and guidelines have emerged and the field of incident management has matured. Based on this and several other studies, Ahmad et al. [40] presents a case study exploring issues faced by incident response teams that affect the greater organizational security function. They found that organizations lack the ability to exploit their organizational learning capability. A lack of proper information dissemination and the fact that organizations tend to focus on technical learning over policy and risk were also discussed. The participants in their study agreed that if the organization had better information dissemination it would improve their security practices and thus the overall security in the organization. Additionally, they found that organizations often disseminate information from "high impact" incidents, but that "low-impact" incidents do not result in disseminated information despite being potentially very useful from a learning perspective. Ahmad et al. sees the distinction between high and low impact incidents as key to efficient learning processes in organizations. Further, Wiik et al. [41] presents a simulation model to better understand the main factors influencing an IRT's effectiveness. They identified that short-term pressure from a growing incident work load prevents attempts of improving the organization's response capability long-term.

While studying related work we came to understand that the threat landscape, standards and best practice guidelines change rapidly. Surveys conducted only few years apart reveal that information security and incident

management are maturing. Hence, we found studying how organizations perform incident management in practice highly relevant.

Chapter 4

Case Introductions

This chapter gives an introduction to the specific cases studied in this thesis. Three different organizations are studied in separate cases. All three organizations in this study are large. In Norway, organizations are categorized as large if they have more than 100 employees [42].

4.1   Case A

The organization studied in case A is a large Norwegian government-owned organization with several thousands employees and a large number of user accounts. Throughout the rest of this report, the organization in this case will be referred to as Organization A. The interviewee was the IT security manager. He has had this role for about two years and his responsibilities include both technical and administrative tasks.

The organization handles most of their IT operations themselves, even though some services are outsourced. They have an IT manager leading a staff that includes the IT security manager. They have a customer service center that handles user support and receives notifications from users that observe unusual activity. The organization has a network section that is responsible for ensuring that their network infrastructure works as intended. Additionally, they have a section that operates their servers. They have large systems, one for e-mail in addition to a system for handling employee and user data. The organization has a section responsible for developing, maintaining and operating their applications.

The documents studied in this case were their information security policy, principles for information security document, IT regulations and contingency plan.

A total of 15 employees participated in the employee survey in case A. They were randomly selected from four departments at different geographical locations.

4.2   Case B

The organization in case B is a large Norwegian, independent and non-commercial organization with a couple of thousands employees. They process large amounts of valuable and sensitive information and thus information security has high priority in their business operations. Throughout the rest of this report, the organization in this case will be referred to as Organization B. The two interviewees from the organization were the IT security manager and the supply chain manager, both working in the IT department. They have had these roles for the past four and six years respectively. They deliver IT support for all of the organization's departments and are involved in incident management regularly.

In addition to the central IT department, each individual department has their own IT manager responsible for local IT support in the department. The local IT managers are also responsible for information security within their departments.

Organization B has to a large extent outsourced their IT operations and has several suppliers. The main IT operations are delivered by one organization, whereas application management is delivered by a consortium. The former is referred to as Supplier 1 and the latter as Supplier 2 in this report. These two are the main suppliers of IT operations, but there are others as well. As part of case B, representatives from the two main suppliers were interviewed to get a holistic picture of Organization B's incident management. Because of the large extent of outsourcing distributed over a number of parties, the suppliers need to coordinate and cooperate.

Supplier 1's entire team in basic IT operations is available for Organization B. They have customer service available for the organization as well. These two teams consist of about 18 and 25 people respectively. This does not mean that all of them have access to the organization's system. About 20-

30 people have access. The interviewee from Supplier 1 is a technician in basic IT operations as well as being a security coordinator between Supplier 1 and the organization. He has had this role for 3-4 years.

Supplier 2 has a team of 15-20 people available for organization B. They are responsible for application management which involves improving applications and making sure that applications are without errors. Additionally, they advise the organization about how they can improve their applications and work processes. The interviewee from Supplier 2 is the service manager for one of Organization B's systems. He has had this role for about one and a half years. Supplier 2 cooperates with Supplier 1.

The document studied in this case was Organization B's IT contingency plan.

15 people from three departments participated in the employee survey in case B. They were randomly chosen and the selection includes both employees with administrative tasks and employees with tasks related to the organization's core activities.

4.3   Case C

This organization is a large Norwegian organization with several thousands employees. They deliver IT services to customers in addition to operating their own infrastructure. Throughout the rest of this report, the organization in this case will be referred to as Organization C. The interviewee was the IT security manager and the operational leader of a department that is responsible for security, quality, compliance and risk. He has had this role for about two years. In addition, we had e-mail correspondence with one employee with several years of experience from the organization's IRT.

In Organization C, departments have different requirements for security and thus various policies are implemented throughout the organization. In addition to operating their own incident management, they are responsible for incidents concerning services they deliver to customers. Consequently, the organization deals with security incidents frequently.

The documents studied in this case were their IRT handbook, corporate information security policy, enterprise risk management process description,

incident management process description, major incident routine description and contingency policy.

11 people from the organization participated in the employee survey. They were randomly chosen and had different roles, tasks and responsibilities within the organization.

Chapter 5

Findings

This chapter presents findings from the case study. The findings from each case are described separately. It should be noted that in this chapter, information has not been analysed or interpreted by the authors, but only introduced as given in the interviews or found in the documents. The *grouping* of the information however, is based on the standards and guidelines presented in section 3.2 and represents the first step of the qualitative data analysis approach, as presented in section 2.3.5.

5.1 Case A

This section describes findings from case A, where the interviewee was the IT security manager.

5.1.1 Preparation

The IT security manager defined an incident as the occurrence of something unwanted. This includes both occurrences belonging to a predefined category of unwanted events and other unwanted events. More specifically an Information and Communications Technology (ICT) incident will usually involve loss of information or loss of control over information systems. The categories of unwanted events are determined through risk assessments. It is stated in their "principles for information security" document that they

have to perform risk assessments. This document is approved by the management and distributed to all parts of the organization.

The IT security manager identified loss of information related to the organization's core activities as the worst information security incident they can experience. Such an incident could damage their relationship to partners, their general reputation and their credibility. Additionally, it may damage the work and career of individuals with ownership of the information. Another aspect is that the organization processes information that is very sensitive and it is crucial that this information is not disclosed to any outside party.

Organization A has an information security policy, a central contingency plan, department specific contingency plans and a principles for information security document. The latter is to be updated if there are changes in the threat landscape or at least every other year. It is currently a subject for audit. Each department is responsible for making sure that employees and other users are aware of these documents. The IT security manager suspected that not all users have detailed knowledge of these documents, even though it is stated that all users have to comply with them. During the last years the threat level has increased for this organization and as a consequence they have planned to perform a risk and vulnerability assessment for all departments in the organization. In addition to the mentioned documents, they have an internal policy for incident handling.

The IT security manager believed they have satisfactory continuity plans. They have among other things tried to avoid single points of failure to increase redundancy as several of their systems are critical for their operations. Consequently, they need backup solutions for these systems in case of severe incidents.

Their information department is responsible for all external communication and they cooperate closely with the IT department. Organization A has procedures for contact with the police in case of violations of the law. If they wish to report a crime it is the manager that has to do this, although the IT security manager will upon request provide the police with any relevant information he has access to.

Organization A has not developed a holistic plan for incident handling as there are many different incidents that require different responses. They do however have general guidelines for handling security incidents. Certain types of incidents, like phishing, are common and the organization has more

detailed guidelines for these specific types of incidents. The IT security manager stated:

> *"To have a detailed guideline that takes all possibilities into account and that you have to change each time you get a new system [...] we are not that thorough [...] and I don't think we have ambitions to be that thorough either"*

If a system owner discovers a vulnerability in a system he will notify the IT security manager and inform about the scheduled update for the patch.

Standards and Guidelines   Organization A has implemented the ISO/IEC 27001 and 27002 standards, but does not aim to be certified. Their information security policy states that they are to be in compliance with these standards. Because they are a government-owned organization they are required to implement ISO standards. This is a relatively new requirement and the IT security manager saw it as being one step closer to a certification. He thinks that a certification could be useful, since the most important part of a certification is the management's commitment to the standard. The organization conducts reviews of incidents and uses this to make changes in their ISMS.

They have implemented the ITIL framework in their incident management and security work. They have not implemented all recommendations from the ISO/IEC 27001 and 27002 standards and the ITIL framework, but have chosen the parts they see relevant for their organization. The IT security manager is somewhat familiar with the ISO/IEC 27035 standard, but it is not implemented in the organization.

Awareness and Training   Organization A conducted an awareness campaign in cooperation with an external supplier about a year and a half ago. The supplier delivered slides containing small lectures that were sent to employees via e-mail. The lectures addressed themes such as how to protect your password. In relation to their attitude towards awareness, the IT security manager stated:

> *"There is a principle that says, never waste a good crisis."*

This means that they communicate incidents, typically incidents that others have experienced, to employees. He mentioned that personally he takes any opportunity to talk about the importance of protecting information.

About a year ago, Organization A conducted a contingency rehearsal that addressed information security. The management was involved in this rehearsal. It had seven levels of escalation. The training contributed to increased information security awareness in the management as well as being a test of their central contingency plan.

The IT security manager stated that rehearsals are always beneficial and he therefore uses all possibilities to increase management awareness related to information security. It is however challenging to conduct rehearsals. He said:

> *"The most important part of preparing a rehearsal is to make sure that the responsible people train on the right things and to create a good and relevant game that is challenging to the involved people and that they feel is realistic [...] That is the most important thing, to give them what they need in order to be able to handle a real situation."*

Organization A uses their risk and vulnerability assessments to determine what to focus on in rehearsals. They use rehearsals both for situations where they already have routines and where they do not yet have any. A rehearsal may thus identify what routines they should implement. They have planned rehearsals this year as well, where one is to be conducted in cooperation with a partner organization.

There are many examples of issues that have been revealed through rehearsals. One such example is the employees' lack of understanding of risk. Even though various employees may have a certain risk awareness they may not agree on what the actual risk is.

The IT security manager claimed that their classification of information is not satisfactory. He believed that users are not aware that the information security policy states that they have to classify the information they process. Establishment of the information security policy is the manager's responsibility. The IT security manager emphasized again that a more extensive use of the ISO/IEC 27001 and 27002 standards could help as this might lead to increased management commitment. Increased management commitment might lead to the information security policy being better established in the organization, and consequently employees become more familiar with their responsibilities.

5.1.2   Detection and Analysis

Organization A uses several means for detection of incidents.

Initial Detection   Incidents can be reported via their abuse system. Additionally their internet supplier notifies them if they see that there are any compromised hosts in their network.

Organization A has a relatively new deviation management system. This system can be used to report various types of deviations, from information security to Health Safety and Environment (HSE) related deviations. The deviation does not necessarily have to be an incident, but can be any type of deviation, such as a vulnerability. The system is mainly used for internal cases, and thus differs from the abuse system. The IT security manager wished that the system could be used for information security related incidents to a larger extent than it is today. The system also works as a database of incidents, as it includes information about all reported deviations.

They have a tool that can be used to monitor connections to their network. This is a source of incident detection.

The IT security manager was convinced there is underreporting of incidents. However, he had the impression that people in the organization reporting some issues, such as suspicious e-mails but that they do not report to which extent they have actually disclosed sensitive information. He believed this might be due to employees not understanding security which indicates that they trust systems even though they are not secure. He said that this originates in establishment of attitude and training. He stated:

> *"Users of a system need to understand what possibilities there are in the system, but also what security limitations there are."*

Categorization   Organization A categorizes incidents based on type (spam, phishing, botnet etc.) and based on what service or system they affect. Incidents reported in their deviation management system are categorized based on whether they are HSE-related, technical or of other categories. An explicit category for information security deviations does not currently exist in the system, but they have planned to include it in the future.

Organization A categorizes incidents based on impact as well. They use the categories low, medium and high. Medium is when service is unavailable

for several people and high is when service is unavailable for the whole organization. Other incidents are categorized as low. The assigned impact category sets a time limit for when the incident must be resolved.

5.1.3   Incident Response

Cases reported to the abuse system are categorized and dispatched to the second line of incident response. From that point it is either resolved or transferred to another section, such as the network section, if they are better equipped to handle the incident. It can also be solved in cooperation between incident handlers and employees from other sections.

The IT security manager does not mainly focus on getting systems up and running as fast as possible after an incident. He wants to make sure that incidents are properly resolved before restoring normal operations. He is also concerned with determining whether the affected systems are vulnerable to other attacks. However, there have been situations where he wanted to perform risk and vulnerability assessments of systems, but has not been allowed to do so due to resource restrictions.

After an incident the system owner identifies what information has been lost or compromised. It is also his job to assess whether the organization has suffered economical losses. It is easy to estimate the number of man-hours spent on resolving an incident, but other factors, such as the value of information, are more difficult to estimate. The IT security manager said that he wanted to work on value assessment of information by asking information owners.

If an incident is serious it will be reported to the management. The IT manager is notified about larger incidents, but not small routine cases.

Organization A has tools that they use to analyse e-mail in spam cases. They have the possibility to use an admin account to fetch e-mails in serious cases. If this is done, they only examine e-mails relevant to the case in order to ensure privacy. The IT security manager has only done this once, in relation to a targeted phishing attack. This attack happened in two stages where the first stage was targeted to the organization and was used to retrieve usernames and passwords from users. The compromised user accounts were subsequently used to send bank-phishing e-mails.

Incident Response Team   Because Organization A has an internet do-
main they are required to have an abuse e-mail address. The cases sent
to abuse go straight into a case management system. Incident handlers
are required to give the reporting user an answer such that he knows that
the potential incident is being looked into and that his report is appreci-
ated. Incidents that involve employees, botnets or spam are handled by the
full-time employees at the service desk.

Most of the employees involved in incident handling have an IT background
and thereby a solid technological knowledge. Additionally they go through
a training process when they are hired in addition to training when they
are appointed new tasks. Organization A has a team that is responsible for
receiving and handling cases reported to the abuse e-mail address. Some
of the members of this team are part of the IT support function of the
organization and are part-time employees. Others work at the service desk
and are full-time employees. One of the full-time employees is the leader of
the team. The IT security manager is also part of this team in a supervising
role.

Usually, notifications are received during work-hours, but someone is avail-
able 24/7 if something extra serious occurs. In those cases they need to be
alerted specifically.

The team does not perform much preventive work. They see repeating
incidents and conduct reviews of larger incidents and use this to identify
changes that are needed. They use the ITIL framework, discussed in section
3.2.4, and treat repeating incidents as problems that needs to be analysed
further to find the root cause.

The team often needs to communicate with various sections of the organi-
zation when incidents occur. Regular employees are not necessarily special-
ized in handling security incidents, but they know how the systems work,
and are thus important resources in resolving incidents. There is a daily
designated contact person for some of the sections. The IT security man-
ager mentioned that this communication can be challenging, especially for
sections that do not have a permanent designated contact person. Last year
they experienced a targeted phishing attack and this led them to gather a
team consisting of resources from various sections.

Workflow   Organization A has developed workflows for specific types of
incidents. They have not developed a general workflow that applies to all

incidents. Figure 5.1 illustrates common steps for incidents of a prede-
fined category. These steps are conducted before the incident specific steps
are initiated. Figure 5.2 illustrates the incident specific steps for a bot-
net incident. The figures are derived from a description given during the
interview.
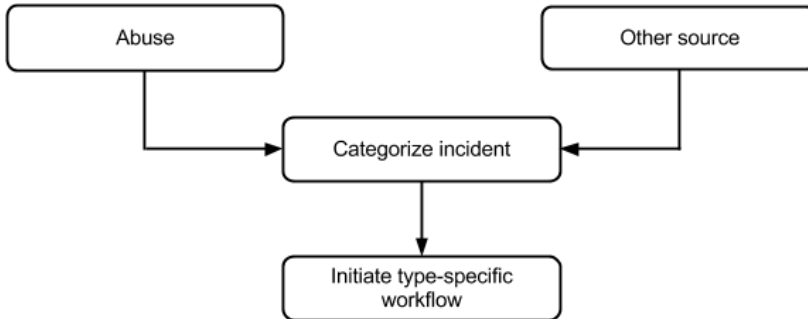
Figure 5.1: Common Workflow Steps

General steps for incidents of predefined categories:

- The process is initiated by a report received in their abuse system or
  from some other source.
- The incident is categorized based on type (botnet, virus etc.)
- Incident specific steps are initiated.

Steps for a botnet incident:

- If there is more than one affected host, the case will be split into one
  case per host and the following steps will be taken for each case:
- If the incident is particularly serious the host will be blocked and the
  user in question will subsequently be contacted.
- If the incident is not so serious the user in question will be contacted
  and subsequently blocked.
- If contact is not established the user will be blocked and then tried
  contacted again.
- The affected host is cleaned up.
- The user will regain access.
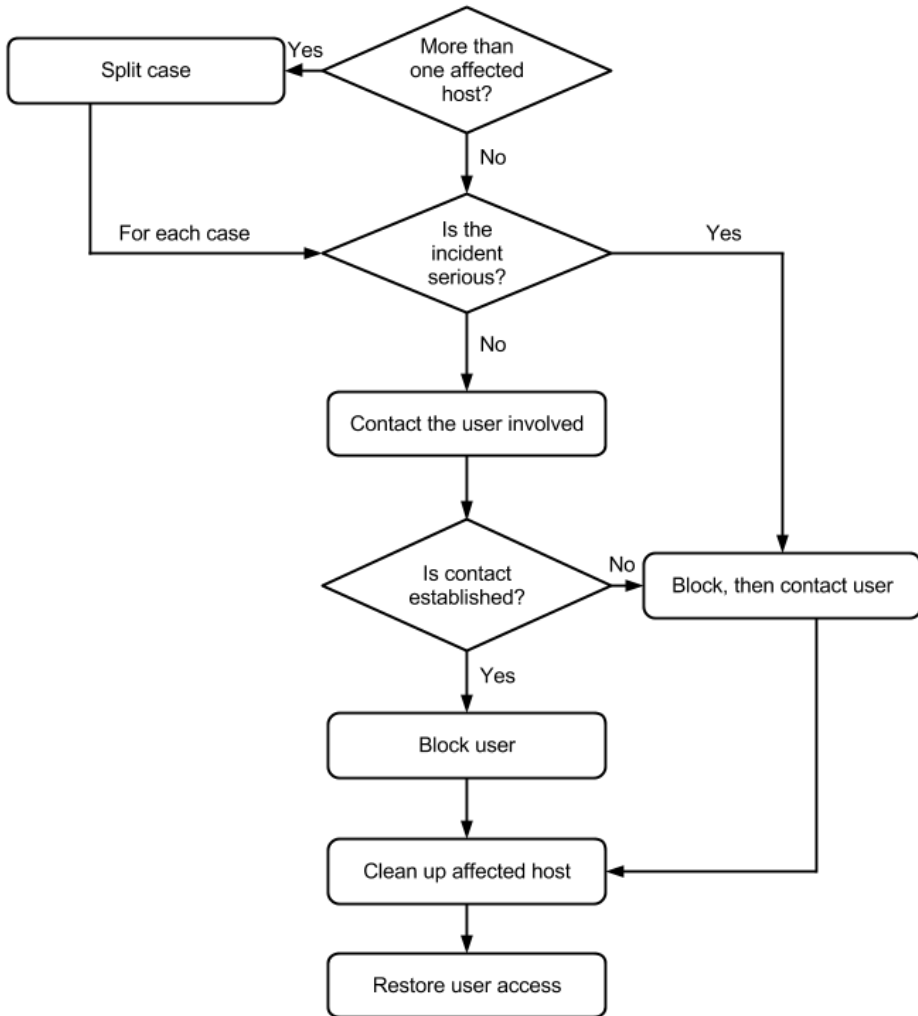
Figure 5.2: Workflow for a Botnet Incident

Escalation Organization A has a contingency plan for the IT department that describes a set of incidents. This plan is initiated if an incident is particularly serious. It does not directly target information security incidents, but it includes scenarios where systems are unavailable. When an incident is of such a severity level that the contingency plan must be initiated, the management is also involved. The contingency plan includes communication routines related to incidents.

Electronic Evidence   The organization has a well functioning coopera-
tion with the police. In situations that might lead to criminal cases they
do not try to investigate themselves, to avoid compromising evidence. If
they suspect criminal activity they contact the police and do nothing else
prior to this contact. They do however block users upon request from the
police, in order to preserve evidence. Accessing user-owned files is done in
compliance with the Norwegian Personal Data Act.

5.1.4   Lessons Learned

The IT security manager stated that their routines usually work well. In
cases where they have not worked well they perform a review of the incident.
The IT security manager pointed to the allocation of responsibilities as well
as lack of staff and routines as challenges related to incident management
in the organization:

> *"I would say that it is perhaps too often that we have incidents*
> *where we do not have routines that are sufficiently described*
> *[...] You cannot have routines for everything, but I also think*
> *it originates in the organization and how we are staffed to han-*
> *dle situations. There is no point in writing routines that do*
> *not establish ownership to a process [...] For example we have*
> *routines for handling a botnet incident, and two cases were dis-*
> *patched this morning and no-one has addressed them yet."*

The IT security manager collects information about information security
incidents and delivers annual reports to the management. This way they
keep an overview over previous incidents. They do not evaluate all inci-
dents as this would be too much work. It turns out that lack of awareness
among users is often the root cause of incidents. Therefore he believed
the "solution" to these incidents is awareness-raising activities rather than
changes in routines.

Organization A has a review process, where they review processes and
people and not only technical details. They have reviews for incidents of a
certain scope and when they experience that their process is not efficient
enough or their process description is unclear. The IT security manager
is satisfied with their review process. Identified improvements have been
implemented to avoid mistakes being repeated.

Organization A has exchanged information and experiences with partners, NorCERT and other CERTs in relation to specific incidents.

In relation to lessons learned activities he stated:

> "There is always room for improvement"

5.1.5 Employee Survey

When the 15 employees were asked whether they were familiar with the organization's security policy their answers varied greatly. Three answered yes and five answered no, whereas seven said they had heard about a security policy but that the content was not known in detail.

Most employees said they had received suspicious e-mails, many on several occasions. However, one employee emphasized that it is primarily spam and rarely customized or targeted e-mails. None of the employees in the survey acknowledge to have opened attachments or carried out instructions given in these e-mails. The majority of the participants said they did not report suspicious e-mails to anyone, while a few said they report some cases.

Only a few of the employees in the survey claimed they knew what an information security incident is. About half acknowledged that they did not know or that they were not familiar with the definition, whereas the rest were unsure. When asked to give examples most employees mentioned sharing passwords, login credentials or sensitive information as possible information security incidents. Even though many employees were uncertain what an information security incident is, all of them stated that they were attentive to incidents in their everyday work. Several employees explained their uncertainty by statements such as:

> "I'm not often in situations where information security is relevant."

One employee said that an implementation of a new door locking system to improve security in the department had led to employees becoming more incautious and left their computers and office doors unlocked more often.

Only one employee claimed to know in which cases and to whom security incidents should be reported. The majority of the survey's participants were unsure which incidents to report. Nevertheless, most said that common

sense guided their choices and that they would report to their immediate supervisor if necessary.

About half of the employees had participated in online lectures or presentations addressing information security. One employee emphasized that:

> *"There are always things that are useful to be reminded of."*

Even though several employees said most of the content in these lectures was already known material, they still found it useful.

5.2   Case B

This section describes the findings from case B, where the two interviewees from the organization were the IT security manager and the supply chain manager, both working in the IT department. The interviewee from Supplier 1 was a technician in basic IT operations as well as being a security coordinator between Supplier 1 and the organization. The interviewee from Supplier 2 was the service manager for one of Organization B's systems.

5.2.1   Preparation

The interviewees from Organization B define *security breaches* as events violating the organization's security principles caused intentionally by employees. Examples include employees visiting illegal websites or sharing their passwords. *Security incidents* on the other hand, are events threatening information security, but not necessarily caused by disloyal employees. Security breaches and incidents are often seen as deviations from normal activity and often require some sort of structural change. Organization B has a deviation system that keeps track of all kinds of deviations, whether it involves physical shortcomings or issues related to information security.

The interviewee from Supplier 1 defines a security incident related to monitoring of a network as when malware has entered the systems and has the potential to exercise either limited or massive damage. Other security incidents are related to users of the systems, such as disloyal employees, and are much harder to detect. He claimed it is almost impossible. This definition is known among those working with security related to Organization

B. The interviewee from Supplier 2 defines unauthorized access of information as being a security incident when this access can cause harm to the organization, customers or other related parties. This is the interviewee's personal definition, but it is grounded in a definition internal to Supplier 2.

When the interviewees from Organization B were asked to consider the worst possible security incident the organization could experience, they said that their biggest fear is disloyal employees leaking information to outsiders without being discovered. Compromised or disclosed information is considered very serious, but in most cases where this is caused by an error it is easier to detect than disloyal employees. Information is the most important asset to protect for the organization as most other things can be restored or repaired.

In addition to information disclosure, the interviewees from Organization B see service interruption as a severe consequence of incidents. Ensuring service availability and business continuity are thus high priorities. Unavailable services could lead to employees not getting any work done which may cause major financial losses for the organization. Availability is therefore extremely important and thus investments to ensure availability are justified by the financial costs of unavailable services. Redundant equipment and other mechanisms are implemented to ensure the availability of services. Supplier 1 makes sure that Organization B's systems are backed up daily and performs tests to confirm that these backups are usable. They have two data centres in order to increase the level of redundancy.

In addition to financial losses and information leakage, the organization sees reputational damage as a serious consequence of incidents:

> "If sensitive information concerning customers is leaked or lost,
> it is a contractual breach as well as a violation of trust that would
> imply risk of reputational damage."

The interviewee from Supplier 1 stated that loss of sensitive data that are important to the organization's core activities as being the worst possible incident Organization B could experience. He named financial losses, breach of trust and reputational damage as consequences of such incidents. The interviewee from Supplier 2 saw industrial espionage as being the worst security related incident organization B can experience. Such an incident can have financial consequences, as foreign organizations could develop Organization B's products at a lower cost.

The security policy is the main governing document for activities conducted within Organization B. Its intention is to define senior management's position concerning IT security, and give an overall picture of where the organization stands with regard to information security. They have no policy that specifically addresses incident management, only practical routines and supporting tools.

To avoid vulnerabilities in legacy software being exploited, Organization B's computers are scanned regularly and software with security holes or not in use is removed. When new vulnerabilities are discovered they are categorized and prioritized and Supplier 1 determines how urgent the following update is. For zero-day vulnerabilities they may shut down certain services.

The IT manager said that one of the most challenging parts of incident management is constructing a holistic plan. More often than not, things no one had thought of occur and they need to be handled. Hence, ensuring a solid information collection during incidents and making correct decisions at the right time are more important than having a detailed plan. Their experience indicates that the most important thing is to scale correctly, understand the situation and put relevant measures into action. That is also why they believe it is important that not too many have the authority to make important decisions during incidents, which they have tried to limit through their contingency plan.

Organization B has developed plans for communication during incident handling. The contingency plan states who is responsible for communication, both internally and externally. It is always a representative from Organization B that is to communicate with the media or the police, not any of the suppliers. The IT manager or the supply chain manager are always available in case of an emergency. To ensure communication during serious incidents, important contact persons have an instant messenger application as well as SIM-cards from several network providers. Organization B has a general contingency plan as well as supplier specific contingency plans and a specific plan for IT services and infrastructure. The IT contingency plan is connected to both the general plan and the supplier specific plans. The IT contingency plan is initiated when the IT manager in consultation with the management and their IT operations suppliers define an incident as a crisis or a catastrophe according to the definitions in the plan.

Supplier 1 keeps track of trends related to security incidents, by monitoring

their own internal systems. These trends are discussed with Organization B. Supplier 1 has a case management system where all cases are logged. This way they keep track of previous incidents for Organization B. They also have specific contingency plans developed in cooperation with the organization. These plans are audited every second year. As preventive work, Supplier 1 is responsible for securing the network.

Supplier 2 has a plan for incident management for Organization B as well. The plan is based on various impact levels of incidents. This plan is only related to applications, as Supplier 2 is not responsible for data. They need plans to be in compliance with the Service Level Agreement (SLA). They have specific plans regarding communication that specify who to call, when to call, how often to call and what the conversations should contain. Their PR department handles communication with media. Supplier 2 is required to try to fix any vulnerabilities when they are discovered. They are relatively new as a supplier for Organization B and thus have no records of previous incidents.

Standards and Guidelines   Organization B bases many of their processes on the ITIL framework. Standards are mainly used as a basis for the fundamental thinking related to security in the organization. All IT managers have had training in the ISO/IEC 27001, 27002 and 27035 standards. Additionally, some employees are certified in ITIL security. Organization B has set compliance with the ITIL framework as a requirement for Supplier 2.

Supplier 1 bases everything on ISO standards and tries to adapt their contingency plans to these standards. They have not implemented any standards specific to incident management, such as the ISO/IEC 27035 standard.

The IT manager said that just as important as being familiar with standards is being familiar with the internal documents describing how the organization performs incident management.

He emphasized that:

> "The most important thing when a crisis occurs is knowing what to do, not knowing what the standard says."

It is important that employees are familiar with internal routines, hence rehearsals are conducted regularly.

Awareness and Training   All employees participate in an introductory course where routines for reporting incidents are explained. Additionally, employees are informed through the intranet in cases where they need to be aware of new trends or specific spam e-mails. To raise awareness around IT security, Organization B has previously conducted online lectures for employees via the intranet, addressing various security related topics such as secure use of USB sticks, viruses, social engineering and spam.

The supply chain manager said that it is difficult to measure the effect of awareness campaigns. Nevertheless, the number of security incidents has decreased during the last three years.

To raise awareness and best prepare for incident handling in practice Organization B conducts rehearsals regularly, discusses internal routines with employees and includes external suppliers in their training. Both Supplier 1 and Supplier 2 are included in contingency rehearsals. Previously, rehearsals have been set up such that incidents escalate and change as employees discuss what to do in given scenarios.

IT managers within Organization B as well as the crisis team, basic operations and customer service from Supplier 1 can be involved in rehearsals. They will be presented with an incident and the rehearsal seeks to reveal whether their routines work well or not. It is normally Organization B that initiates these rehearsals. The interviewee from Supplier 1 emphasized the importance of rehearsals:

> *"Yes, we have to continuously rehearse our routines, otherwise they would never work."*

Supplier 2 conducts contingency rehearsals on paper for the crisis team. Additionally they have training for the service desk employees. They have as a requirement that employees are to be ITIL certified.

Information management, allocation of responsibilities, communication and crisis communication have been identified as areas of improvement after rehearsals. They have revealed the need for a way to communicate to employees during emergency situations that is not dependent on e-mail or the intranet, as these are not necessarily available during a major crisis.

Organization B has outsourced services with several external suppliers and thus collaboration and coordination are extremely important factors in their incident management. Having effective and sufficient coordination as well as distinct and well-established roles during incident response are highlighted

by the IT manager as important things to train for. This is supported by
the interviewee from Supplier 2 who mentioned that if rehearsals reveal
ambiguity concerning roles and responsibilities, they need to change the
contracts in order to clarify this.

5.2.2   Detection and Analysis

Organization B's network supplier or other partners may detect incidents.
The supply chain manager is convinced that underreporting of incidents
exist, but does not see it as a problem. This is supported by the interviewee
from Supplier 1. He also mentioned that it is probably impossible to detect
everything. The potential high degree of underreporting does not imply
that they miss seeing what the main threats are. The supply chain manager
said that even though not all incidents are reported, the overall trend is still
very apparent in their statistics and thus the right measures to avoid serious
incidents can be implemented.

Initial Detection   Organization B detects incidents in several ways. Anti-
virus detects and reports viruses, and in some cases employees themselves
report that their computer is not working as expected. In the latter case
the employees are to report to the service desk at Supplier 1. Supplier 1,
that has the overall responsibility for monitoring the network, may also de-
tect changes in traffic indicating security incidents. This sensor network is
further outsourced to an external security company. The IT manager said
that most of these initial detections are handled automatically, and that
very few incidents require manual responses.

Categorization   Organization B has developed their own framework for
categorizing incidents. Inputs to the categorization are the number of per-
sons and departments that are affected in addition to the incident's severity
level. The IT manager emphasized that this categorization is quite similar
to what is presented in standards and that it is often the availability aspect
that is in focus for incident categorization. The central contingency plan
states when incidents should be categorized as a crisis or a catastrophe to
ensure that they are handled correctly.

Supplier 2 categorizes an incident to be a crisis if it concerns most of the
users and a system is down. This categorization is based on the contract
between Supplier 2 and Organization B. The categorization is further used
to prioritize incidents.

5.2.3   Incident Response

Minor incidents such as infected computers happen quite often and are seen
as part of normal operations. If there is a risk of escalation, users' network
ports can be shut down before users are contacted. Sometimes situations
arise indicating a serious security breach and the IT manager is contacted.
In case of security breaches, the employee involved has to be dealt with
which might need involvement from the management.

Organization B does not have an established check-list to follow during
incident response. There is a check-list included in the central contingency
plan, but not one that addresses IT specifically. This was one of the things
that were discovered through a rehearsal and they are currently working on
developing such a check-list. The IT manager said this is an area they wish
to further develop to improve their incident handling capabilities.

Lack of proper communication may lead to unnecessary trouble. The supply
chain manager said that the implicit knowledge of responsibilities in minor
cases is an example of routines that are difficult to document properly.

> *"Problems may arise even with minor incidents when everyone
> assumes that it is someone else's responsibility."*

The supply chain manager highlighted the challenge of deciding in what way
and how much information should be given to employees during incident
handling. This is challenging as it is very individual how much information
people both want to share and receive, he said. Further, the IT manager
stated that knowing when to communicate, what to say and to whom might
be the most challenging aspects of incident management.

When Supplier 1 first detects incidents they usually notify the organization
by e-mail. After detection they initialise a team that handles the incident.
If the incident spreads there can be assembled a crisis team and the commu-
nication in that case is by e-mail, phone and personal contact. Most cases
that Supplier 1 handles are routine cases and standard procedures can be
used. If an incident is very serious the security coordinator is involved and
is responsible for communication between Supplier 1 and the organization.
All incidents are logged in the same system. The log includes root cause
of the incident, the impact, potential breaches of SLAs, actions taken and
possible solutions.

Supplier 2 has procedures for handling known security incidents. They do

not have any automatic processes as incidents suited for automatic handling are handled by Supplier 1. Many of the activities in incident handling are determined as the incident evolves. This is based on what is experienced at that time, previous experiences, feedback and expectations. To ensure that incidents are solved a fast as possible, the technician(s) who gets the task will only focus on fixing the incident and is not to be disturbed until it is solved.

Incident Response Team Organization B does not have a dedicated IRT, but they have a dynamic team responding to incidents, it changes with the type of incident they are dealing with. Supplier 1 acts as a response team and handles most minor incidents related to IT operations as part of their normal activities. The responsible person and the response team depend on the characteristics of the incident.

For minor incidents, the team is almost entirely outsourced to Supplier 1, but is gradually insourced as the severity of the incident increases. Thus, members of the team may vary. The IT manager said:

> "We try to scale the team in response to the specific incident we are dealing with."

The sequence of the scaling is stated in the IT contingency plan, where particular roles and activities are described. The permanent members of the team are the IT manager and the supply chain manager as they are involved in the handling of most incidents. Team members have other tasks beside incident management, but if there is need for them to aid in incident response, all other tasks are put on hold.

For incidents categorized as a crisis, a crisis team will be formed. The team is composed of the IT manager, the supply chain manager, management from Supplier 1, the person at Supplier 1 responsible for IT operations for Organization B at the time of the crisis and whenever necessary representatives from Supplier 2. For the most serious incidents, a central manager in Organization B will be in charge of the situation.

Supplier 1 has a team available 24/7 that receives (often automated) incidents reports. They can subsequently determine what to do about it. Supplier 2 also has teams to handle incidents for Organization B. They have a crisis team and a support function to handle daily management and maintenance. The members of the team are available 24/7. They look for improvements in the process and have ongoing reviews of plans.

Workflows   Supplier 1 handles incidents related to IT operations. Figure 5.3 illustrates the workflow for incidents (that are not escalated and categorized as crises).
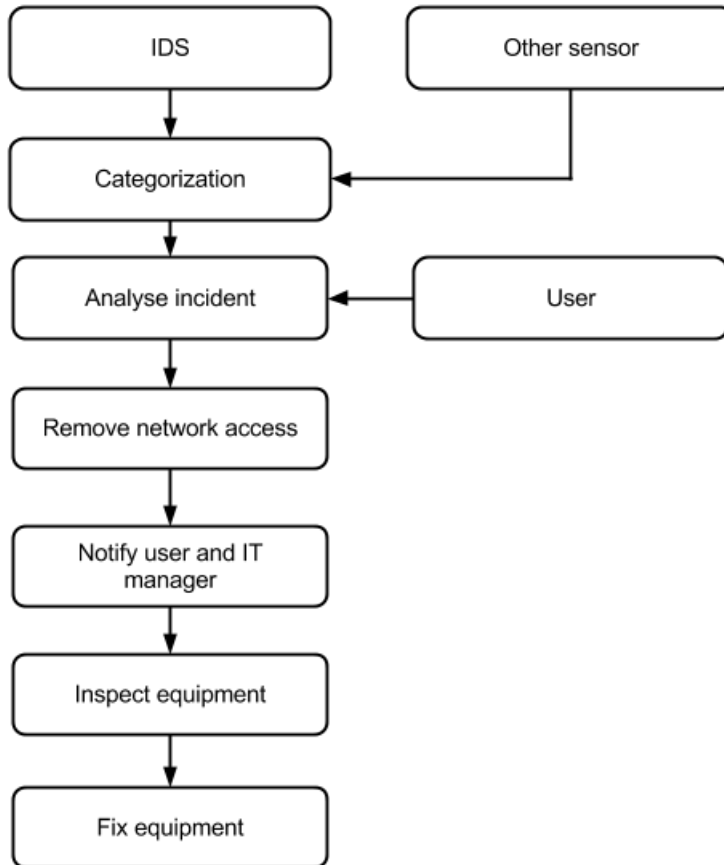
Figure 5.3: Workflow for Incidents for Supplier 1

- The external supplier of the sensor-network receives notifications from sensors and categorizes the incidents.

- If the incident is categorized as high the customer service centre at Supplier 1 gets a notification as well as a phone call from the external supplier of the sensor-network. The customer service centre can also receive notifications from users.

- The customer service centre investigates each individual case.

- The network access for the equipment in question is removed

- The user and the IT manager of the department involved are notified.

- The equipment is brought in to Supplier 1 for inspection and subsequently fixed.

There are dedicated people that take care of this process and there are 2-3 people on rotation. These people are well informed of the procedure.
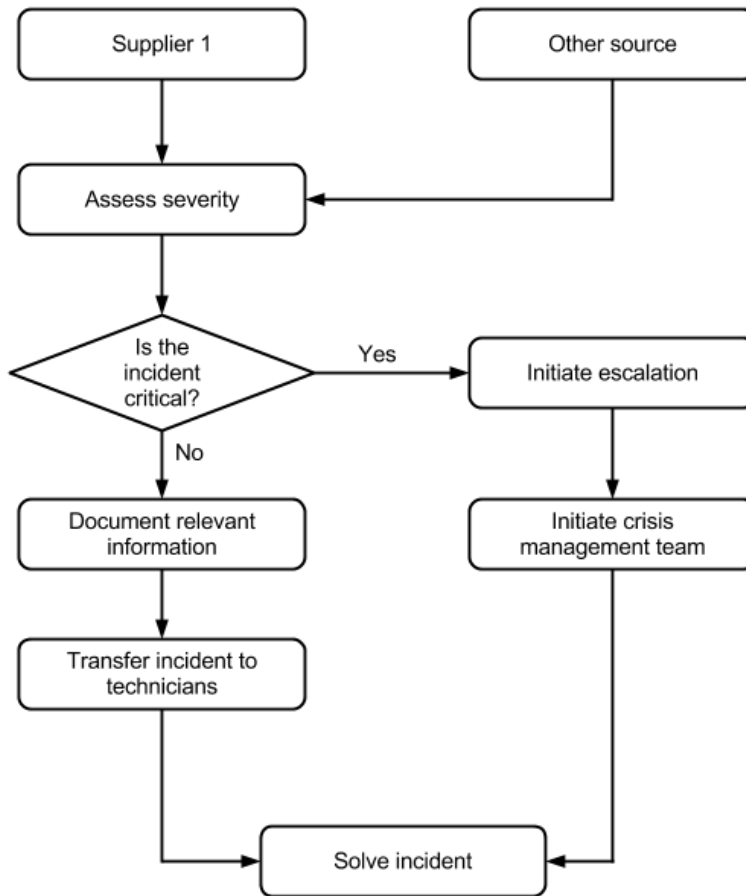
Figure 5.4: Workflow for Incidents for Supplier 2

Supplier 2 is responsible for handling incidents related to applications in Organization B. Their incident workflow is illustrated in figure 5.4.

- The service desk receives incident reports. Supplier 2 is the second line of incident handling, so they do not get reports directly from users. Usually they receive reports from Supplier 1.

- The severity of the incident is assessed by the service desk employee in cooperation with the person reporting.

- If the incident is critical the service desk calls a person responsible for escalation who subsequently initiates the crisis management team. This person can call people and have them come to work if necessary. The crisis team is responsible for getting the incident solved.

- For any other incident the service desk will document all reported information and transfer the case to the correct group of technicians.

Escalation   Organization B's team is scalable, but it escalates whenever incidents escalate and reach a high severity level. Whenever incidents are of such severity that escalation is necessary, they primarily try to recruit extra internal employees to the team. In some cases external experts are needed to respond effectively to an incident.

For incidents that are related to employee privacy, Supplier 1 calls in a central security advisor. This is done to avoid privacy violations. Supplier 2 has developed clear routines for escalation and contact persons both in Organization B and Supplier 1. They have mandate to call in an external crisis management team if necessary.

Electronic Evidence   In case of security breaches, i.e. employees violating policies deliberately, all logs are preserved in case of need for future investigations. In cases where it is suspected that an employee is being disloyal, his user account is blocked to avoid potential evidence being deleted. The supply chain manager said assessing what to do in each individual case is difficult as sometimes incidents may be more serious than first assumed. Supplier 1 brings in an expert from central parts of their organization in cases where electronic evidence must be preserved. In these cases all communication must be encrypted. The police can be brought in or evidence can be handed over to the police for further investigations.

5.2.4 Lessons Learned

Incident reports are in most cases constructed by the two main suppliers and include excerpts from logs, information on what happened, what was the cause, what was done to solve the incident and proposed measures to avoid similar incidents in the future. Organization B receives monthly reports from both their main IT suppliers, where all incidents are recorded. Supplier 2 only includes critical incidents or specially requested incidents in their reports. All IT managers as well as the security coordinator from Supplier 1 participate in a monthly meeting where monthly incident reports from the organization's main suppliers are discussed.

Organization B only conducts review meetings after serious incidents, which might be a couple of times a year. The participants in these meetings are the involved IT manager(s), the service manager and the security coordinator from Supplier 1. Additionally, four times a year, incidents concerning intelligence, espionage, crime for profit and information security are discussed within the organization's security board and are reported to the management.

The IT manager said that they are interested in obtaining a high contingency and security in their operations and that learning from others is an important factor in achieving that. To benefit from others' experiences they often think about how incidents in other organizations would have affected themselves. In that matter, incidents that occurred in other organizations contribute to development and improvement of contingency plans. The IT manager said that learning from others' experience is important since the scenarios are real and could most likely happen in their organization as well.

The interviewee from Supplier 1 said that when they detect botnets they are able to handle them fast and effectively. He mentioned that one thing they learned from rehearsals is not to trust electronics. Thus, contingency plans should be available on paper as well as electronically. Supplier 2 has so far been able to handle all critical incidents the last years in accordance with the SLA. One contributing factor to this success was that they contacted the right technical resources when needed. Nevertheless, routines have not always worked well, and an example is when various suppliers are involved and no one takes responsibility for the error. Supplier 2 is a consortium and therefore they often have to cooperate. The interviewee has experienced various suppliers with different focuses:

> *"Some are for example of the understanding that they do not own the error, while someone else understands that they own it. In cases where the owner does not understand it, it is very challenging to make it work. And it takes a lot of time [...] This is the greatest challenge [...] It is also a political "game". Who will pay for it?"*

Supplier 2 shares experiences from incident handling internally in their team. They conduct post-review sessions where they discuss what was done and what could be improved. This is done in cooperation with Organization B, but not with other suppliers. The interviewee mentioned that there are many sources of information and handling these and collecting the correct information can be very difficult.

5.2.5   Employee Survey

Among the 15 participating employees, only two answered that they were not familiar with the organization's information security policy. Eight answered that they were to some extent familiar with it, but that they did not know the details or that they had read it once. One of the employees mentioned that there have been made many changes in the policy during the last years and that employees have not always been notified about the changes.

Only one employee had never received any suspicious e-mails. Several said that they receive such e-mails very often, but that it is mainly "common" spam and easy to recognize. No one mentioned to have received targeted e-mails. No one acknowledged to have carried out instructions in such e-mails, except one that claimed he once did it in a secure way out of curiosity. He clicked a link to examine the quality of the phishing-site, but did not carry out any instructions from there on. A few of the employees have reported to have received such e-mails, but several mentioned that they do not report it, because it is so common. One mentioned that it happens so often, so it is difficult to know when you are suppose to report, but that he would report whenever in doubt.

Six employees claimed they knew what an information security incident is. Five could not provide a definition, but had an idea of what it is. The rest claimed that they did not know. Most of them were however able to give examples. Among them were information or passwords astray, storage of

confidential information on unencrypted USBs sticks, use of unknown USBs sticks, breach of security instructions or sharing once computer. There were also given examples that showed that there were employees who obviously did not know what an information security incident is:

> *"Information security incident [...] That must be when someone gives away money they are not supposed to?"*

Most employees claimed they were attentive to incidents, even though several of them stated that they did not know what an incident is. Some elaborated their statement by providing examples. They said that they lock their screens when they leave their computers and lock their doors when they leave their offices and destroy sensitive documents. The IT manager of one of the departments said that they try to make sure employees know that they will not be held responsible if they caused a security incident. This is done to mitigate underreporting of incidents.

Most of the employees were unsure about which cases they should report. Most of them claimed that they would have reported to the local or central IT manager, but some mentioned that they did not know if this was correct. One employee said that he would report to the local IT manager or to Supplier 1. Some of the employees that were not able to define a security incident, still believed they would be able to know whether to report should an incident occur. There were also a few claiming that they were not familiar with reporting procedures, because they had never needed to be.

Organization B has previously conducted an awareness campaign where all employees received a set of online slides each week for a period of time. The IT manager of one of the departments claimed they got positive feedback from employees. This is supported by several of the employees in the survey who acknowledged to have read these slides and thought it was useful, even though much of it was well-known material. Several of the employees wanted such lectures more often:

> *"The content was known, but it is all right to have read it."*

> *"Having an IT instruction is one thing, but being **reminded** of security instructions is always useful."*

Only two employees who had read the slides in the awareness campaign did not find them useful. One of them mentioned that some of the proposed measures were socially unacceptable, such as refusing a customer to use

their own USB sticks when using one of the organization's computers during a presentation. The other employee mentioned that some of the measures were so strict that he would rather take the risk of security incidents than following them.

5.3   Case C

This section describes the findings from interviews and document study for case C. The interviewee was the IT security manager.

5.3.1   Preparation

Organization C has implemented several measures to prepare for security incidents. Various expertise areas are required to respond effectively to different types of incidents and thus Organization C uses several incident handling plans. They have developed three frameworks for incident management where each framework addresses a specific category of incidents. These frameworks describe relevant roles and activities for handling Organization C's three main categories of incidents:

- IT operational-related incidents (service interruption etc.)

- Information security incidents (breach of confidentiality, integrity and in some cases availability (such as DDOS attacks))

- All other incidents (terror, accidents etc.)

The IT security manager described an incident as being loss of information. However, other events such as DDOS attacks are also defined as incidents even though it is the availability of information that is compromised rather than confidentiality or integrity. He stated that in most cases he thinks of security incidents whenever there is an attacker trying to steal information. He highlighted:

> "90-95% of the security incidents we experience are availability related incidents"

It is essential for Organization C that customers trust them and their services. The IT security manager identified loss of sensitive customer information, service unavailability and other incidents that could possibly lead

to a weakening of the trust relationship with customers as the most serious consequences of information security incidents.

Organization C's security policy aims to communicate the management's direction and commitment to information security. One of the main objectives stated in their security policy is that information security should be part of their risk management and long-term strategy. Information security should be revised, improved and sufficient resources should be allocated. The policy states that it is the management that has the ultimate information security responsibility, but that their success relies on the collective effort of everyone involved. Information security is stated to be a critical business issue, and thus Organization C strives to create a security-positive environment.

In addition to the top level security policy, there are different policies for each individual department as their need for security varies. Additionally, contingency plans are implemented and revised continuously. The organization has a predefined plan for communication with the media during major incidents.

Awareness and Training The IT security manager stated that they perform extensive work to raise awareness related to security among employees. New employees participate in courses where they are introduced to the organization's security handbook and they have to sign that the content is known and understood. The security handbook is also revisited annually during employee appraisals where employees have to reconfirm that the content is known. In addition, employees are invited to lunch colloquiums and security related presentations regularly. The intention is to increase the overall competence and to ensure that security guidelines are known.

Organization C does not conduct training for employees that addresses the most common incidents. The IT security manager emphasized that their plans and procedures are being used so often in practice that there is no need to arrange training for these cases. However, Organization C conducts rehearsals once a year with a scenario they believe is useful. They perform rehearsals in cooperation with customers regularly, as the customers often wish to include their IT service providers. Additionally, training in cooperation with the government takes place every other year.

5.3.2   Detection and Analysis

There are several ways that incidents can be detected.

Initial Detection   The initial detection of incidents can either be performed automatically by a server, triggered by an alarm or discovered manually. Often, network analysis has to be conducted manually to detect security breaches. One of Organization C's requirements for incident management states that all incidents must be registered in their systems. Whenever employees experience something abnormal or unexpected they are advised to report it to the IRT. Examples include e-mails from unknown senders or e-mail attachments that do not work as intended.

The IT security manager suspected underreporting of incidents among employees. He believed the threshold for reporting is high and that employees often omit to report suspicious events. This could either be due to employees failing to see the importance of reporting incidents or that they do not want to acknowledge potential mistakes they made. The IT security manager said they would rather have too many events being reported than too few, and they therefore work continually to emphasize the importance of reporting incidents.

Security vulnerabilities are reported through a risk framework, where they are evaluated, categorized and potentially escalated. Organization C does not operate with anonymization for employees that report security events, but codes of conduct say one could use an external law firm if someone wishes to report incidents anonymously. However, this opportunity has never been utilized by employees.

Categorization   Organization C bases their incident categorization on the ITIL framework. They categorize incidents as being of low, medium or high impact. Whenever incidents are handled they are linked to these levels and handled according to predefined procedures. An incident's impact level will determine what can be done in response. For high impact incidents, authorization is needed from customers in case systems need to be shut down or changes have to be made in the production environment. This represent complex incident responses and are referred to as emergency changes, that are in some cases necessary to mitigate serious consequences.

5.3.3 Incident Response

The main purposes of incident response in Organization C are to retain normal business operations, minimize business impact by ensuring service availability and to find a temporary solution to the problem. The IT security manager stated why keeping services up and running at all times are so important:

> *"Customers evaluate us mainly based on the availability of the services we deliver."*

Hence, restoring service availability is the number one priority in the organization's incident response.

Incident Response Team   In addition to dedicated incident managers, Organization C has its own IRT to assist in major incidents. The IRT handles incoming notifications from internal users regarding security issues and may deal with incidents concerning customers. Employees work continuously with "normal business operations" and thus need security expertise available 24/7 in case of incidents. The IRT works as a point of contact for the entire organization. They primarily assist in incident response and otherwise work as a pool of resources for incident managers.

It is the incident managers that handle incidents, whereas the IRT assists with their expertise on security incidents. Additionally, the IRT is granted certain mandates that allow them to shut down systems or acquire external expertise and assistance up to a predefined cost limit.

Organization C has their own IRT handbook. The handbook aims to describe how the IRT should operate and is used to explain internal routines to new team members. The IRT handles most of Organization C's security incidents as well as some customers'. Most customers have their own IRT, although Organization C offers their IRT as a service for customers that do not have the capacity for establishing or need of their own team.

The IRT communicates and coordinates with involved parties throughout the incident response. For critical incidents, a second team called the Critical Incident Management (CIM) team works as an internal support function for the IRT and provides complementary competence. The two teams work together to resolve critical incidents. One of the requirements for Organization C's incident management process is that all actions taken

by the teams that add value to the incident handling process should be
recorded such that others can continue the work if necessary.

Standards and Guidelines   Organization C bases all of their service
management processes on the ITIL framework presented in section 3.2.4.
They have implemented the ISO/IEC 27001 standard, and have several
certifications. Their incident management processes, however, are mainly
built on the ITIL framework. The IT security manager is not familiar
with the ISO 27035 standard that addresses security incident management
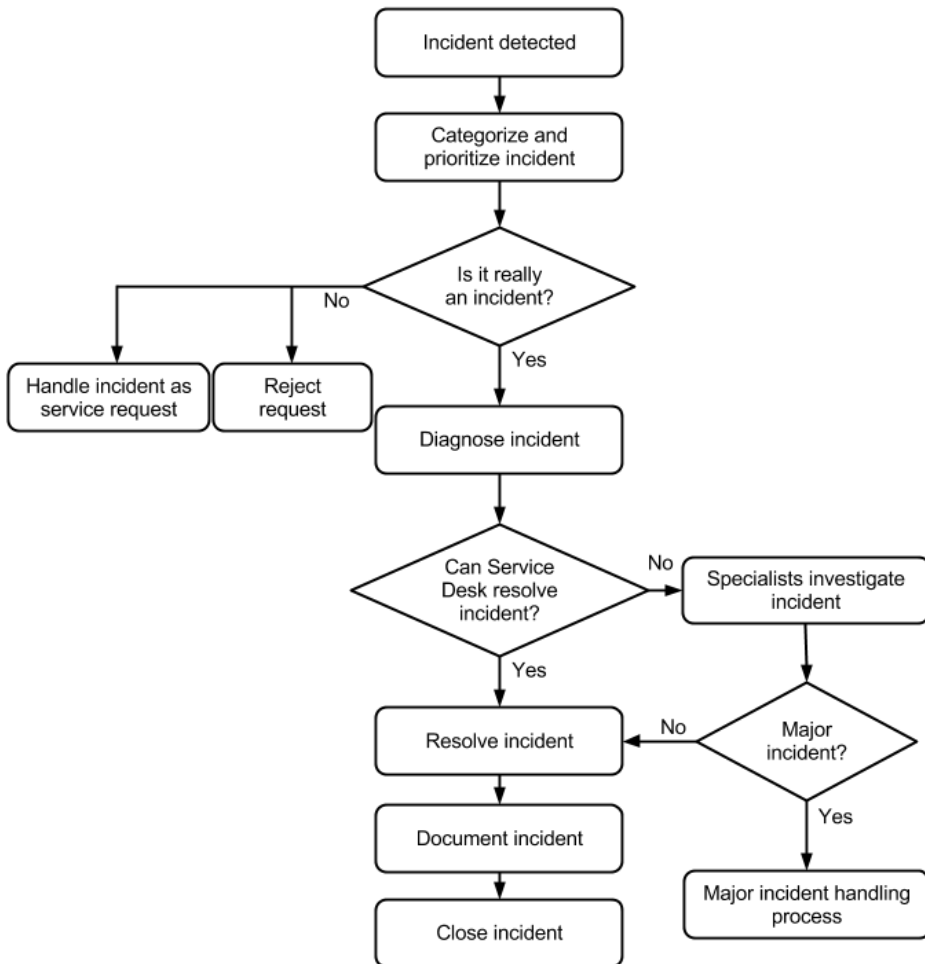specifically.

Figure 5.5: Workflow for Incidents

Workflow for incidents   The workflow for incident management is based on the processes described in the ITIL framework. Figure 5.5 illustrates the workflow, and is derived from organization specific documentation as well as information given in the interview.

- An incident is first detected by or reported to the service desk.

- Each incident is categorized and prioritized such that it can be handled correctly. Further, the service desk decides whether the reported event is truly an incident. In case of false alarms, the reported events are either rejected or handled as service requests.

- The incident is diagnosed and possible negative effects are considered.

- The service desk assesses whether the incident has a known solution and whether they are capability of handling it.

- Incidents with unknown solutions are sent to a group of specialists that conduct further investigations.

- Escalated and severe incidents are passed on to the "Major incident handling" process when appropriate.

- Once a solution is found, either by the service desk or group of specialists, incidents are resolved.

- The incident is fully documented with all relevant information.

- The incident is closed and users confirm that the incident is fully resolved.

Workflow for major incidents   Major incidents are defined by the ITIL framework as incidents of the highest and second highest priority. Organization C has separate procedures for major incidents. Incidents in this category usually have a high degree of user impact and thus have higher urgency and stricter time constrains for response activities. These procedures are initiated in the "Major incident handling process" whenever incidents are assessed as major. Figure 5.6 illustrates the workflow for major incidents. The content is based on organization specific documents as well as information given during the interview.

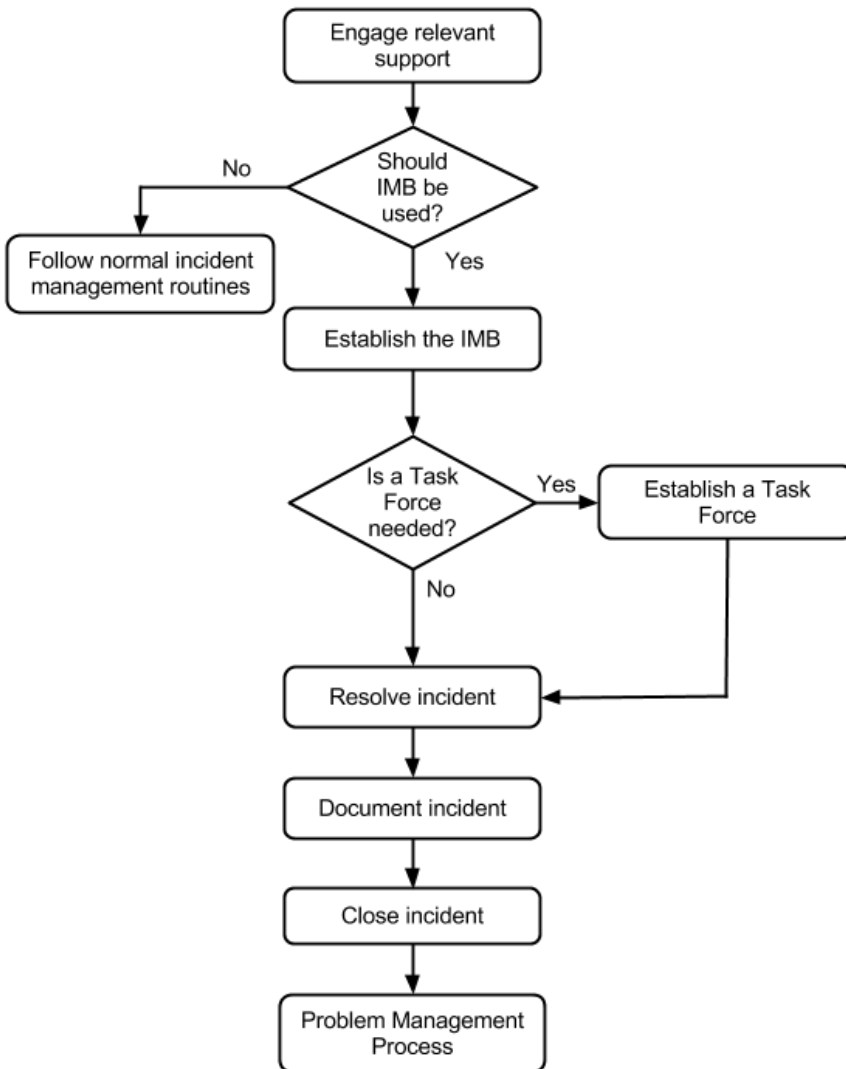Figure 5.6: Workflow for Major Incidents

- When the organization handles major incidents, support in form of a Service Manager, Incident Manager or the CIM team are engaged in the incident response.

- It is evaluated whether an Incident Management Board is needed to handle the incident. If it is not, the incident is handled according to normal incident management procedures as illustrated in figure 5.5.

- An Incident Management Board is established to ensure proper management and appropriate handling of the major incident. The IRT may be part of the Incident Management Board if necessary.

- If dedicated resources are needed, a Task Force is established. A Task Force is an ITIL term for a dedicated group of resources that are put together to solve a specific task.

- When a solution is found, either by the Task Force or the Incident Management Board, the incident can be resolved.

- The incident is documented and activities are logged.

- The incident is closed and users have to confirm that it is fully resolved.

- The incident is handed over to the Problem Management Process for further analysis.

Escalation   Organization C has no predefined routines for external escalation during incident response, even though they have done it several times in practice. Internal escalation is performed as described in the workflows.

Electronic Evidence   Organization C has no in-house expertise on forensic analysis of electronic evidence. Mirroring disks for use as digital evidence approved for Norwegian courts is the only thing done by the organization itself with regard to electronic evidence. If there is need for analysis of the disks, this is performed by an external third party or by the police.

5.3.4   Lessons Learned

Organization C structures their learning process in accordance with the problem management process from the ITIL framework. Improvements are identified during this process.

After rehearsals a set of improvements are identified and summarized. Often, interaction with external parties are identified as areas of improvement, especially interaction with customers. Collaboration and coordination across organizations and teams have proven to be challenging as IT service providers and customers often handle different parts of incidents.

A centralized tool is used to document incidents in addition to experiences, potential improvements and internal audits. Meetings are held after major

incidents where the incident response process is reviewed. Post-incident
meetings are held by a problem manager who is responsible for the ITIL
problem management process. Participants vary with the nature of the
incident and the targeted environment. The IT security manager recognizes
the benefits of post-incident meetings and stated:

> *"Often concrete measures are identified after incidents. Both
> organizational, process-related and on the investment side."*

The IT manager explained why he thinks their routines work well:

> *"Since we are such a large organization we deal with a large
> volume of security incidents and thus our frameworks work well.
> I believe it is much tougher for smaller organizations. If it has
> been years since the last incident it becomes more challenging to
> respond effectively."*

Organization C is currently working on a project for improving their inci-
dent management and so far it has proven to be very effective. It mainly
involves improving the quality of their many and complex value chains. The
IT security manager described why this is important in incident manage-
ment:

> *"One of the most important things with incident management is
> keeping track of and understanding value chains: which, when
> and how components are communicating."*

Through the improvement project they identified weak quality in their value
chain descriptions as a problem for effective incident response. The diag-
nostic work was complex, and sometimes it was challenging to identify what
happened, where it happened and with what consequences. Organization
C has started extensive work to identify any single-point-of-failure. The
project started in one of Organization C's departments but quickly esca-
lated to include larger parts of Organization C as they saw positive results.
The project's objective is to identify vulnerabilities and areas of improve-
ment, whereas it is the various departments' responsibility to implement
the recommended changes. So far the project has led to improvements
and new routines for interacting with third parties and it shows an overall
positive trend for minor incidents within the organization.

5.3.5 Employee Survey

All the 11 participants in the survey said they were familiar with the organization's security policy. A few said the policy's content was partially known, whereas one employee mentioned to have participated in a course addressing the security policy specifically.

Only two of the participants acknowledged to have received suspicious e-mails. Neither performed instructions or opened attachments in these e-mails. They did not report the e-mails to anyone, but one said they discussed it internally. One employee mentioned that he had noticed suspicious e-mails in an inbox for shared e-mails.

Overall, employees seemed to have a good understanding of what an information security incident is. Only one participant did not provide any definition or examples, whereas most mentioned sensitive or internal information being disclosed as typical incidents. All of the 11 participants claimed to be attentive to incidents in their everyday activities or at least that they tried to be.

When asked in which situations and to whom they are supposed to report incidents, their answers varied. Three employees said they did not know, but emphasized that they knew where they could find the relevant information. Leaders and security managers were mentioned as points of contact in case of incidents. However, none of the participants had ever reported incidents. One employee stated:

> "I have the impression that it's probably more situations that should have been reported than that are actually reported."

Except from a couple of employees, everyone had conducted some kind of courses or been given information about information security. Apart from one employee stating that the information provided was too obvious, everyone found it useful. Several measures for raising awareness such as video lectures via the intranet, internal and external courses, seminars and information meetings were mentioned by the participants. The employees who found the measures useful said that it reminded them of best practice for information security.

Chapter 6

Discussion

In this chapter the findings from chapter 5 are discussed and links between research questions and findings are established in sections 6.1, 6.2 and 6.3. The research questions were presented in section 1.2. Further, underlying structures of experiences are discussed in section 6.4. These findings are not necessarily directly linked to the research questions, but emerged from the data. This analysis method is based on the general inductive research approach as described in section 2.3.5. Finally, section 6.5 presents our recommendations for performing successful incident management.

6.1   Case A

SANS and ITIL state that having an information security policy is important. Further, the ITIL framework emphasizes that employees should have access to and be aware of this policy. Organization A has developed an information security policy. It may, however, not be well enough established throughout the organization. This is supported by the employee survey where few claimed to be familiar with the policy. It is also consistent with the fact that the IT security manager believes that not all users have detailed knowledge of the policy. Organization A is compliant with the ISO/IEC 27035 standard's recommendation of having a specific policy for incident handling.

Management commitment is highlighted as critical by the ISO/IEC 27001 standard and the IT security manager stated that it is the management's

responsibility to make sure the policy is well established. The policy does not seem to be well established throughout the organization which might indicate that there is lack of management commitment as this is their responsibility.

It is stated in Organization A's information security policy that information shall be classified by the information owners. This is compliant with recommendations from the ISO/IEC 27002 standard that additionally emphasizes the importance of classification to ensure proper protection of information. The fact that so few of the employees were familiar with the information security policy could indicate that they are not aware of their responsibility for classifying their information. This is supported by the IT security manager who stated that the organization's information classification is not satisfactory. He believes that employees are not aware of this specific policy requirement. This could indicate that the organization's information is not sufficiently protected with regard to its sensitivity and value. Organization A processes large amounts of sensitive data, and this finding is therefore alarming.

Organization A has reporting and documentation systems and procedures, which is recommended by all guidelines presented in section 3.2. They also follow the implementation guidance in the ISO/IEC 27002 standard which recommends that those reporting information security events should be notified of results.

Organization A has implemented monitoring systems, such as IDSs, which is recommended by most relevant standards and guidelines. In addition to technical detection mechanisms, users can be valuable resources for detecting incidents, and therefore organizations should have available reporting systems. This was highlighted in a presentation at the "Sikkerhet & Sårbarhet 2013" conference:

> *"Consider employees as part of the organization's sensor network."*
>
> – Vidar Sandland and Hans Marius Tessem, NorSIS

This is especially important with regard to social engineering and targeted attacks, which are increasing. One interesting observation is that employees in Organization A seem to lack knowledge and qualifications to be able to recognize incidents, which might indicate that they are not fully utilized as resources for incident detection. We found that the employees that participated in the survey were unaware that they are required to report

incidents, unaware of how to report and under which circumstances reporting is necessary. Even though the majority of the participants thought that they would be able to figure out whether incidents should be reported, this finding is alarming, especially if it is representative for the entire group of users.

According to SANS, NorSIS, ITIL and ISO/IEC, incident prioritization rules should be based on an organizational impact analysis. One way to evaluate potential organizational impact caused by incidents is to conduct risk assessments. Organization A conducts risk assessments regularly, which has led to a categorization scheme that provides the basis for their prioritization. Hence, Organization A complies with these recommendations. Another important part highlighted in the standards and guidelines is the establishment of an IRT. Organization A does not comply with this recommendation as they do not have their own IRT, but only dedicated personnel for incident handling and a crisis team to handle the most severe incidents.

Several employees mentioned that information security did not concern them. They believed it was not relevant to their work and that they were not exposed to attacks or incidents, despite having access to sensitive information and performing their work on computers. Even though most of the employees in the survey did not know what an information security incident is, they still claimed to be attentive to incidents in their everyday work. These contradictory statements might indicate that information security is not well understood and that employees have an erroneous picture of their own security knowledge and awareness. These findings might indicate a lack of risk awareness among employees and are supported by the IT security manager who said that an issue revealed through rehearsals was employees' lack of understanding of risk. As mentioned in section 1.1, vulnerabilities in organizations exist mainly due to lack of employees' understanding of risk. This finding is therefore worth noting. We believe that by raising employees' awareness, certain vulnerabilities and incidents can be mitigated.

The ISO/IEC 27035 standard and the NorSIS guideline recommend to conduct rehearsals. Organization A complies with this recommendation. One observation is that Organization A's rehearsals include situations where they are aware of their lack of routines. This gives the team an opportunity to train on improvising in situations where there are no predefined plans. We believe that routines developed through such a bottom-up ap-

proach might be better established within the team than routines imposed
by others, due to the team's participation in the development and imple-
mentation.

According to the ISO/IEC 27035 standard, employees' awareness and par-
ticipation in incident management procedures are important. The employee
survey indicates that employees are positive to awareness campaigns and
have found previous campaigns useful. The positive attitude towards learn-
ing more about information security, might indicate that it is a lack of
management commitment that is the reason for insufficient understanding
and awareness of information security and not employees' attitudes. If that
is the case, it would be unfortunate as senior management commitment to
incident management is highlighted as important in the ISO/IEC 27035
standard. Another indication of a lack of management commitment to in-
formation security in Organization A is that the IT security manager is
often not allocated the resources needed to ensure that the root causes of
incidents are identified and eradicated.

Organization A is compliant with the ISO/IEC 27035 standard's recom-
mendation of having escalation procedures. The standard also specifies
that it should be a main activity for the IRT to allocate responsibilities.
Organization A allocates responsibilities by delegating parts of the incident
handling to employees with expertise relevant for solving the incident.

Organization A's lessons learned phase is relatively compliant with the rec-
ommendations in the majority of the standards and guidelines. They per-
form reviews of severe incidents to identify root causes and improvements.
Further, these improvements are implemented and in specific cases shared
with trusted communities and partners. The latter is specifically recom-
mended in the ISO/IEC 27035 standard. We believe mutual sharing of
experiences is beneficial for organizations as it will make them better pre-
pared for handling incidents. Other organizations may have experienced
incidents that can be avoided if the appropriate security measures are im-
plemented.

The research questions revisited   Organization A has not implemented
any specific standard or guideline for incident management, but has based
their approach on components from the ISO/IEC 27001 and 27002 stan-
dards as well as the ITIL framework. Still, they seem to comply reasonably
well with recommendations in most of the standards and guidelines pre-
sented in this report. They have developed several plans and procedures

addressing information security and incident management specifically, but
not all of these seem to be well *established* throughout the organization. Ad-
ditionally, they do not always have the staff required to respond efficiently
to incidents. Nevertheless, the overall impression is that incidents generally
seem to be handled in accordance with their predetermined plans.

6.2   Case B

Organization B has developed an information security policy, with inten-
tion to define senior management's IT security position. This might indi-
cate some level of management commitment. Having a security policy is
stated to be important by SANS and ITIL. Further, the ITIL framework
recommends that employees should have access to and be aware of the in-
formation security policy. Organization B seems to be compliant with this
recommendation as most employees answered that they were to some extent
familiar with the organization's information security policy.

The interviewees that participated in case B provided slightly different def-
initions of an information security incident. One variation in their defini-
tions was that the interviewees from Organization B specified a distinction
between *security breaches*, i.e. incidents caused intentionally by employees,
and other incidents. The interviewees from the suppliers did not specify
this distinction. This makes sense as the two external suppliers are mainly
concerned with affected systems, whereas it is the organization itself that
handles incidents caused intentionally by employees. They all agreed that
incidents causing loss of sensitive information are the worst possible inci-
dents Organization B can experience. This common understanding might
indicate that they have the same priorities during incident handling.

Even though not all employees knew what an information security inci-
dent is or could provide a definition, most of them gave relevant examples.
This might indicate a reasonably sound understanding of information se-
curity. However, most employees stated to be attentive to incidents, even
though they also said they did not know what an incident is. This shows
that there is still room for improvement of employees' information security
understanding and awareness.

Organization B and its suppliers have implemented various measures to
prevent the occurrence of incidents. Prevention of incidents is stated to be

fundamental to the success of an organization's incident response by NIST SP 800-61. Supplier 1 keeps track of trends related to security incidents, by monitoring their internal systems. This is compliant with recommendations for the preparation phase in the ISO/IEC 27035 standard.

Organization B's development of communication and escalation procedures is compliant with recommendations from SANS, NorSIS and ISO/IEC. In NorSIS's guideline for incident management it is emphasized that information security should be considered when SLAs are developed for outsourcing. Supplier 2's incident management plan is developed to ensure fulfilment of the SLA, and this complies with the recommendation in NorSIS's guideline.

Allocating resources for the development of detailed plans is not Organization B's main focus, as they believe having experienced incident handlers are more important for a successful incident handling. This is an interesting observation as standards and guidelines tend to focus more on plans and procedures than experienced incident handlers. This might indicate that Organization B has evaluated their own needs and perform their incident management accordingly. Further, Organization B performs regular rehearsal to test their plans and gain experience. This is compliant with the ISO/IEC 27035 standard and NorSIS's guideline.

The supply chain manager highlighted information dissemination as one of the most challenging parts of incident management. A challenge mentioned by the interviewee from Supplier 2 was handling and collecting information from various sources. Organization B is well aware of these challenges and focuses on them in rehearsals. We believe making wrong decisions about information dissemination could cause delays in the incident handling and may result in serious consequences. The finding that information dissemination is challenging, supports the findings from a case study conducted by Ahmad et al. [40]. That case study's participants meant that better information dissemination would improve their security procedures, which in turn would improve the overall security of their organization.

Both the supply chain manager and the interviewee from Supplier 2 highlighted allocation of responsibilities as a challenge in incident management. Some incidents may be so complex that knowing exactly where they originated, and thus determining who is responsible for handling them is difficult. We believe the challenge of determining who is responsible in various cases could be mitigated by improving communication procedures and es-

tablishing well defined responsibilities beforehand.

Organization B conducts awareness campaigns that address various topics. Two employees stated that these campaigns were useless as the proposed security measures were too strict. These statements emphasize the importance of having an appropriate balance between security and usability. This was also discussed in one of the presentations at the "Sikkerhet & Sårbarhet 2013" conference:

> *"Security must **never** stop business."*
>
> – John Arild Amdahl Johansen, Buypass AS

In this presentation it was stated that if security measures are too complex, users will find ways to circumvent the rules and thus the initial security measures are compromised. The two employees who did not find the campaigns useful have IT backgrounds which might indicate that employees' impressions of such campaigns vary with individual background and IT knowledge. Even though these two employees were familiar with the content of the campaigns, their answers indicated a negative attitude towards awareness raising activities, and might imply an unsatisfactory security culture in Organization B. However, it should be noted that most employees in the survey found awareness campaigns useful.

Organization B uses monitoring systems and employees as sources of incident detection, which is in accordance with recommendations from most of the standards and guidelines presented in section 3.2. The employee survey indicated that the knowledge of reporting procedures for employees is not satisfactory, as most of the employees were not sure where to report incidents. Their overall uncertainty related to reporting may indicate that reporting procedures are not well enough established throughout the organization. Additionally, a few stated that they were not familiar with reporting routines as they had never needed to report anything. This attitude is similar to the one found in case A where some employees believed that information security did not concern them.

Organization B uses a predefined classification scale based on impact level for the categorization of incidents. This is compliant with the ISO/IEC 27035 standard and ENISA's Good Practice Guideline for Incident Management. The categorization is further used to prioritize incidents. Incident prioritization based on impact level is recommended by ISO/IEC, SANS, NorSIS and ITIL.

All incidents are logged and the root causes of incidents are included in the log. Most of the standards and guidelines discussed in section 3.2 specify logging as being important. Further, the ITIL framework focuses on root cause analysis in the problem management process.

Organization B holds regular meetings where they discuss serious incidents and they perform trend analyses by evaluating incident reports. These activities are described as essential in the ISO/IEC 27035 standard. Overall, the organization's post-incident activities seem to be in accordance with relevant standards and guidelines. The organization has routines for preservation of electronic evidence, which is compliant with the ISO/IEC 27002 standard.

As described in the standards and guidelines, recovery is an important part of incident response. Organization B has tried to ensure a high level of redundancy, which we believe makes recovery easier and more efficient. Additionally, it might limit availability related consequences of security incidents.

Werlinger et al. recommended incident handlers to acquire knowledge about the organization's IT systems and services in order to better be able to recognize abnormal behaviour [37]. Organization B may have difficulties utilizing tacit knowledge as incident handling is to a large degree outsourced. However, we believe that the incident handlers at Supplier 1 and Supplier 2 may have gained such knowledge, as they handle Organization B's daily IT operations and application management respectively.

The research questions revisited   Organization B has not strictly based plans and procedures on standards or guidelines for incident management. Still, they are relatively compliant with the standards and guidelines presented in section 3.2. Some of their procedures seem to be well established such as their escalation procedures. They do, however, have some procedures that do not seem to be sufficiently established. It seems that reporting procedures are not sufficiently established in the organization as employees showed uncertainty related to these procedures. Organization B has a set of predefined plans, but the importance of having experienced incident handlers is extra evident in this case as their incident handling is distributed and their team scalable. Their plans are quite general and they thus focus on being able to improvise during incident handling, i.e. make situation-specific decisions. Our overall impression is that incident handling has been performed in accordance with predefined plans.

6.3 Case C

Organization C has an information security policy which is reasonably well known among participants in the employee survey. In one of the presentations at the "Sikkerhet & Sårbarhet 2013" conference, Difi[1] recommended discussing security during employee appraisals. The IT security manager said that their security handbook is always a topic in the annual employee appraisals. Further, most of the employees in the survey seemed to have an understanding of what an information security incident is. This could indicate that information security is well understood among employees in Organization C. There are several findings that could explain this. It can be assumed that the annual review of the security handbook aids employees in becoming aware of their individual security responsibilities. Further, Organization C believes it is important to have a security-positive environment. The organization's focus on employees may have increased the overall security understanding. We believe an important factor contributing to this is that Organization C's core activity is delivery of IT services. Consequently, they have a high focus on information security.

ISO/IEC, SANS and NorSIS emphasize the importance of management commitment both to incident management and information security in general. We believe Organization C has some extent of management commitment as the aim of their information security policy is to communicate the management's direction and commitment to information security. One reason for this commitment might be that they have several ISO/IEC 27001 certifications, and this standard states that management shall provide evidence of its commitment to information security.

The fact that all of the employees had attended courses or other awareness raising activities, supports Organization C's claim of having a high focus on improving employees' security knowledge and awareness. This observation is further supported by statements from the IT security manager, and may confirm that the organization follows through on their policy objectives. Additionally, employees' attitude towards awareness raising activities shows signs of a security-positive environment.

The employee survey showed some uncertainty with regard to reporting procedures. The few employees that did not know where to report claimed to know where to find relevant information. Employees' knowledge of where

---

[1]The Norwegian Agency for Public Management and eGovernment

to find relevant information is positive, but we believe this is not efficient enough in all situations as it introduces an extra delay. The IT security manager said that employees are advised to report incidents to the IRT. However, none of the employees mentioned this. Suspicious e-mails was given as one example of cases that should be reported. Still, none of the employees had previously reported such e-mails. The fact that none of the participants in the survey had reported incidents could indicate that employees are not fully utilized as part of the organization's sensor network for detecting incidents. This assumption is supported by one of the employees who stated that they should probably report incidents more often. Further, this is supported by the IT security manager who suspects underreporting. This is unfortunate as Organization C tries to establish a security-positive environment. Underreporting might indicate that they still have some work to do with regard to achieving this.

Organization C has monitoring systems for incident detection. This is in compliance with recommendations from ISO/IEC, NIST and ENISA.

Handling vulnerabilities can aid in incident prevention, which is an important part of incident management and is stated to be a fundamental factor by NIST. Additionally, NorSIS specifies preventive measures to be one of the most cost effective ways to perform incident management. Organization C has a risk framework where vulnerabilities can be reported and measures can be implemented thereafter. They are thus in compliance with recommendations.

Organization C bases their incident categorization on impact level, which is in accordance with the categorization method from the ITIL framework. The categorization determines which incident response procedures to initiate. Categorizing incidents and using the categorization to determine further actions are compliant with recommendations from the majority of the standards and guidelines discussed in section 3.2.

As illustrated in figure 5.5 in chapter 5, the service desk function is the first line of incident response. This figure, in combination with figure 5.6 show Organization C's escalation routines. We believe this shows mature and well established escalation routines in Organization C, that are compliant with recommendations from the ITIL framework.

It is stated in Organization C's internal documentation that they believe successful incident management is based on contingency plans and predefined tasks. The employee we had e-mail correspondence with acknowledged

that it would be ideal to have plans and procedures for all possible incidents, but that this might not be practically feasible. He emphasized that incident handlers who compose a set of predefined activities to customize the incident response for specific incidents are key to successful incident handling. He stated that due to variations in incidents, an experienced incident handler is more important than rigid process adherence. We believe that thorough preparation for incident handling is of utmost importance. However, incident handlers that are capable of having situational awareness are essential to utilize these preparations to the fullest.

Organization C has developed procedures for handling electronic evidence. The establishment of routines for handling electronic evidence is compliant with NIST SP 800-61 and the ISO/IEC 27002 standard.

Two requirements for Organization C's incident management process are that all incidents should be registered and all actions logged. It is fair to say that the organization follows best practice, as most of the standards and guidelines discussed in section 3.2 emphasize the importance of logging.

The fact that Organization C has initiated a project to improve their incident management scheme shows their commitment to improve their incident management process. This project is allocated extensive resources which again supports the assumption of established management commitment to information security and incident management.

Incident handling is distributed among Organization C and its customers. Hence, the challenges of collaboration and coordination are evident in this case. Communication emerges as a challenge, which has been revealed through rehearsals. We believe the establishment of more specific communication routines as well as well defined responsibilities might mitigate these challenges.

The research questions revisited We believe Organization C has a set of well established plans and procedures as well as a focus on having experienced incident handlers. Additionally, they have several ISO/IEC 27001 certifications and has implemented the ITIL framework for their IT service management. Their incident management is highly compliant with the ITIL framework as well as relatively compliant with the other standards and guidelines presented in section 3.2. It seems that incidents have mostly been handled in accordance with predefined plans. The uncertainty among employees with regard to reporting routines might indicate that

these routines are not sufficiently established throughout the organization. Nevertheless, our findings indicate that this organization has an overall mature incident management process.

6.4   Prominent Challenges and Observations

This section discusses challenges and observations that we found prominent in our case study. There are several factors involved in determining how successfully organizations respond to information security incidents. In chapter 1 we stated that we wanted to assess how these factors contribute to the efficiency and effectiveness of organizations' incident management. The challenges discussed in this section are some of the factors that are part of determining the level of success in organizations' incident management processes. It is important to note that our findings cannot be directly generalized. Due to the organizations' size and core activities they are extra vulnerable to attacks and we therefore have assumed that they are experienced in incident handling. Hence, we find it reasonable to believe that some of these challenges and observations will be evident in other organizations as well.

6.4.1   Communication

During our case study we found that communication was regarded as challenging among all of the participants. Both internal communication, within teams and towards employees, and external communication are part of this communication challenge. The organizations had to various extents developed and implemented plans and procedures addressing communication. Successful incident response requires cooperation, thus establishing sound communication procedures for incident management is essential. Communication is further emphasized as one of the most important parts of incident management by NIST. The organizations we studied are large organizations and it is therefore not surprising that several parties are involved in their incident management. Even for Organization A, that does not have to coordinate with external parties during incident handling, incident handlers have to communicate and coordinate across several internal departments and sections. As an example from our study we highlight that the designated contact person in Organization A changes daily for some sections

which imposed uncertainty for the IT security manager.

Communication becomes even more challenging with distributed organizational structures and the establishment of sound communication procedures is vital. Our impression is that it is important to have available and updated contact lists, but being able to determine the correct person to contact during incident response is just as important. In some cases, people with special knowledge or authorizations need to be involved. To be able to determine who the correct person is, situations have to be assessed and tacit knowledge about the organization and its employees is essential. This type of knowledge is difficult to document and thus difficult to include in plans. We therefore believe that in order to mitigate communication related challenges, employees involved in incident handling must have experience.

A speaker at the "Sikkerhet & Sårbarhet 2013" conference presented results from an audit performed by The Norwegian Data Protection Authority that highlighted a problem we also found evident in our case study. E-mail is still used for unstructured and informal communication, even though it is not a secure channel. Using insecure communication channels exposes the organization to targeted phishing attacks, e.g. as seen in a recent attack against the large Norwegian telecom corporation Telenor [43]. The organizations in our case study used e-mail for communication not only as a first notification of incidents but also during major incidents. To mitigate the risk of phishing attacks and disclosure of sensitive information, we recommend using more secure communication channels where this is practically feasible.

6.4.2   Information Collection and Dissemination

Collecting information relevant to incident management was pointed out as challenging by participants in our case study. Especially for organizations with distributed organizational structures, there are many sources of information which makes the collection of correct information difficult. This observation supports findings from a case study conducted by Ahmad et al. [40] where an information security manager stated that the sharing or rather the finding of information was one of the most challenging parts of her job.

Several of the participants in our study pointed out information dissemina-

tion as a challenge in incident handling. Knowing how much information to share can be difficult. Too little information could give an erroneous picture of the incident which could in turn lead to wrong decisions being made. On the other hand, too much information can be overwhelming and can cause delays in decision making as information has to be structured in order to be useful. It is important to communicate the *right* information to the *right* people. Information about incidents can obviously be sensitive and communicating such information to people who are not supposed to receive it can have serious consequences. Additionally, providing unnecessary information can be an annoyance and could at worst be counterproductive.

One employee mentioned that they have often not been notified about changes made in the security policy, which is an example of poor information dissemination. However, we believe that employees' knowledge of details in the policy is not essential to a successful incident management as long as they are familiar with relevant procedures and are capable of performing necessary actions. Providing information to employees is important, although this information should be relevant and useful.

We believe the development and establishment of clear information dissemination procedures, that can for instance be based on incident categories, could improve information dissemination in organizations. If procedures for each predefined incident category exist and are established, it will be easier and more efficient to determine what information to share and with whom.

6.4.3   Experience

To be able to customize responses to specific incidents, experience is essential. This was highlighted by several of the participants in our study. Developing detailed plans for all possible scenarios is not feasible and probably not useful, even though well established plans and procedures for incident handling is obviously important. Several of the participants in our study highlighted that there could always occur incidents that no one thought of beforehand. Hence, we believe allocating resources to the development of detailed plans for all potential incidents is unproductive as this is not possible.

We believe having experienced incident handlers is key for making rapid and correct decisions in a complex and dynamic environment. One obvious way

to gain experience is by handling real incidents. However, organizations cannot wait for incidents to occur to gain experience, and thus rehearsals is a necessity. By conducting rehearsals addressing various types of incidents, plans and procedures can be tested and incident handlers will gain experience at the same time.

In our opinion, neither experience nor rehearsals are sufficiently highlighted in the standards and guidelines considering how important this is for incident management. The organizations in our study focus on these two factors in their incident management. However, we believe they could benefit from conducting rehearsals more often.

Our impression is that having competent and experienced incident handlers that are both familiar with existing procedures and are capable of handling unexpected scenarios is essential to a successful incident management.

6.4.4 Responsibility Allocation

It can be challenging to know exactly where an incident originated. Hence, knowing what to do and who is responsible for handling the incident is difficult. One of the interviewees said that the greatest challenge with incident handling is cases where no one understands that they "own" the incident and thus no one takes responsibility. This ambiguity of who owns an incident can be due to uncertainty of where it originated. This challenge was also mentioned by another of the interviewees who stated that minor incidents can escalate and have serious consequences if no one takes responsibility. Further, ambiguous responsibilities in combination with costs of handling an incident might lead to a delay in the incident response if no one claims ownership and takes responsibility.

Even though developing detailed plans for all possible scenarios is not feasible, we still believe that having an appropriate detail level in plans addressing *responsibilities* could be beneficial. As it in some situations is difficult to determine who owns an incident, our best recommendation is to improve communication to better be able to determine ownership and responsibilities in situations where this cannot be determined based on a predefined plan.

We believe that rehearsals can contribute to revealing grey areas regarding responsibilities. Additionally, rehearsals can make incident handlers more

suited to determine where incidents originated. As organization's incident management procedures mature, the organizations become better equipped to determine responsibilities. The supply chain manager in Organization B emphasized that after years of working closely together, their experience and tacit knowledge help them determine who is responsible for handling an incident without specific responsibilities being determined or documented beforehand.

The challenge of determining responsibilities is extra evident in case B, as several suppliers are involved in their incident management. In this specific case, the two suppliers have separate main responsibilities. However, we assume that grey areas may emerge with regard to responsibilities even for this case if new or unexpected incidents occur. NorSIS' guideline emphasizes that responsibilities should be determined in an SLA when (parts of) incident management is outsourced. The standards and guidelines presented in section 3.2 do not provide specific recommendations for resolving ambiguities with regard to incident ownership and thus responsibilities for specific incidents. We recommend organizations to comply with the NorSIS Guideline for Incident Management, i.e. to determine responsibilities in the SLA.

6.4.5   Employee Involvement

When we contacted people for the employee survey we observed an interesting attitude among employees. Several employees seemed reluctant to participate due to their perception of their own lack of knowledge about information security. This was evident in comments such as:

> "I don't know if I can help, I don't know anything about information security."

We suspect that some of the reluctance was due to employees being scared that the survey would "reveal" their insufficient knowledge about information security. They seemed somewhat embarrassed about this insufficient knowledge and several said that they should probably have been more familiar with the organization's information security policy. There were however, some employees that admitted lack of knowledge and "excused" this by saying that information security did not concern them. We find this very alarming as information security concerns **everyone** and as attacks taking advantage of employees, such as targeted malicious e-mails, is an

increasing trend. As the example provided by the IT security manager in case A shows, regular employees' accounts can be hacked and used to send phishing e-mails. This highlights that employees do not necessarily need to have direct access to sensitive information to be exposed to attacks.

Findings from Organization A showed that their information classification is not satisfactory. Employees seem to fail in recognizing that the value and sensitivity of the information they process should determine how information should be secured and handled. Failing to classify information can lead to the information not being sufficiently secured according to its value. This could lead to a gap between the sensitivity and value of information and implemented security measures, something that was also highlighted in a recent survey [9].

Employees in our survey seem to have an overall positive attitude towards awareness campaigns. Many of them stated that they wished such campaigns would be conducted more often. We can imagine that, as long as the campaigns are not too extensive, this attitude is consistent throughout organizations. Due to this positivity we also believe that employees can benefit from being more involved in rehearsals. Our findings did not show any employee involvement in rehearsals beyond the involvement of incident and crisis handlers. We believe that if employees are trained in reporting procedures and incident detection they can be utilized as part of the sensor network in a larger degree than they seem to be today.

6.5 Recommendations

This section presents our recommendations for performing a successful incident management. These are based on both challenges and successful practices found evident in the organizations studied. We believe these recommendations can be useful for various types of organizations.

1. Use well established standards or guidelines as a basis for incident management, as these are based on years of experience.

2. Perform rehearsals to gain experience, as experience has shown to be just as important as having established plans.

   a) Perform rehearsals both for large and small incidents. Remember that a small incident that is not sufficiently handled could escalate

and lead to more serious consequences than necessary. Additionally, both small and large incidents can be valuable for learning.

b) Focus on challenging areas such as information dissemination, communication and allocation of responsibilities in rehearsals.

c) Perform rehearsals for regular employees, in addition to incident handlers, as all employees have an information security responsibility. Recommended topics for such rehearsals are information classification, incident detection (such as malicious e-mails) and reporting procedures.

3. Share experiences with trusted parties and communities to become better prepared to handle incidents in the future. This way organizations can utilize other organizations' experiences in addition to their own.

4. Develop clear and sound plans for communication.

5. Focus on establishing a security-positive organizational culture, where employees do not hesitate to report security events.

6. Utilize employees as part of the sensor network. Make sure that developed reporting routines are actually *established*.

7. Conduct awareness campaigns with a reasonable regularity, each being of a reasonable length.

a) Send awareness campaigns by e-mail to make them easily accessible. A tip is to send them such that they are in the employees' inboxes when they arrive at work in the morning. We believe that people are extra susceptible to campaigns at that time, as they have not started other activities yet and will thus not be disturbed.

b) Focus on making sure that employees are aware that information security *does* concern them, such that they can get familiar with their responsibilities.

c) Make employees aware of security limitations in the systems they use, such that sensitive information is not unnecessary exposed. Provide examples of how information can be lost or compromised.

d) Focus on improving employees' assessment of the value and sensitivity of information they process such that appropriate security

measures can be implemented to make sure that the information they process is properly secured.

e) Focus on making sure employees are attentive to malicious targeted e-mails as well as teaching them to recognize such e-mails.

f) Use incidents caused by employees or incidents that were/could have been detected by employees, as examples in awareness-raising activities. Incidents experienced by others can also be used as examples. Further, we recommend using incidents discussed in the media as many employees will be familiar with these.

g) If the organization does not have the resources to create awareness campaigns themselves, it is possible to buy these from external providers, as successfully done by Organization A and B.

Table 6.5 shows the relationship between the challenges we observed and our recommended measures for mitigating these challenges. Our first recommendation involves using well established standards for incident management. As can be seen in the table, we have only listed recommendation 1 as a secondary measure to one of the observed challenges. This might indicate that the standards and guidelines do not focus sufficiently on these challenging factors. We believe there might be a connection between the challenges in organizations' incident management and that the standards and guidelines do not focus on these areas. Hence, basing incident management on standards alone are not satisfactory.

Challenges	Main measures	Secondary measures
Communication	2b, 3	1
Information	2b	5
Experience	2	4, 5, 6
Responsibility	2, 6b	6c, 6d
Employee Involvement	2c, 4, 5, 6	

Table 6.1: Links Between Observed Challenges and Proposed Measures

Chapter 7

Conclusion and Future Work

In our thesis we have studied how three large organizations perform information security incident management in practice. We have examined what plans and procedures they have developed and how well these are established. Additionally, we have examined to what extent existing standards and guidelines are adopted in the organizations' plans and whether their practices comply with the standards and guidelines we studied.

We found that the organizations have plans and procedures that are to some extent compliant with standards and guidelines. However, some of these procedures were not well established throughout the organizations. We highlight reporting procedures in particular, as procedures that were not sufficiently established. In addition to finding answers to our research questions, other findings emerged as we analysed the data. One observation was that the organizations found an experienced incident handler just as important for incident response as having detailed plans. Despite the organizations in our study being large and experienced in incident handling, some challenges were prominent in all of the cases. These challenges were related to communication, information collection and dissemination, employee involvement and allocation of responsibilities.

By evaluating the challenges we developed a set of recommendations for improving incident management practices. We recommend using standards and guidelines as a basis for incident management. Further, conducting

regular rehearsals to gain experience is essential. The development of clear and sound plans for communication could also improve current practice. We saw that employees could be better utilized as part of organizations' sensor networks and thus we emphasize the importance of making sure reporting procedures are well established. Additionally, conducting awareness campaigns has proven to be useful.

We hope that by conducting this research and providing these recommendations, we can contribute to organizations becoming better prepared to respond to information security incidents in the future.

We believe it is valuable to continue the research on incident management as recent reports and surveys have indicated that threats are changing and increasing. It would be interesting to implement our recommendations in the studied organizations and perhaps other organizations as well, to see whether they can have a positive effect on incident management. As we have only studied a limited number of organizations, our results are not generalizable and thus it would be interesting to conduct the same study with a larger number of organizations. This can verify whether our findings apply to organizations in general. Such a study can reveal more challenges and thus lead to more recommendations. It can further be supplemented by a quantitative study, to see whether these challenges are evident in the majority of organizations. By including a large number of organizations, one can compare industries as well. This can lead to both general and industry specific recommendations.

Bibliography

[1] Taktisk Etterforskningsavdeling, Kripos. Den Organiserte Kriminaliteten i Norge - Trender og Utfordringer 2013-2014. (In Norwegian).

[2] ISO/IEC 27035:2011(E). Information technology - Security techniques - Information security incident management - First edition. International Organization for Standardization, 2011.

[3] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. NIST Special Publication 800-61: Computer Security Incident Handling Guide, 2011. Revision 2 (Draft).

[4] About NSM. `https://www.nsm.stat.no/Engelsk-start-side/About-NSM/`. Visited 2013-01-19.

[5] About NorCERT. `https://www.nsm.stat.no/Engelsk-start-side/English2/`. Visited 2013-01-19.

[6] NorCERT. Kvartalsrapport for 3. kvartal 2012. (In Norwegian).

[7] National Police Directorate. The Police in Norway, June 2010.

[8] Nasjonal Sikkerhetsmyndighet (NSM). Rapport om sikkerhetstilstanden 2012, March 2013. (In Norwegian).

[9] Næringslivets Sikkerhetsråd. Mørketallsundersøkelsen 2012 - Informasjonssikkerhet og datakriminalitet, 2012. (In Norwegian).

[10] Nasjonal Sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST), and Etterretningstjenesten (E-tjenesten). Trusler og Sårbarheter 2013 - Samordnet vurdering fra E-tjenesten, NSM og PST, February 2013. (In Norwegian).

[11] Nasjonal Sikkerhetsmyndighet (NSM). Rapport om sikkerhetstilstanden 2011, June 2012. (In Norwegian).

[12] Politiets sikkerhetstjeneste (PST). Årlig trusselvurdering 2013, February 2013. (In Norwegian).

[13] NorCERT. Kvartalsrapport for 2. kvartal 2012. (In Norwegian).

[14] Norwegian Police Security Service (PST). Annual threat assessment 2012, February 2012.

[15] Nasjonal Sikkerhetsmyndighet (NSM). Grunnsikring - Årsmelding 2011. (In Norwegian).

[16] Verizon RISK Team. 2012 Data Breach Investigations Report, 2012.

[17] Robert K. Yin. *Case Study Research Design and Methods*, volume 5 of *Applied Social Research Method Series*. SAGE Publications, fourth edition, 2009.

[18] Anol Bhattacherjee. Social Science Research: Principles, Methods, and Practices. 2012.

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

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

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

[22] David R Thomas. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2):237–246, 2006.

[23] Sally Thorne. Data analysis in qualitative research. *Evidence Based Nursing*, 3(3):68–70, 2000.

[24] Lars Arne Sand, Gaute Bjørklund Wangen, and Anders Sand Frogner. Hendelseshåndtering i små og mellomstore bedrifter. Gjøvik Univeristy College, 2010. (In Norwegian).

[25] Allen S. Lee. A Scientific Methodology for MIS Case Studies. *MIS quarterly*, pages 33–50, 1989.

[26] ISO/IEC 27000:2012(E). Information technology - Security techniques - Information security management systems - Overview and vocabulary - Second edition. International Organization for Standardization, 2012.

[27] European Network and Information Security Agency (ENISA). Good Practice Guide for Incident Management, 2010.

[28] European Network and Information Security Agency (ENISA). A basic collection of good practices for running a CSIRT, 2008.

[29] ISO/IEC 27001:2005(E). Information technology - Security techniques - Information security management systems - Requirements - First edition. International Organization for Standardization, 2005.

[30] ISO/IEC 27002:2005(E). Information technology - Security techniques - Code of practice for information security management - First edition. International Organization for Standardization, 2005.

[31] Ernest Brewster, Richard Griffiths, Aidan Lawes, and John Sansbury. *IT Service Management: A Guide for Itil Foundation Exam Candidates.* BCS, The Chartered Institute for IT, second edition, 2012.

[32] NorSIS. Veiledning i hendelseshåndtering, 2010. (In Norwegian).

[33] Patrick Kral. Incident Handler's Handbook. SANS Institute Information Security Reading Room, December 2011.

[34] Eugene H. Spafford. A Failure to Learn from the Past. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pages 217–231. IEEE, 2003.

[35] Tore Larsen Orderløkken. Security Incident handling and reporting – a study of the difference between theory and practice. Gjøvik Univeristy College, 2005.

[36] Rodrigo Werlinger, David Botta, and Konstantin Beznosov. Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 149–150. ACM, 2007.

[37] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 18(1):26–42, 2010.

[38] Maria B. Line. Identifying Current Practice for Information Security Incident Management in the Power Industry. Norwegian University of Science and Technology (NTNU), 2013.

[39] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. State of the Practice of Computer Security Incident Response Teams (CSIRTs). Technical report, DTIC Document, 2003.

[40] Atif Ahmad, Justin Hadgkiss, and AB Ruighaver. Incident response teams–Challenges in supporting the organisational security function. *Computers & Security*, 2012.

[41] Jose J Gonzalez, Klaus-Peter Kossakowski, and Johannes Wiik. Limits to Effectiveness in Computer Security Incident Response Teams. Boston, Massachusetts: Twenty Third International Conference of the System Dynamics Society.

[42] Finansdepartementet. SMB-definisjoner. `http://www.regjeringen.no/nb/dep/fin/dok/nouer/1995/nou-1995-16/5/2/1.html?id=336716`. Visited 2013-04-05. (In Norwegian).

[43] Snorre Fagerland, Morten Kråkvik, Ned Moran, and Jonathan Camp. Operation Hangover: Unveiling an Indian Cyberattack Infrastructure. Norman Shark AS, May 2013.

Appendix A - Information Sheet

Forespørsel om å delta i intervju i forbindelse med en masteroppgave

Vi er to masterstudenter i kommunikasjonsteknologi med fordypning informasjonssikkerhet ved Norges Teknisk og Naturvitenskapelige Universitet (NTNU) og vi holder på å skrive masteroppgaven vår. Temaet for oppgaven er håndtering av sikkerhetsbrudd og vil omfatte planlegging i tillegg til håndtering av faktiske hendelser. Vi ønsker å finne ut av hvilke planer virksomheter har når det gjelder sikkerhetsbrudd i tillegg til hvordan disse planene har blitt utført i praksis.

Vi ønsker å foreta intervjuer ansikt-til-ansikt med en eller flere personer fra ulike virksomheter for å kunne svare på dette. Spørsmålene vi ønsker å stille handler om hvilke planer som finnes, hvilke standarder som følges, hvordan planene brukes i praksis og til hvilken grad dette har fungert som man har ønsket.

Vi planlegger å bruke båndopptaker under intervjuene. Intervjuene kommer til å bli gjennomført i full fortrolighet og opptakene og eventuelle notater kommer til å bli oppbevart og behandlet konfidensielt på NTNU.

Intervjuene kommer til å bli foretatt av oss og noen deler kan bli diskutert med vår veileder Maria B. Line, stipendiat ved NTNU og forsker ved SINTEF og ansvarlig professor Karin Bernsmed, førsteemanuesis II ved NTNU og forsker ved SINTEF.

Resultatene fra intervjuene kommer til å bli en del av en rapport som leveres på NTNU. Ingen enkeltpersoner eller enkeltvirksomheter vil kunne identifiseres i denne rapporten. Ved prosjektets slutt, 17.06.2013, vil alle lydopptak bli slettet og øvrig datamateriale vil bli anonymisert. Det vil si at eventuelle direkte personidentifiserende opplysninger slettes og eventuelle indirekte personidentifiserende opplysninger fjernes eller slettes.

Det er frivillig å være med og du har mulighet til å trekke deg når som helst underveis i prosjektet uten å måtte begrunne dette nærmere. Dersom du velger å trekke deg vil all samlet informasjon bli anonymisert og lydopptak vil slettes.

Dersom du har noen spørsmål er det bare å kontakte oss. Vi håper du ønsker å delta.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelige datatjeneste (NSD).

Med vennlig hilsen
Marte Tårnes og Cathrine Hove
martetar@stud.ntnu.no / cathrhov@stud.ntnu.no
Tlf: 98 47 40 67 / 90 74 60 28

Samtykkeerklæring:

Jeg har mottatt skriftlig informasjon og er villig til å delta i studien.

Dato/Sted: Navn: Signatur:

Appendix B - Interview Guide

Intervjuguide

Håndtering av IKT-sikkerhetsbrudd

Cathrine Hove, Marte Tårnes

Vi skal kartlegge hvordan IKT-sikkerhetsbrudd håndteres i virksomheter. Vi ønsker å finne ut hva slags planer som eksisterer, i hvilken grad disse planene er basert på standarder, i hvilken grad de blir fulgt i praksis og om det har fungert bra. Datainnsamlingen vil, i tillegg til en bakgrunsstudie om hendelseshåndtering, danne grunnlaget for en masteroppgave.

Intervjuene vil bli gjennomført ansikt til ansikt i full fortrolighet og alle svar anonymiseres. Resultatene vil ikke kunne spores til enkeltindivider eller enkeltvirksomheter.

Innledning

Hvem vi er:

Masterstudenter i kommunikasjonsteknologi med fordypning informasjonssikkerhet.

Kontekst:

Masteroppgave

Forskningsspørsmål:

- Hvordan utfører virksomheter hendelseshåndtering i praksis?

Med underspørsmålene:

- Hvilke planer og prosedyrer for hendelseshåndtering er etablert i virksomheter?
- Til hvilken grad blir eksisterende standarder/retningslinjer brukt i planer for hendelseshåndtering?
- Hvordan har tidligere hendelser blitt håndtert i henhold til forhåndsbestemte planer?

Meldeplikt:

Vi kommer til å bruke båndopptaker og derfor er studien meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelige datatjeneste (NSD). Informasjon til intervjuobjektene finnes i eget informasjonsskriv sammen med en samtykkeerklæring.

Formalia:

Tidsramme: mellom en og to timer

Vi bruker båndopptaker.

Vi har en intervjuguide som følges løst og vi ønsker å få til en samtale rundt temaet.

Spørsmål

Spørsmålene er nummererte med potensielle underspørsmål. Hva slags spørsmål som faktisk stilles kan variere etter f.eks. hvilken rolle intervjuobjektet/intervjuobjektene har i virksomheten og hva slags type virksomhet det er (f.eks. om de drifter systemer for andre).

Innledende:

1. Hvor mange ansatte er dere i virksomheten?
2. Hva slags type organisasjon er dette/hva er kjernevirksomheten deres?
3. Hva er din/deres rolle i virksomheten?
   a. Hvor lenge har du hatt denne rollen?
4. Hvordan er IT-driften deres organisert?

Generelt:

5. Hvordan definerer du et IKT-sikkerhetsbrudd?
   a. Er denne definisjonen noe som virksomheten har utviklet og som er kjent blant ansatte?
6. Hva er det verst tenkelige sikkerhetsbruddet dere kan oppleve?
   a. Hva slags konsekvenser kan et eventuelt slikt brudd få?
7. Har dere en oversikt over tidligere sikkerhetsbrudd?
8. Har dere en sikkerhetspolicy?
9. Har dere en egen policy for hendelses-/sårbarhetshåndtering?

Incident Response Team:

10. Har dere noe dedikert team for hendelseshåndtering (CIRT/CSIRT/ISIRT/IRT)?
    a. Hvordan er teamet organisert?
        i. Hvem er med?
        ii. Hvordan ble de valgt?
        iii. Er teamet internt eller helt/delvis outsourced?
        iv. Er teamet sentralt eller distribuert?
        v. Jobber medlemmene heltid eller deltid i teamet?
        vi. Hvordan er tilgjengeligheten på medlemmene?
        vii. Hvordan er roller og ansvar i teamet organisert?
    b. Inngår forebyggende arbeid som en del av teamets oppgaver, dvs. sikring av nettverk, systemer osv.?
        i. Holdningsskapende arbeid?
        ii. Har de andre oppgaver?
    c. Hvordan er samarbeidet/kommunikasjonen mellom teamet og
        i. Ledelsen?
        ii. CISO/CIO og IT-sjef?
        iii. Kriseteam?
        iv. Andre team?
    d. Hvilken opplæring har teamet gjennomgått?

          i.   Ekstern?

         ii.   Intern?

       iii.   Får de kontinuerlig opplæring?

11. Hvilken nytte kan dere se/har dere sett av å ha et slikt team?

Planlegging/forberedelse:

12. Finnes det en *helhetlig* (altomfattende) plan for håndtering av sikkerhetsbrudd?
    a. Brukes den i praksis?
    b. Er denne koordinert med eventuelle kunder som dere drifter systemene for?
13. Hvilke planer for kommunikasjon eksisterer?
    a. Hvem skal/kan kontaktes i ulike tilfeller?
    b. Hvordan håndteres kontakt med "outsiders" (media, politi, operatører osv.)?
14. Har dere en spesifisert work flow for hendelseshåndteringsprosessen?
    a. Hvordan er den utarbeidet og vedlikeholdt?
    c. Hvordan blir den kommunisert til medlemmene i hendelseshåndteringsteamet?
    d. Hvordan har denne fungert i praksis/har den blitt fulgt?

Standarder:

15. Følger dere ISO/IEC 27001/27002?
    a. Er dere sertifisert?
    b. Hvordan oppfyller dere kravene som omhandler hendelseshåndtering? (Gå gjennom standard, steg for steg)
16. Følger dere noen standarder eller guidelines som spesifikt omfatter hendelseshåndtering?
    a. Hvilke?
    b. Bruker dere ISO/IEC 27035 (tidligere ISO/IEC 18044)?
        i. Har dere hørt om den?
    c. Hvordan har dere tilpasset guider til deres organisasjon ut fra standardene?
    d. Hvorfor ikke?
        i. Har dere vurdert det?
17. Når begynte dere å følge standarder?
    a. Hvilken innvirkning har det hatt på hendelseshåndteringen?
18. Brukes en standard/guide for kategorisering av hendelser, basert på
    a. Alvorlighetsgrad?
    b. Type?

Rutiner:

19. Hva slags rutiner har dere for varsling av potensielle sikkerhetsbrudd?
    a. Hvordan blir de ansatte informert om disse rutinene?
    b. Hvilke rutiner for varsling finnes hos kunder dere drifter for?
    c. Kan sårbarheter varsles på samme måte?
    d. Hvordan håndteres konfidensiell informasjon ved varsling om sikkerhetsbrudd?
        i. Blir anonymitet for de som varsler om hendelser ivaretatt?
    e. Hvem mottar varslene og avgjør hva som skal skje videre?
20. Har dere noen form for sjekkliste for bruk ved hendelseshåndtering?
    a. Har dere laget den selv?
        i. Hvis nei, hvor kommer den fra?

21. Hvordan håndterer dere sårbarheter som blir oppdaget (som enda ikke er utnyttet)?
22. Hva slags rutiner har dere for "høynet beredskap" ved hendelser deres eget team ikke har kompetanse til å håndtere eller ressurser til å utføre håndteringen raskt nok?
    a. Utvider dere håndteringsteamet?
    b. Kalles det inn et kriseteam?
        ii. Eksternt?
        iii. Internt?

Hendelseshåndtering:

23. Hvordan blir sikkerhetsbrudd vanligvis oppdaget? (automatisert, sluttbruker?)
24. Har dere noen prosedyrer for håndtering av *kjente* sikkerhetsbrudd eller sårbarheter?
    a. Har dere automatisk håndtering av noen typer sikkerhetsbrudd?
25. Finnes det eksempler på hendelser der rutinene/planene har fungert godt?
    a. Hva ble gjort riktig i disse tilfellene?
    b. Ble det dokumentert og delt med eksterne virksomheter?
26. Finnes det eksempler på hendelser der rutinene/planene har fungert dårlig?
    a. Hvorfor fungerte det dårlig?
    b. Ble det dokumentert og delt med eksterne virksomheter?
27. Hvordan sikres digitale bevis i forbindelse med et sikkerhetsbrudd?
28. Før avgjørelser om hvordan hendelser skal håndteres blir tatt, vurderes omfanget og mulige konsekvenser for kjernevirksomheten?
29. Hva gjøres for å sikre at gjenoppretting av systemer etter hendelser skal gå så raskt som mulig?
    a. Hvordan har dette fungert i praksis?

Dokumentasjon og rapportering:

30. På hvilken måte dokumenterer dere hendelser?
    a. Er dette en kontinuerlig prosess eller gjøres det f.eks. kun etter endt hendelse?
    b. Har/bruker dere noen mal for rapporter?
31. Hva dokumenteres?
    a. Kostnader?
    b. Type?
    c. Omfang?
    d. Aktiviteter foretatt av involverte personer?
    e. Hendelsesforløpet?
32. Hvordan blir hendelser rapportert til ledelsen?
    a. Hvilke hendelser blir rapportert?
    b. Hvem i ledelsen blir det rapportert til?

Øvelser:

33. Utfører dere noen øvelser for å sjekke om planene ser ut til å fungere i praksis?
    a. Kan du forklare litt om hvordan det gjøres?
34. Tilsier erfaring at øvelsene var hensiktsmessige?
35. Har du noen eksempler på forbedringsområder som har blitt avdekket gjennom øvelser?

Etterarbeid/forbedringspotensiale:

36. Hvordan samles erfaringer gjort ved ulike hendelser?
    a. Blir erfaring fra alle typer hendelser dokumentert og distribuert?
    b. Hvis ikke, hvorfor det?
37. Hvilke rutiner finnes for å lære av feil (lessons learned)?
    a. Har dere møter etter endt hendelse?
    b. Har dere regelmessige møter?
    c. Kan dere komme på tilfeller hvor dere har brukt "lessons learned" fra en tidligere hendelse for å håndtere en ny hendelse på en bedre måte?
38. Deles erfaring fra enkelthendelser med andre (begge veier)?
    a. Andre virksomheter?
    b. NorCERT?
    c. Andre?

Appendix C - Employee Survey

Ansatteundersøkelse

1) Er du kjent med virksomhetens sikkerhetspolicy? (Og eventuelle andre bedriftsspesifikke dokumenter som omhandler sikkerhet)

2) Har du noen gang mottatt en mistenkelig mail (med dårlig norsk, vedlegg som ikke fungerer osv.)?
   a) Utførte du instruksjonene (trykket på linker, sendte passord, sendte annen informasjon)?
   b) Meldte du ifra om dette til noen?

3) Vet du hva et informasjonssikkerhetsbrudd er?
   a) Hva tror du det er (gjerne svar ved å komme med eksempler)?
   b) Er du observant med tanke på sikkerhetsbrudd i arbeidshverdagen din?

4) Er du kjent med hvilke tilfeller som bør rapporteres og til hvem?

5) Har du deltatt på øvelser/foredrag/nettleksjoner som omhandler informasjonssikkerhet og føler du det var nyttig?