Author version. Published version available at https://www.sciencedirect.com/science/article/pii/S0167404814000819

Information security incident management: Experiences reported in the literature

Inger Anne Tøndel[a,1,1,*], Maria B. Line[b,a], Martin G. Jaatun[a]

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

Abstract

This paper reports results of a systematic literature review on practice and experiences with performing incident management, covering a wide variety of organisations. Identified practices are summarised related to the incident management phases of ISO/IEC 27035. The study shows that the recommendations of this standard seem to be in line with what is considered good practice. Implementing the recommended activities is however challenging, including management commitment, access to proper tools, information retrieval, communication and collaboration, and learning after incidents. As a result, the paper identifies a set of aspects that should be given particular attention when developing support for incident management, e.g. in the form of guidelines, best practice descriptions or tools. In addition, they should be used as input to further research on information security incident management.

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

*Corresponding author

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

[1]Tel.: +47-97088476, Fax: +47-73594302

[2]This work has been supported by the Research Council of Norway through the IMMER project - Information Security Incident Management and Emergency Preparedness in ICT-based operations. The IMMER project is led by Intra Point.

1. Introduction

Today, Information and Communication Technology (ICT) plays an important role in all organisations. ICT has brought a lot of benefits to our society. At the same time, it has made us vulnerable to failures and attacks that come via the ICT systems. As organisations have become more and more dependent on ICT, the threats towards these systems have also become more prominent. The current situation can be summarised by the following quote by Ahmad et al. [1]:

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

Though a lot of measures can be taken in order to prevent information security incidents from ever taking place, it is not economically feasible to fully protect all systems [2]. Thus organisations need to prepare for what to do in case of incidents in their ICT systems.

This paper provides an overview of the documented experience in literature on information security incident management. The remainder of the paper is structured as follows: In Section 2 we describe our research method. Section 3 provides an overview of the most recognized and well-known standards and guidelines related to information security incident management, and Section 4 summarises relevant surveys and experience reports. We identify and discuss potential input to best practice descriptions and tools for incident management, as well as future research in Section 5. Section 6 offers concluding remarks.

2. Research method

The work presented in this article has been organised as a systematic review and conducted based on recommendations by Kitchenham and Charters [3]. The goal with performing the systematic review was to identify best practice for information security incident management, and in particular experiences made. The research questions that guided the review were thus:

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

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

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

We limited our study to literature that had incident management as its primary topic and that covered larger parts of the incident management process. Also, we were only interested in literature that covered incident management in enterprises, and that were not limited to a specific type of technology. As a consequence, literature that focused on how to identify malicious code or covered primarily forensic activities was excluded. The same goes for literature covering e.g. how national governments should interact to support incident management, and literature only considering incident management for Cloud environments. We limited our study to literature published after 2005.

Relevant literature were identified through a Scopus[3] search using search terms intended to identify all literature that covered incident management of information security incidents: ("incident management" OR "incident response" OR "incident reporting" OR "computer emergency response" OR "computer emergency management") AND ("information security" OR "cyber security" OR ict OR "computer security" OR "information technology")

Such a broad search string was used in order to identify as much as possible of the relevant literature. The identified literature was then manually included or excluded in the study by one researcher based on title and abstract. Only literature that described practice and/or experiences and met the above listed criteria were included in the study. A first Scopus search was performed in March 2012, and then a second search was performed in February 2013 in order to identify any literature added since the first search. We also manually went through the publicly available information from Terena and FIRST conferences, whitepapers etc. from Cert.org, and publications

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

from SANS. When going through the literature that was included in the study, we studied the references in order to identify additional literature. We have also added one recent study by one of the authors, and a study from a local university.

Two researchers were involved in the analysis work, where one of the papers was analysed by both. The others were analysed by one of the researchers. In the analysis the practices and experiences were identified. Then the practices and experiences were related to one of the incident management phases described in standards. We also identified in particular the experiences and practices that were related to communication and collaboration during incident management, as this was a topic that was considered important in several of the identified papers and spanned all phases.

3. The incident management process

An information security event can be defined as an *identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant* [4]. An information security incident is then a *single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security* [4].

Two of the main standards and guidelines related to information security incident management are the ISO/IEC 27035 standard on Information security incident management [4] and the NIST Special Publication 800-61 "Computer Security Incident Handling Guide" [5]. Both offer a structured approach to incident management, including planning and preparing for incident response, what to do when incidents strike, and how to extract lessons learned afterwards. SANS (Kral, 2010) and ENISA (2010) have also provided guidelines for incident handling, which resemble the structure offered by ISO/IEC and NIST. The guide from SANS is quite short and contains merely an overview of which activities belong to each phase. ENISA have excluded the preparations phase and just focussed on the activities performed by a response team in case of an incident. The documents from ISO/IEC and NIST are hence much more comprehensive, and Figure 1 provides an overview of the incident management process described by them[4]. As can be

[4]Note that the phases in this figure are not similar to the phases used in either of the

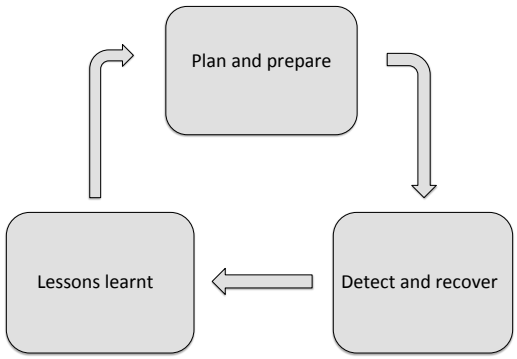


Figure 1: Before, during, and after an incident

seen from the figure, the main recommendations are similar. The ISO/IEC 27035 standard is developed by experts worldwide based on consensus, while the NIST guidelines are composed by a group of authors. Hence, the former should be considered more recognised than the latter, and we therefore explain the recommendations in the ISO/IEC 27035 standard in more detail in the following.

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

- Produce information security incident management policy and gain senior management commitment to that policy
- Update information security and risk management policies, so that they include incident management
- Define and document a detailed incident management scheme, including a classification scale used to grade incidents, information security

documents, but are instead based on the phases used by Jaatun et al. [6]. These three phases represent what happens before (planning), during (detect and recover) and after (learn) an incident. Such a rough classification was appropriate for comparison of the two documents. The "detect and recover" phase covers phase 2-4 in the ISO/IEC 27035 standard.

incident forms, procedures and actions to use the forms, and operating procedures for the Information Security Incident Response Team (ISIRT)

- Establish an ISIRT
- Establish and preserve relationships and connections with appropriate internal and external organisations
- Establish, implement and operate technical and other support mechanisms[5], and document responsibilities and operating procedures for the operations support team.
- Design and develop an awareness and training program
- Test the information security incident management scheme

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

- Alerts from security monitoring systems such as Intrusion Detection Systems (IDS) or Intrusion Detection and Prevention systems (IDP), antivirus software, honeypots, log monitoring systems, security information management systems and correlation engines.
- Alerts from network monitoring systems such as firewalls, network flow analysis, and web filtering.
- Analysis of log information from various systems and devices is also mentioned
- User reports, notifications from the help desk, and external notifications from third parties.

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

After detection, information on the event should be collected. Also all activities in this phase should be documented, any electronic evidence should be gathered and stored securely and the incident should be registered in an Incident Tracking System, with time and date for detection, observations, and contact information (optional). Any change control regimes should be maintained, keeping relevant databases up to date. Incidents may also be escalated[6] at this stage.

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

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

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

Incidents may be escalated, and the incident rating may be changed as more information is available. When the incident has been successfully dealt

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

with, the incident should be formally closed. The responses phase does not only include immediate actions, such as cutting off or shutting down systems or networks, but also later responses restoring the system and preventing similar incidents from happening again.

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

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

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

4. Reported experiences in the literature

The systematic review identified a set of studies and experience reports that documented organisations' practices regarding incident management:

1. Ahmad et al. (2012) studied incident management in a large financial institution (FinanceOrg) [1]
2. Werlinger et al. (2010) studied the practices related to diagnostic works during incident response in a variety of organisations [7]

3. Jaatun et al. (2009) studied incident response in the petroleum industry [6]
4. Line (2013) studied information security incident management practice in the power industry [8]
5. Scholl and Mangold (2011) presented a case study of planning, implementation and operation of a proactive incident response process [9]
6. Metzger et al. (2011) documented experiences from the work of the Computer Security Incident Response Team (CSIRT) at Leibniz Supercomputing Centre (LRZ) which operates the Munich Scientific Network [10]
7. Koivunen (2012) studied the reporting performed related to a set of incidents that were reported to CERT-FI [11]
8. Hove and Tårnes (2013) studied three large Norwegian companies to survey current practice and challenges [12]

These studies are different in scope and focus. Werlinger et al. dig deep into the diagnostic work done, while Ahmad et al. mainly address learning aspects. Jaatun et al. summarise high-level results from several smaller studies in the same sector, while Line at this stage only presents preliminary results of the case study. The studies have also been performed over a period of about 7 years. The types of organisations studied also vary, where some surveys summarise practices of several organisations [12, 6, 8, 7], while other consider the practices of individual teams [1, 10, 9]. Also, some teams are responsible for incident response within an organisation [1], while others deliver services to partners [10] or act as a national CERT [11]. Hove and Tårnes present three companies where one operates all IT services themselves (Company 1), another depend highly on two external suppliers (Company 2), while the third acts as a supplier for several large organisations (Company 3). As a result of these differences, it is not possible to compare the studies to say what practices are more common or which practices are lacking. Instead the studies together provide broad input on how information security incident management can be practiced, and identify experiences. This is important input to researchers, as well as tool developers and enterprises wanting to improve their own incident management.

In the following we summarise findings from these studies and experience reports related to the phases of ISO/IEC 27035. Findings related to collaboration and communication in incident management is also summarised.

4.1. Plan and prepare phase

The study of the petroleum industry [6] identified the need for a short and common plan for incident response. A finding from that study was that there were often several plans that impacted incident response, and that the current approach could appear scattered and randomly structured. The three Norwegian companies surveyed [12] all have incident management plans in some form. This may include plans and guidelines for handling (specific types of) security incidents, established routines, incident management handbooks for the incident response team, and plans for communication during incidents. Contingency plans may also cover major IT incidents. One of the companies has however identified a lack of an established check-list to use during incident response. In the power industry [8] plans for incident management were not widely established.

One of the main recommendations based on the experiences at LRZ-CSIRT [10] is the establishment of a security incident response process. This implies specifying roles, responsibilities and tasks related to incident response. At LRZ-CSIRT, incident response is divided into six phases: classification, escalation, analysis, diagnosis, solution and closing. The phases have been documented in different formats, with a short summary for administrators and service managers, a detailed description of the process (more than 20 pages) for the CSIRT team, as well as a five-page checklist that summarises the important steps. The short summary contains contact details, the most important data to be reported and a few best practice recommendations, while the detailed descriptions contain descriptions of responsibilities, tasks, and the detailed workflows, and provides links to other documents and workflow descriptions.

Experiences from LRZ-CSIRT also result in the recommendation that organisations clearly define what a security incident is, so that a security incident is distinguished from other issues such as system misbehaviour due to configuration errors. For the financial institution (FinanceOrg) studied by Ahmad et al. as well as the Norwegian companies surveyed [12], the definition of impact ratings was important, as this determined how incidents were handled.

Note that though plans and processes are important as a basis, some organisations consider experienced incident handlers to provide much more value during an emergency situation [12]. Tacit knowledge and frequent training make the organisation better prepared for unexpected incidents, as it is impossible to plan for all eventualities. Ownership to the routines is also

important, if they are to be useful. Hence, the IT manager of Company 2 in the study by Hove and Tårnes considers the construction of a holistic plan to be the most challenging part of incident management.

Incident handling may include a number of different roles, e.g. system administrators and users, network administrators, the public relations department, management and law enforcement authorities [10]. Defining responsibilities is thus important. This is especially important in cases where IT has been outsourced [12]. At LRZ-CSIRT a Security Incident Coordinator (SIC) is selected on a case-to-case basis and is granted extended decision-making power. The SIC is then responsible and can coordinate the whole process [10]. In FinanceOrg, the response to high-impact incidents was coordinated by a High-impact Incident Response Coordination Team, while other incidents were handled by a Network Incident Response Team more independently [1]. Two of the Norwegian companies surveyed [12] construct teams based on the incident, and one of these companies have a specific team that are involved for major incidents. None of the distribution system operators (DSOs) surveyed by Line had established their own CSIRT within the organisation. However, in the case where the ICT services were outsourced, the suppliers might have established response teams, but this was not elaborated in the study.

The studies and experience reports provide an overview of a lot of technical measures taken to prepare for incident detection and response. Both Werlinger et al. and Metzger et al. explain the importance of proper tools for monitoring, and also the need for centralised tools that can integrate input from several monitoring tools to gain a proper overview of the situation. Incident response teams often also perform proactive activities [1, 12, 10, 7] like vulnerability assessments and penetration testing, and these also require the use of tools. As stressed by Werlinger et al., proper use of such tools often requires very specific knowledge about the network and the type of traffic to expect. This is rarely documented, and is thus difficult to obtain. Werlinger et al. also found that security practitioners often combined tools in unique ways to maximise their utility. Due to usability and budget constraints, practitioners also often created their own tools in form of scripts of programs for the command interpreter of an operating system.

Metzger et al. explain their success with automating part of the incident response process, something that has made it possible to achieve adequate response in spite of limited personnel, and also outside normal business hours. As of now, more than 85 percent of all incidents are (at least partially) auto-

matically processed. One of the reasons why this is possible is their definitions of Standard Security Incidents. These are specific types of security-related incidents that occur frequently and that are considered to be of low risk. As a consequence they allow certain simplifications of the process, compared to other incidents.

"Awareness training and official statements of the management" is mentioned by LRZ-CSIRT [10] as important in building a culture where incidents are reported. The study by Ahmad et al. identified a positive reporting culture at FinanceOrg where those that reported incidents were not punished, something that was an advantage for incident management. This was also the case for the power companies surveyed by Line. One of the recommendations from LRZ-CSIRT is that possible reporting ways have to be defined and each user has to be aware of these ways. At LRZ-CSIRT they used a group telephone number and a mailing list for these purposes.

In the study of the petroleum industry [6] it was found that individual awareness related to information security should be improved. Also scenario training that was commonly used for HSE and other loss prevention areas was not used for ICT incidents. The three companies studied by Hove and Tårnes perform awareness raising activities - not necessarily on a regular basis, but from time to time. They also train on incident management. The other studies do not document any general awareness raising and training activities in the organisations.

Motivations for performing training activities include increased awareness among managers, to stay familiarised with routines, and to have well-established roles and effective coordination. The companies have also used rehearsals to identify areas of improvement. Conducting rehearsals is however considered challenging; especially ensuring that participants train on the right things, that the scenario is realistic and that it is useful for real situations. Training activities may include external suppliers, customers and government. In general, rehearsals are not used for common low-impact incidents [12].

4.2. Detection and reporting phase

Scholl and Mangold found that security events and incidents were captured from technical monitoring tools, vendors, and employees or contractors. At LRZ-CSIRT [10], incidents were detected in three different ways:

1. By local system and service administrators that reported incidents manually by phone or email.

2. From automatic security warnings from DFN-CERT, or reports from other third party services
3. Through local security monitoring mechanisms.

From their experience, the manual approach was essential and the most frequently used. In the studies and experience reports, most attention is however given to the local security monitoring tools in use. In the study by Werlinger et al., common detection activities identified were monitoring the organisation's IT system with various tools such as antivirus and IDS, and sending and receiving notifications. LRZ-CSIRT reports on using IDS systems, as well as added monitoring mechanisms in custom NAT gateways, mail monitoring mechanisms and analysis of netflow data. All Distribution System Operators (DSOs) surveyed by Line have IDS/IPS systems, antivirus solutions, and firewalls[7] in place for their administrative ICT systems. The tools currently in use however have their limitations. The three Norwegian companies surveyed [12] also report on automatic monitoring systems. The results of this survey however also emphasise the role of users in detecting and reporting abnormal and suspicious system behaviour.

Werlinger et al. report on a lack of accuracy in tools, resulting in high false positives rates. Also, usability of tools was a concern, and often there was a need to write own tools or make adjustments to existing tools [10, 7]. In addition, the most common tools may not be applicable or typically used for all types of systems. DSOs reported that new power automation systems might have detection systems in place, while in most cases they relied on manual detection by operators that experienced abnormalities or unexpected behaviour from the system. In some cases control room managers did not know if there were any detection systems in place or not [8]. Some organisations [12] had outsourced the responsibility for network monitoring and detection of incidents to third parties.

Effective detection often required tacit knowledge about the organisation's systems and services, and due to complexity and lack of resources teams often relied on notifications to detect incidents. Notifications could come from various stakeholders, including users and other IT professionals. One of the observations by Koivunen was that, of the incidents studied, none of the victims of the security breaches seemed to have discovered the inci-

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

dent on their own. External reports were required to get information that an incident may have happened, or to complement the victims' limited understanding of the true scope of the incident. In each of the incident cases studied, the incident was discovered by someone with no apparent dealings with the compromised party. Intermediaries were needed in order to pass on the information, and often not all affected parties were included in the information sharing. Koivunen claims that "victims of many internet threats are among the last ones to learn about the information security incidents affecting them" [11]. Some incidents are also more difficult to detect. In the study by Hove and Tårnes, one of the interviewees claimed that it is almost impossible to detect security incidents caused by disloyal employees.

Receiving and handling notifications was in some cases challenging. Lack of involvement from suppliers and service providers was observed in the study of the petroleum industry [6]. Werlinger et al. found that the notifications often resulted in a need for more communication among the stakeholders. LRZ-CERT experienced that some administrators did not report incidents, either because they did not know that they should or because they expected that the reporting would result in "worst-case consequences" as they were responsible for the system and therefore considered themselves fully responsible for the incident.

The case study performed by Hove and Tårnes also included a set of regular employees. In general it was found that few of the employees knew to whom security incidents should be reported, and that they also were not sure which incidents to report. Reporting channels commonly mentioned was the immediate supervisor, the local or central IT-manager or the security manager. For all companies the IT-manager suspected underreporting of incidents. This was also supported by a quote from one of the employees: *"I have the impression that it's probably more situations that should have been reported than that are actually reported"* [12].

Some studies found that security events and incidents were reported through existing help desk functions [1, 12, 9]. LRZ-CERT however had bypassed traditional first level support, by establishing a group telephone number and a mailing list as the main points of contact. The central ticketing system was still used to ensure all security incidents were documented in a uniform manner regardless of the reporting channel. In the case study presented by Scholl and Mangold, several reporting options were available. The service desk was normally used, but it was also possible to contact the security team directly. They also allowed for anonymous reporting through

a portal.

Several of the studies and experience reports explain a lot about the way incidents are registered, and it seems from the cases that best practice is that documentation begins when incidents are reported [10, 9]. Ticketing or incident tracking systems are mentioned in several studies [1, 10, 9]. In some cases, aspects of the collection and reporting process are automated [10, 9]. For LRZ-CSIRT standardised XML-based notifications from DFN-CERT made it possible to automatically process such alerts. The use of a central system for collection, correlation and analysis of all data related to security incidents was also recommended [10].

4.3. Assessment and decision phase

At LRZ-CERT [10] the incident reports shall include the contact details of the incident reporter, description of the identified security issues, evaluation of the sufficiency of the data and an initial classification.

Werlinger et al. found that typical activities for analysing an anomaly was to confirm, often with alternate data sources, that a compromise has actually occurred, estimating magnitude and consequences, and tracking the source of the anomaly. The diagnosis work relied on various security tools, as well as key personal skills: "Pattern recognition, hypothesis generation, communication, bricolage (i.e. dynamic integration of security tools in novel, unanticipated ways), and tacit knowledge about their organisations and systems" [7]. Verification that an incident in fact has occurred may require collaboration with external organisations. Also it requires expertise and knowledge of what is normal in the system. The same way, tracking of the source of the anomaly often required specific technical expertise and knowledge of attack patterns. If it was difficult to find the source, it was considered useful to interact with other specialists that could offer novel perspectives as they were new to the investigation or had a different background. Simulations of the incident could also be performed.

Koivunen points to the problem of verifying the validation of reports received from externals. It eases the process if there is already a trust relationship between the reporter and the organisation (such as the one that exists between CERT-FI and F-Secure). However, the survey identified a considerable demand for the incident discoverers to retain their anonymity. Also it was the experience of CERT-FI that the ultimate recipients of these reports were best being kept secret from the reporters. As a result, reports

from incident-reporting clearing houses had an important role in three of the six incidents studied.

Classification of incidents is central in several of the cases described, though the approach may vary slightly. FinanceOrg [1] considers the criteria for incident rating to be sensitive, but explain that incidents are classified into two categories - low-impact and high-impact - based on their impact on the organisation. All three Norwegian companies surveyed [12] classify incidents based on impact/severity (typically high, medium or low). Company 1 also categorises based on type of incident and the service or system affected. In the case studied by Scholl and Mangold, a four level severity system was used, where severity was assigned based on impact to business operation, impact to human life/safety, type of incident, and target or source of the incident. LRZ-CSIRT also uses four priorities - low, medium, high and very high. Their classification is based on aspects such as the number of affected systems and services, whether internal or customer-operated machines are affected, which services and SLAs may be impacted, additional dependencies on other services, where the assumed attacker is located, and what type of attack has been observed. A cross-correlation with other open and resolved security incidents is also performed. In particular SLAs and the maximum reaction time that has been negotiated with the affected customers is important. In the study by Werlinger et al., some organisations explained that the potential cost of the incident was communicated to managers, who then decided whether to proceed.

The classification of an incident is important for what happens next, in particular it may impact who is involved [1, 12, 9]. In the study by Werlinger et al., it was however identified that in some circumstances incidents that did not qualify as high-risk according to the organisation's criteria were still investigated by the security team in order to protect their systems. Classification also influences priorities, such as in the case described by Scholl and Mangold where events tagged as "security events" were processed within 5 minutes.

Decisions on how to handle an incident can be particularly challenging when IT operations are outsourced and there are several suppliers involved. In the study by Hove and Tårnes, this is pointed out both by the company that have outsourced IT operations and companies that act as suppliers. Incidents at Company 2 are normally handled by a team from a supplier, say Supplier A. In cases where the incident concerns systems from other suppliers, Supplier A is responsible for reporting the incident to them. Problems arise

if none of the suppliers take responsibility for the dealing with the incident.

4.4. Responses phase

The survey of Hove and Tårnes reveal differing purposes for the response phase. Company 1 state that the main purpose is not only to get the systems up and running as fast as possible. It is also important to make sure that the incident is properly resolved before restoring normal operations, and to determine whether the system is vulnerable to more attacks. Company 3, on the other side, states that their main purpose is to find a temporary solution to the problem so that they can retain normal business operation and minimise business impact. This is important as they are evaluated by their customers based on the availability of the services they deliver. The study of FinanceOrg [1] highlights the need for communication and cooperation in the responses phase. The organisation's incident tracking system facilitates communication between technical teams. It also is important for documentation, and provides a timeline of activities and a chain of evidence for incident handling. As such it is important for monitoring and logging the progress of the incident handling. For high-impact incidents, the collaboration process is characterised as "highly mature". Both technical and business staff is involved, with one conference call set up for each. In the business conference call, progress is explained in a non-technical way, to ensure that the business gets relevant and understandable information about the incident. Phone, email and the helpdesk system are also used for communication, particularly towards the technical personnel at the Network Incident Response Team.

Metzger et al. provide more insight into the types of responses a CSIRT typically performs. Immediate responses may include removal of affected systems from the network, creating backups and disk images, performing basic IT forensics, escalating the incident, and documenting all steps. The main goal in these early stages is to keep in touch with the individual that reported the incident and to find a way to restore the affected system. A challenge experienced by CSIRT is the lack of sufficient personnel with expertise in using forensic tools. Thus they do not use specific or custom-built forensic tools for this, but instead rely on general-purpose tools and mechanisms that are part of the default system configuration for this. Limited expertise on forensics is also reported in the study by Hove and Tårnes [12]. For such activities the companies rely on third parties or the police.

For common and less severe incidents the CSIRT response is performed in a fully automatic manner [10], where examples of automatic actions include

forwarding of information to responsible on-site administrator, suspension of the offending machine's internet access, and notification of the CSIRT team. Later responses, such as re-activation of blocked IP addresses are currently a manual task. After a solution has been implemented, the system is monitored extensively for a period of up to 14 days.

The Norwegian companies studied [12] are aware of potential privacy implications of response work. They explain that access to user-owned files is done in compliance with privacy legislation, and one of the companies has a central security advisor that is involved in cases concerning employee privacy.

4.5. Lessons learnt phase

The study of the petroleum industry [6] showed that learning from incidents was considered important, but that organisations found it difficult in practice. Activities aimed towards learning seems however to be common in the surveys and experience reports we have identified. Sholl and Mangold [9] explain that incident statistics are generated every month, and that periodic reviewing of all major and minor information security incidents is performed on a monthly basis. At LRZ-CERT [10], reviews are performed after each major incident, as well as periodically. In one of the organisations surveyed by Werlinger et al. [7], recent security incidents are discussed weekly. At FinanceOrg [1], the goal is to review each high-impact incident within 24 hours of the system services being restored, resulting in a post-incident report. There is no structured process for reviewing low-impact incidents, however the team involved still attempt to learn from such incidents and identify areas of improvements. Most DSOs surveyed by Line had routines for regular meetings or for evaluations after an incident had occurred, but still there were some DSOs that did not perform regular reporting or evaluations, neither in the team, nor with top management. The companies studied by Hove and Tårnes all perform post-incident activities for major incidents. Company 1 also performs reviews of incidents where the incident handling was not considered efficient.

The motivation for performing learning activities include: keeping security practitioners updated on current threats [7], getting new ideas on how to resolve challenging incidents [7], to discuss possible improvements of the incident management process and its activities [12, 10], to perform trend analysis [12, 10], to identify direct causes [1, 12], to identify security measures that can prevent future incidents [1, 12, 10], and updating risk assessments of

involved systems [1]. At FinanceOrg compliance requirements through Basel II and Sarbanes Oxley require assessment and reporting of incidents.

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

Dissemination of incident information and lessons learnt seem to happen in varying extent and by different means in the surveyed organisations. Scholl and Mangold explain that incident statistics are generated for review of the information security forum, which is responsible for coordinating information security activities throughout the organisation. In the study by Hove and Tårnes, Company 2 receives monthly incident reports from the suppliers, and arranges monthly meetings where incidents are discussed. In addition they have a quarterly meeting in their security board, where also information security incidents are discussed. At FinanceOrg, information on low-impact incidents is included in formal reports to management, where the focus is on technical means and statistical information. These reports therefore contain only generalised learning information. At FinanceOrg, informal communication channels are also used for dissemination of incident knowledge, but there is a lack on formal policies on what should be disseminated and what information channels should be used. Few of the surveys mention sharing incident information outside the organisation. The survey of the petroleum industry [6] identified a lack of openness about incidents and a lack of willingness to report incidents to the industry as a whole. One of the companies in Hove and Tårnes' study reports on sharing information on some specific incidents with trusted communities and partners. One of the companies in this study also points at the potential for using incidents for increased awareness, and the IT-manager is quoted: *"never waste a good crisis"* [12].

Several challenges are reported when it comes to learning from incidents. Inadequate involvement of suppliers is pointed out as a problem in the petroleum industry [6]. A focus on direct causes, rather than underlying

causal structures, is mentioned by Ahmad et al. They also identified a strong focus on technical information over policy and risk. Especially for low-impact incidents, a focus on solving the problem as fast as possible seems to have evolved into a dislike for "paperwork". Incidents are solved effectively and efficiently, and the team gathers a large amount of technical information to solve the problem. Gathering additional data important for future learning is however not considered. For high-impact incidents, there is an understanding of the importance of identifying the root causes of an incident, also including organisational and human factors. However, they also struggle with how learning should be done in practice. In particular their high-impact incident management process does not respond to incident precursors[8], identified dissemination challenges have not been addressed, and key areas such as policy and risk do not benefit from incident data.

Although learning from incidents has its challenges, the incident statistics reported by FinanceOrg should motivate more organisations to improve on this aspect. They claim that their learning process for high-impact incidents has resulted in a reduction of incidents of around 200 per month in 2002 down to only 16 at the time of the study[9].

4.6. Collaboration and communication in incident management

Studies in the petroleum industry [6] revealed that the organisations usually had several plans covering different aspects of the incident management process. It was also found that suppliers were not adequately involved in planning for incidents, although the operator would in many cases depend on them during incident management. Individual information security awareness was also not at a satisfactory level. Finally, and maybe most disturbing, the study revealed a "deep sense of mistrust" between process control engineers and ICT network administrators.

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

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

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

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

The importance of collaboration and communication is also reflected in the procedures for responding to high-impact incidents at the FinanceOrg [1]. Technical and business conference calls are set up in order to gather knowledge and communicate progress; in general, the management of the incident relies heavily on communication via teleconferencing, phone, e-mail and the helpdesk system. It is not without reason that Werlinger et al. list 'communication' as one of the five key skills required for diagnosis work.

The study by Hove and Tårnes emphasises the challenge of information collection and dissemination during the incident handling process. Especially for organisations with distributed organisational structures there are many sources of information. Also knowing how much information to share can be difficult. Too little information could lead to wrong decisions due to an erroneous picture of the situation, while too much information can be overwhelming and cause delays in decision-making. This is also supported by Ahmad et al. where an information security manager states that the sharing, or rather the finding, of information was one of the most challenging parts of her job.

In cases where IT operations are outsourced, collaboration during incident management is even more challenging. Even minor incidents can be problematic if all assume the incident is someone else's responsibility. As pointed out by one supplier, *"It is also a political "game". Who will pay for it?"* [12]. Also customers and suppliers often handle different parts of the incident [12].

The study of the petroleum industry revealed that information security was viewed merely as a technical issue. This technical focus was also found in the study of FinanceOrg. Especially for low-impact incidents, the emphasis

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

5. Discussion

The surveys and experience reports provide important insights into current practice when it comes to incident management (Research question 1 and 2), and can be used as a foundation for identifying best practice. Below we discuss how the surveys and experience reports relate to the recommendations of ISO/IEC 27035 (Research question 3). We also identify and discuss potential input to best practice descriptions and tools for incident management, as well as future research.

5.1. Practice vs. standards

Table provides a summary of the recommended activities of ISO/IEC 27035 related to the identified practice in the surveys and experience reports. The main impression is that the recommendations of the standard are in line with what is considered good practice. The surveys and experience reports however document that several of the recommendations are not easy to perform in practice. As examples, the organisations seem to struggle with gaining management commitment and efficient information collection and communication during incidents.

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

that the activity is not performed, but that it is not documented in the papers.

Phase	ISO/IEC 27035 re
lan and prepare	Produce policy; de
Gain senior management commitment	Official statements
Update security and risk management policies	-
Establish ISIRT	Defining roles is co
Establish relationships with relevant organisations	Clearly defined rol
Implement technical and other support mechanisms	Technical tools are
Awareness and training	Mentioned related
Test incident management scheme	Rehearsals are valu
etection and reporting	Detection of securi
Collection of information	Use various tools.
Reporting and documentation	Documentation be
ssessment and decision	Decide if security i
Classify incident	Classification of in
Decide on actions, and distribute responsibilities; provide formal procedures	Classification is im
esponses	Immediate respons
Later responses	Monitoring of syst
Forensic analysis, if required	A possible challeng
Communicate internally and externally	Need for communi
Escalate, if necessary	Escalation mentio
essons learnt	Further forensic ar
Identify lessons learnt	Incident statistics
Review and improve controls, policies and risk assessments	Motivation include
Review effectiveness of response	One motivation m
Update relevant databases; share results with trusted community	Learning activities

5.2. Recommendations for best practice descriptions and incident management tools

The ISO/IEC 27035 standard seems to be in line with what is considered best practice. The surveys and experience reports however identify some aspects that seem particularly challenging, and where additional support and concrete guidance is needed. They also identify examples of good practice that can motivate and inspire organisations to improve their own way of performing incident management. The following aspects should be taken

into account when developing support in form of guidelines, best practice descriptions or tools, and in future research on information security incident management:

- **Creating plans and classifications of incidents:** Proper plans and incident classifications seem to be very important. Creating a short and common plan has however been identified as a challenge [6]. There is a need for plans that are useful for a variety of stakeholders. There is also a need to identify what a security incident is, and decide what to do for different types of incidents [10]. Organisations could probably benefit from templates and examples in this respect.

- **Gaining senior management commitment:** This is something all agree is important, but that seems difficult in practice. Examples of successful approaches should be highlighted, where available, and turned into practical advice.

- **Involving all employees:** As information security concerns everyone and current trends show that attacks are now targeting employees directly, not necessarily the technical systems, all employees should be aware and well trained in recognising and reporting incidents [12]. Current standards describe training activities for incident handlers only.

- **Coping with the existing tools and their lack of usability:** A lot of the studies mention a high number of technical tools that are used for incident detection and response. Though highly useful, they generally seem to suffer from a lack of usability, a high number of false positives, and a need for very precise and rarely documented information [10, 7]. Organisations that are new to incident response would probably benefit from an introduction to common tools. Also there is a need for a strategy for dealing with the current dependence on tacit knowledge.

- **Using automation as a mean to improve efficiency:** Automation seems to be best practice for dealing with common and low-risk incidents [10].

- **Arrange for manual reporting of incidents:** Despite the focus on technical tools, manual reporting seems to be a key when it comes to detection of incidents [12, 11, 8, 10, 7]. Organisations would benefit from advice on how to motivate reporting of incidents, how to make it

easy to report incidents (both for internals and externals), and how to verify reports.

- **Dealing with events and low-impact incidents:** The importance of detecting events early and understanding their potential implications was stressed by Scholl and Mangold. Based on available data breach investigation reports they claim that "most breaches do not happen immediately, but take place over time." [9] Thus, by detecting initial or early events, it is possible to prevent incidents. For the same reason, learning from low-impact incidents and security events should not be omitted [1].

- **Documenting incidents:** Best practice seems to be to start documentation as soon as an incident is reported or detected [10, 9]. An incident tracking system should be used [10, 9], and it is recommended to collect all data related to the incident into one single system[10].

- **Collaboration among teams and across disciplines:** It seems that collaboration within the team works satisfactorily, but that communication with externals and also collaboration including both technical and business staff is more challenging [1, 12, 7]. The impression is that response and learning activities mainly include technical staff. Still, the business units affected and management have a potential role to play – at least for severe incidents.

- **Identifying root causes:** Current learning activities are focused on technical aspects and identification of direct causes. But the root cause may well lie in policies, procedures, lack of competence, or other underlying aspects [1]. To increase the learning outcome from incidents, organisations should receive more support for learning activities so that they are able to include relevant types of personnel in the analysis and ask questions that will help reveal underlying causes.

- **Motivating learning activities:** Organisations seem to agree that learning from incidents is important. It is however considered difficult by some [6]. Learning from low-impact incidents also seems not to be prioritised [1, 12]. There is a need for good stories about the potential that learning activities bring when it comes to improved security. The reduction in incidents experienced by FinanceOrg [1] can be one such story.

- **Sharing lessons learned:** It seems that lessons learned and other incident information is often available only to some selected few, though there may be several other individuals or departments in the organisation that would benefit from such information [1]. Organisations could benefit from examples regarding what incident data could be used for and who could be interested in such information, as input to creating strategies for dissemination of this type of data.

6. Summary and conclusions

We have summarised recommendations for incident management documented in standards documents, and have provided an overview of documented experiences in literature. We argue that the ISO/IEC 27035 standard is a good starting point for organisations when it comes to incident management. Implementing this standard, with all its recommendations and activities, is however not straight-forward, and the studies of practices and experiences documented in literature have led to identification of a set of aspects that should be given particular attention when developing support in form of guidelines, best practice descriptions or tools. They should also be considered useful input to further research on information security incident management.

References

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

[2] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. Eeten, M. Levi, T. Moore, S. Savage, Measuring the Cost of Cybercrime, in: 11th Workshop on the Economics of Information Security (WEIS'12), 2012.

[3] C. S. Kitchenham B, Guidelines for performing Systematic Literature Reviews in Software Engineering, EBSE Technical Report (2007).

[4] ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management (2011).

[5] NIST, 800-61: Computer Security Incident Handling Guide, National Institute of Standards and Technology (2008).

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

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

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

[9] F. Scholl, M. Mangold, Proactive Incident Response, The Information Systems Security Association Journal (2011).

[10] S. Metzger, W. Hommel, H. Reiser, Integrated Security Incident Management – Concepts and Real-World Experiences, in: Sixth International Conference on IT Security Incident Management and IT Forensics (IMF), 2011, pp. 107–121.

[11] E. Koivunen, Why Wasn't I Notified: Information Security Incident Reporting Demystified, in: 15th Nordic Conference in Secure IT Systems (Nordsec 2010), 2010.

[12] C. Hove, M. Tårnes, Information Security Incident Management: An Empirical Study of Current Practice, Norwegian University of Science and Technology (2013).