COMPUTERS & SECURITY 45 (2014) 42–57

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

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

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

[a] *SINTEF ICT, N-7465 Trondheim, Norway*

[b] *Dept. of Telematics, Norwegian University of Science and Technology, N-7491 Trondheim, Norway*

ARTICLE INFO

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

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

ABSTRACT

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

1. Introduction

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

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

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

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

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

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

http://dx.doi.org/10.1016/j.cose.2014.05.003
0167-4048/

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

2. Research method

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

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

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

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

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

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

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

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

3. The incident management process

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

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

[2] http://www.scopus.com.
[3] Trans-European Research and Education Networking Association, www.terena.org.
[4] Forum for Incident Response and Security Teams, www.first.org.
[5] www.cert.org.
[6] www.sans.org.
[7] IT Security Incident Management and IT Forensics.
[8] The proceedings from this conference were not available at Scopus at the time of the search, and was included because relevant material had been published at previous IMF conferences.
[9] This study was in form of a student thesis and would thus not be available in a Scopus search. Furthermore, we have performed a search for related student work from other universities, but without results (this may be because such student papers may be difficult to access outside the respective universities).

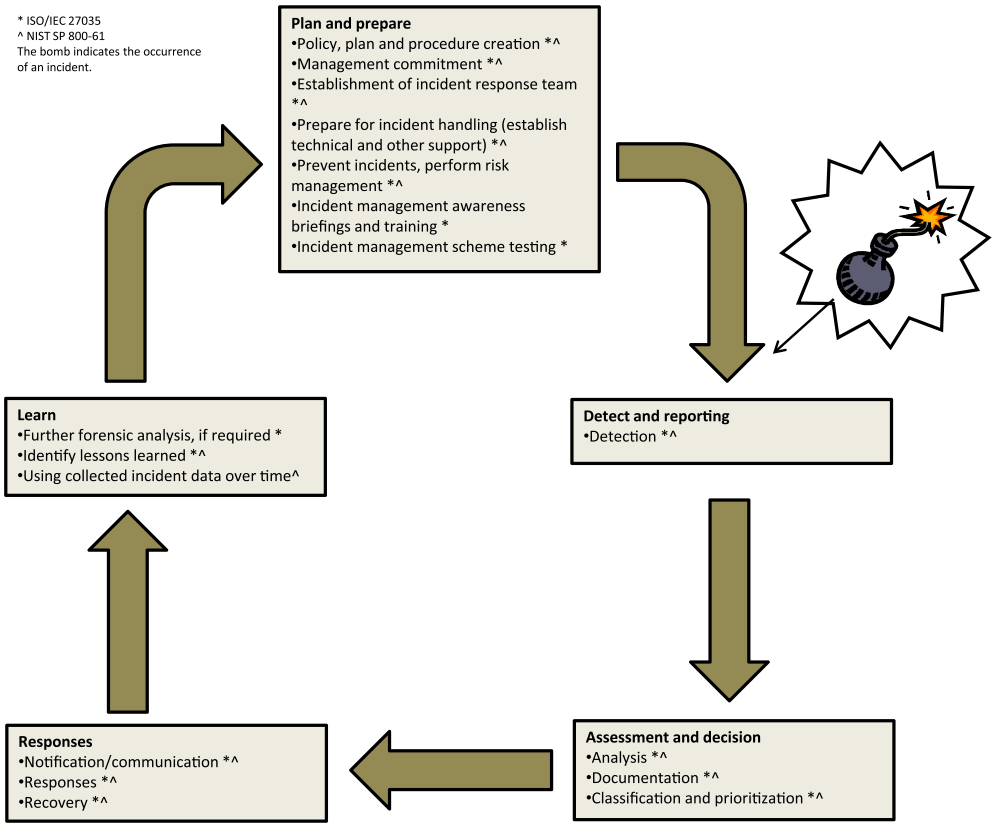

Fig. 1 – The incident management process.

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

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

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

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

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

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

Table 1 – Overview of included papers.

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

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

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

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

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

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

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

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

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

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

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

4. Reported experiences in the literature

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

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

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

4.1. *Plan and prepare phase*

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

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

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

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

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

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

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

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

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

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

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

In the study of the petroleum industry (Jaatun et al., 2009) it was found that individual awareness related to information security should be improved. Furthermore, scenario training, that was commonly used for HSE and other loss prevention

areas, was not used for ICT incidents. The three companies studied by Hove and Tårnes (2013) perform awareness raising activities – not necessarily on a regular basis, but from time to time. They also train on incident management. The other studies did not document any general awareness raising and training activities in the organisations.

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

Summary of reported practices in the plan and prepare phase:

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

4.2. *Detection and reporting phase*

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

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

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

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

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

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

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

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

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

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

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

Summary of reported practices in the detection and reporting phase:

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

4.3. *Assessment and decision phase*

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

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

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

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

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

Decisions on how to handle an incident can be particularly challenging when IT operations are outsourced and there are several suppliers involved. In the study by Hove and Tårnes (2013), this is pointed out both by the company that have outsourced IT operations and companies that act as suppliers. In one of the companies, incidents are normally handled by a team from one supplier, say Supplier A. In cases where the incident concerns systems from other suppliers, Supplier A is

responsible for reporting the incident to them. Problems arise if none of the suppliers take responsibility for the dealing with the incident. Furthermore, assigning priorities for incidents may be a challenge in outsourcing environments, i.e. *"when a particular server is down, what does it mean for the customer?"* (de Souza et al., 2011).

Summary of reported practices in the assessment and decision phase:

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

4.4. *Responses phase*

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

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

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

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

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

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

Summary of reported practices in the responses phase:

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

4.5. *Lessons learnt phase*

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

The motivation for performing learning activities include: keeping security practitioners updated on current threats (Werlinger et al., 2010), getting new ideas on how to resolve challenging incidents (Werlinger et al., 2010), discussing possible improvements of the incident management process

and its activities (Hove and Tårnes, 2013; Metzger et al., 2011), performing trend analysis (Hove and Tårnes, 2013; Metzger et al., 2011), identifying direct causes (Ahmad et al., 2012; Hove and Tårnes, 2013), identifying security measures that can prevent future incidents (Ahmad et al., 2012; Hove and Tårnes, 2013; Metzger et al., 2011), and updating risk assessments of involved systems (Ahmad et al., 2012). At FinanceOrg (Ahmad et al., 2012) compliance requirements through Basel II and Sarbanes–Oxley require assessment and reporting of incidents.

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

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

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

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

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

Summary of reported practices in the lessons learnt phase:

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

4.6. *Collaboration and communication in incident management*

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

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

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

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

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

Table 2 – (*continued*)

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

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

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

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

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

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

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

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

were discussed weekly so that **security practitioners** could learn about new threats and assist in solving challenging incidents.

5. Discussion

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

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

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

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

5.2. *Inspirational examples*

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

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

5.3. *Incident management challenges*

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

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

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

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

5.4. *Approaches to addressing the challenges*

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

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

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

5.5. *Research needs in incident management*

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

Based on the material we have identified, we claim that there is a need for more empirical studies in this field. The material contains a few case studies that go deep into how information security incident management is performed in

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

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

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

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

6. Summary and conclusions

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

Acknowledgement

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

REFERENCES

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

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

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

Proceedings of the 2004 ACM conference on Computer supported cooperative work (CSCW '04). New York, NY, USA: ACM; 2004. pp. 388–95. http://doi.acm.org/10.1145/1031607.1031672.
Brewster E, Griffiths R, Lawes A, Sansbury J. IT service management: a guide for ITIL foundation exam candidates. 2nd ed. BCS, The Chartered Institute for IT; 2012.
Cadavieco JF, Pérez CR, Fernández CB. Information technology incident management: a case study of the University of Oviedo and the Faculty of Teacher Training and Education. Univ Knowl Soc J (RUSC) 2012;9(2):280–95.
Cichonski P, Millar T, Grance T, Scarfone K. NIST SP 800-861: Computer security incident handling guide. National Institute of Standards and Technology; 2008.
Cusick J, Ma G. Creating an ITIL inspired incident management approach: roots, response, and results. In: Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP; 2010. pp. 142–8. http://dx.doi.org/10.1109/NOMSW.2010.5486589.
de Souza CRB, Pinhanez CS, Cavalcante VF. Information needs of system administrators in information technology service factories. In: Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT '11). New York, NY, USA: ACM; 2011. p. 10. http://doi.acm.org/10.1145/2076444.2076447.
ENISA. Good practice guide for incident management; 2010.
Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst 2009;18(2):106–25. http://dx.doi.org/10.1057/ejis.2009.6.
Hove C, Tårnes M. Information security incident management: an empirical study of current practice. Norwegian University of Science and Technology; 2013.
Ismail S, Ahmad A, Shukran MAM. New method of forensic computing in a small organization. Aust J Basic Appl Sci 2011;5(9):2019–25.
ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management; 2011.
Jaatun MG, Albrechtsen E, Line M, Johnsen SO, Wærø I, Longva OH, et al. A study of information security practice in a critical infrastructure application. In: Rong C, Jaatun MG, Sandnes FE, Yang LT, Ma J, editors. Autonomic and Trusted Computing. Lecture Notes in Computer Science, vol. 5060. Springer Berlin Heidelberg; 2008. pp. 527–39. http://dx.doi.org/10.1007/978-3-540-69295-9_42.
Jaatun MG, Albrechtsen E, Line MB, Tøndel IA, Longva OH. A framework for incident response management in the petroleum industry. Int J Crit Infrastruct Prot 2009;2:26–37.
Johnston A, Reust J. Network intrusion investigation preparation and challenges. Digit Investig 2006;3(3):118–26. http://dx.doi.org/10.1016/j.diin.2006.08.001. http://www.sciencedirect.com/science/article/pii/S1742287606000922.
Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering; 2007 [EBSE Technical Report].
Koivunen E. Why wasn't I notified: information security incident reporting demystified. In: 15th Nordic Conference in Secure IT Systems (NordSec 2010); 2010.
Kotulic AG, Clark JG. Why there aren't more information security research studies. Inf Manag 2004;41(5):597–607. http://dx.doi.org/10.1016/j.im.2003.08.001. http://www.sciencedirect.com/science/article/pii/S0378720603000995.
Kral P. The incident handlers handbook [Technical Report]. SANS Institute; 2011.
Kurowski S, Frings S. Computational documentation of IT incidents as support for forensic operations. In: IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on; 2011. pp. 37–47. http://dx.doi.org/10.1109/IMF.2011.18.
Line MB. A case study: preparing for the smart grids – identifying current practice for information security incident management in the power industry. In: Seventh International Conference on IT Security Incident Management and IT Forensics (IMF); 2013.
Metzger S, Hommel W, Reiser H. Integrated security incident management – concepts and real-world experiences. In: Sixth International Conference on IT Security Incident Management and IT Forensics (IMF); 2011. pp. 107–21.
Möller K. Setting up a GRID-CERT, Experiences of an academic CSIRT. Campus Wide Inf Syst 2007;24(4):260–70.
Rhee HS, Ryu YU, Kim CT. Unrealistic optimism on information security management. Comput Secur 2012;31(2):221–32. http://dx.doi.org/10.1016/j.cose.2011.12.001. http://www.sciencedirect.com/science/article/pii/S0167404811001441.
Robson C. Real world research. 3rd ed. John Wiley & Sons Ltd.; 2011.
Scholl F, Mangold M. Proactive incident response. Inf Syst Secur Assoc J 2011;9(2). http://www.issa.org/?page=JournalFebruary2011.
Werlinger R, Hawkey K, Muldner K, Jaferian P, Beznosov K. The challenges of using an intrusion detection system: is it worth the effort?. In: Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08). New York, NY, USA: ACM; 2008. pp. 107–18. http://doi.acm.org/10.1145/1408664.1408679.
Werlinger R, Muldner K, Hawkey K, Beznosov K. Preparation, detection, and analysis: the diagnostic work of IT security incident response. Inf Manag Comput Secur 2010;18(1):26–42.
West-Brown MJ, Stikvoort D, Kossakowski KP, Killcrece G, Ruefle R, Zajicek M. Handbook for Computer Security Incident Response Teams (CSIRTs); 2003.
Wilson M, de Zafra DE, Pitcher SI, Tressler JD, Ippolito JB. NIST SP 800-816: Information technology security training requirements: a role- and performance-based model. National Institute of Standards and Technology; 2008.

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

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

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