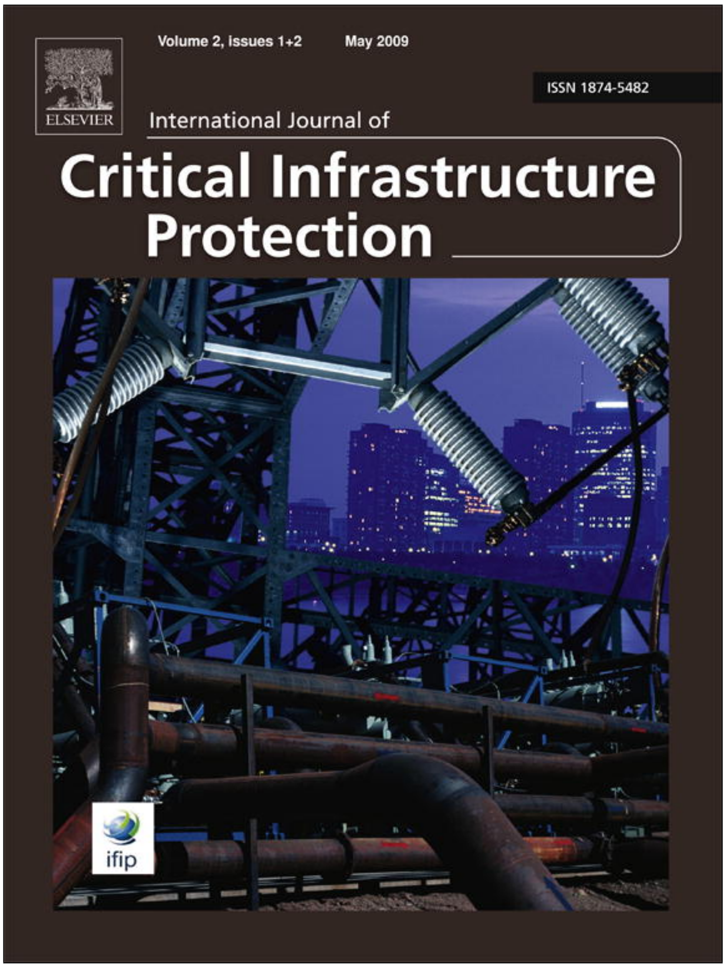
Volume 2, issues 1+2
May 2009
ISSN 1874-5482
ELSEVIER
International Journal of
Critical Infrastructure
Protection
ifip

available at www.sciencedirect.com

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

A framework for incident response management in the petroleum industry

Martin Gilje Jaatun[*], *Eirik Albrechtsen*[1], *Maria B. Line*[2], *Inger Anne Tøndel*[2], *Odd Helge Longva*[2]

SINTEF, NO-7465 Trondheim, Norway

ARTICLE INFO

Article history:
Received 6 November 2008
Received in revised form
30 January 2009
Accepted 24 February 2009

Keywords:
Incident response
Process control systems
Learning
Security culture

ABSTRACT

Incident response is the process of responding to and handling security-related incidents involving information and communications technology (ICT) infrastructure and data. Incident response has traditionally been reactive in nature, focusing mainly on technical issues. This paper presents the Incident Response Management (IRMA) method, which combines traditional incident response with proactive learning and socio-technical perspectives. The IRMA method is targeted at integrated operations within the petroleum industry, but it is also applicable to other industries that rely on process control systems.

1. Introduction

Oil and gas operations on the Norwegian Continental Shelf are increasingly incorporating the new concept of integrated operations (IO) [1]. Integrated operations uses real-time data and information and communications technology to create new work processes that result in improved and more efficient decisions with respect to reservoir exploitation, optimization of exploration and operation processes, and the long-term, managed development of fields and installations. The new ways of organizing work (e.g., remote control/support, integrated vendors, access to experts and cross-disciplinary decision-making) and the introduction of new technology have negative as well as positive impacts on risk [2].

The development of integrated operations has also led to a situation where the technologies used are changing from proprietary stand-alone systems to standardized PC-based systems integrated in networks. The reliance on commercial off-the-shelf (COTS) operating systems such as Microsoft Windows exposes operators to an increased number of information security vulnerabilities and, thus, a higher probability of incidents.

Increased networking between supervisory control and data acquisition (SCADA) systems and the general ICT infrastructure (including the Internet) also increases the overall vulnerability. In process operations on the Norwegian Continental Shelf, it has traditionally been assumed that SCADA systems are sheltered from threats emerging from public networks [3]. However, the integration of ICT and SCADA systems voids this assumption. There has been an increase in incidents related to SCADA systems [4], but the types of incidents and the nature of the attacks are

[*] *Corresponding address:* SINTEF ICT, NO-7465 Trondheim, Norway. Tel.: +47 73592951; fax: +47 73592930.
E-mail address: Martin.G.Jaatun@sintef.no (M.G. Jaatun).

[1] SINTEF Technology and Society.

[2] SINTEF ICT.

1874-5482/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2009.02.004

seldom reported and shared systematically [5]. The operating organization is also changing; integrated operations enable better utilization of expertise independent of geographical location, leading to more outsourcing and greater interaction between professionals [1].

The majority of incidents are relatively harmless, mainly causing disturbances, frustration and reduced efficiency. More harmful incidents may disable technical equipment such as sensors, computers and network connections, which interrupt production continuity. Severe incidents may lead to a chain of consequences, where the end result may be large economic losses, environmental damage and loss of life. Effective incident handling can minimize the consequences of an incident and, thereby, ensure business continuity. Consequently, systematic incident response approaches are needed to cope with the new challenges of ICT/SCADA incidents.

This paper presents a structured approach to incident management taking into account technological, human and organizational factors. The remainder of this paper is structured as follows: Section 2 presents the empirical background and motivation for developing the Incident Response Management (IRMA) method. Section 3 highlights the three phases of IRMA, with additional details presented in Section 4 through Section 6. Section 7 discusses the IRMA method and its implementation in industry. Section 8 concludes the paper.

2. Empirical background and motivation

This section presents the empirical foundations of our work, and shows how our results provide a motivation for developing a solution specifically for the petroleum industry.

2.1. *Method*

The development of the IRMA framework [6,7] for the petroleum industry has been based on a combination of different empirical sources [8]:

- Interview study with key personnel in the Norwegian petroleum industry.
- Case study of incident response management practices at an oil and gas installation in the North Sea.
- Risk and vulnerability assessment of infrastructure and work processes at a Norwegian offshore installation.
- Study of cultural aspects of information security using a tool for assessing information security culture at a particular installation.
- Workshop on information security and integrated operations.
- Workshop on the main findings of IRMA in the Norwegian petroleum industry.
- Workshops on modeling incident handling using system dynamics.

The preceding list shows that a combination of different qualitative social science methods was used to collect information about information security practices in the petroleum industry, which, to our knowledge, has not been the subject of much research effort. Qualitative research methods are useful due to their explorative nature. In general, qualitative research provides an understanding of social phenomena by proximate studies of the local contexts of a study [9]. By interacting closely with interview subjects, researchers obtain an understanding of the processes studied rather than only a description of the processes [10]. This has proved to be very useful in our study.

Qualitative research results should not be treated as generalized facts, but as an understanding of processes in the particular context of the study [9]. As a consequence, the findings presented in this paper are not necessarily generalized facts, but a representation of information security practices in the Norwegian petroleum industry.

2.2. *Findings*

This section presents the main findings from an empirical data gathering process that forms the foundation of the IRMA method.

2.2.1. *Interviews*

Nine interviews of personnel with knowledge and experience of information security in the petroleum industry were conducted by phone from March through June 2007. The interview subjects represented different actors in the Norwegian petroleum industry. Each interview, which involved one or two subjects, was conducted by two researchers. One researcher asked questions based on the prepared interview guide, while the other researcher recorded the information provided by the subjects. The interviews, which attempted to explore how incidents were handled in the Norwegian petroleum industry, were approached by examining how incidents were dealt with and how the subjects believed the best practice for incident response management should look like. The interviews attempted to foster a dialog between interviewers and interviewees, with the interview guide serving as a checklist for the coverage of topics. The interviews were, therefore, semi-structured. The information provided by the interviews was analyzed according to Miles and Huberman [11], i.e., the interview data was first coded and then categorized in matrices. The researchers then interpreted the matrices by searching for patterns in the data (see Albrechtsen et al. [12] for a detailed result matrix).

In general, the interviews demonstrated that the subjects experienced very few information security incidents that impacted on production. The subjects estimated that the period between incidents was one to two years in length.

The interviews showed that existing information security measures tend to focus mainly on technology. There is little coverage of organizational and human factors.

According to the interviewees, several plans exist in their organizations for different aspects of incident response with differing levels of detail. Most interviewees reported that a short, common plan documenting specific incident response management activities incorporated in their organizations was missing. Scenario training, which is widely used in other loss prevention areas in the industry, is seldom used to prepare for information security breaches. Furthermore, the interviews showed that individual awareness related to information security could be improved. In particular, there is room for enhancing employee knowledge and understanding of information security, especially among suppliers.

The learning phase after an incident was considered to be important by the interviewees. However, some interviewees were unsure if learning actually has any effect on future activities, and they feared that learning is quickly forgotten. Root causes are not always identified, discussions do not always involve ICT and process professionals, and lessons learned are not published.

The reporting systems at organizations are seldom tailored to information security and there are often many different reporting systems, which prevents uniform incident reporting. The interviews also indicated a lack of openness about real incidents. A change of focus was demanded to facilitate the transfer of information and expertise both within an organization and between organizations.

2.2.2. *North sea petroleum installation case study*

During the initial phases of the project, a case study of an offshore installation was performed. The effort comprised document studies, a series of individual interviews and group discussions. The case study gave an indication of how incident response was practiced in industry, but it did not provide any generalized findings.

Incident response management at the installation had the potential to be more systematic and planned – the current management approach appeared to be scattered and randomly constructed. The study showed that the only incident handling procedure involved dealing with virus infections; no other procedures for incident response were in place. Several activities for raising awareness were underway at the installation, some of them involving information security. Our findings showed that a virus infection in SCADA systems at the installation might take weeks to detect, even when the system was not operating normally.

The case study also showed that when incidents occurred, there was limited learning in the organization from the incidents. Furthermore, only moderate communication existed within the organization about real incidents.

2.2.3. *Risk and vulnerability assessment at an offshore installation*

To gain more insight into ICT-related risks involved in integrated operations, a risk and vulnerability assessment was performed with the work process of a daily production optimization of an offshore installation. Small-scale workshops with managers were conducted to identify incidents and assess their risk. This was done by employing a traditional approach to qualitative risk and vulnerability assessment by: (i) identifying unwanted incidents; (ii) identifying the causes of the incidents; (iii) identifying the consequences of the incidents; (iv) assessing the risk by plotting the incidents in a risk matrix; and (v) suggesting areas where risk reduction measures were required.

This assessment and the knowledge obtained by analyzing the coupling and dependencies of ICT systems, vulnerabilities, responsibilities, possible consequences of incidents, and incident detection and recovery gave a basis for further work. The most critical incidents identified in the risk assessment were:

- Operations center goes down.
- SCADA system is overwhelmed by network traffic.
- SCADA system goes down.
- Virus or worm infects the system from external sources.
- Lack of situational awareness for central control room operators.

The risk assessment study suggested several risk reduction measures relevant to incident response management: monitoring the stability of SCADA equipment when it is integrated with the ICT infrastructure; scanning and checking external PCs for viruses and malware prior to being connected to the technical or offshore networks; improving incident reporting and learning from incidents; ensuring that the responsibilities related to the technical network and the integration of ICT/SCADA systems are unambiguous and are monitored; improving awareness and the safety and security culture onshore and offshore; establishing and sustaining common risk assessment methodologies among the actors in the organizational network; and incorporating information security incidents in emergency response plans.

2.2.4. *Assessment of information security challenges at an installation*

Check-IT [13,14], a tool for assessing the organizational aspects of information security, was used to identify key challenges related to an integrated operations installation during a half-day workshop with ten managers and staff members. CheckIT incorporates a set of questions regarding organizational aspects of information security, including alternative answers. Although Check-IT is based on a questionnaire, the questions are so open-ended that they stimulate group discussion, which helps provide an assessment of the current status while contributing to improved awareness among the discussants.

The study showed that information security was not satisfactorily integrated in projects and new installations. Furthermore, suppliers and service providers were not adequately involved in incident planning, detection and learning. The identification of critical ICT systems was not satisfactorily performed in developing integration operations. Also, HAZOP analysis [15] (risk analysis) of ICT/SCADA systems was seldom performed.

Productivity goals were sometimes prioritized ahead of information security requirements. This was mainly because rules and procedures related to information security were ignored in situations with conflicting demands.

In general, the personnel on offshore installations had a low level of awareness related to information security (e.g., regarding spyware and viruses). This is partly explained by a lack of communication of information security issues within the organization. The lack of communication was also reflected by the unsatisfactory sharing of incident-related information between organizations in the industry sector.

2.2.5. *Workshop on information security and integrated operations*

A workshop on information security in integrated operations was arranged by the Norwegian Petroleum Directorate, Petroleum Safety Authority of Norway, Norwegian Oil Industry Association (OLF) and SINTEF in November 2006 [16]. The workshop sought to: (i) create awareness in information security related to integrated operations among different organizational groups (ICT, health, safety and environment (HSE), automation and operations); (ii) create a venue for experience transfer and networking; and (iii) identify possible measures. Approximately fifty participants from the petroleum industry, power supply industry, public agencies and research institutions attended the workshop.

Several information security issues pertaining to integrated operations were discussed, including incident response management. One result of the workshop was the identified need for information security metrics (key performance indicators) to evaluate whether the security level corresponds to policies and regulations, to evaluate the effects of measures and to integrate information security with other business areas. Such measurements would ideally engage a reference point such as the OLF Information Security Baseline Requirements (ISBR) [17].

We discovered that there was an overall lack of willingness to report incidents to the industry as a whole. As a consequence, it is important to study how to develop a reporting culture, how to communicate information about incidents, and how to develop best practices related to incident reporting and incident handling. Also, protocols for incident reporting, including obtaining feedback about incident reports, should be simplified.

The workshop results also indicated that training and preparedness for ICT-related incidents was lacking. Industry personnel have traditionally been trained on hazard and accident situation scenarios in other loss prevention areas. These scenarios rarely include ICT-related incidents. Furthermore, the workshop results identified a communication gap between different groups of offshore professionals (ICT, HSE and process). This is reflected by the fact that ICT protocols are rarely, if ever, adjusted to the offshore reality.

2.2.6. *Workshop on IRMA project findings*

In October 2007, a workshop was convened to discuss some of the main findings related to the IRMA Project in the offshore industry. Fifteen individuals from industry, government agencies, consulting companies and research institutions participated in the workshop.

One of the workshop recommendations was that the planning phase of incident management (see Section 4) must incorporate a proactive approach in order for an organization to be prepared to handle incidents and learn from them. In this proactive approach, performing risk analysis should be the foundation for providing decision support on how incident response management should be planned and performed.

In the detect and recover phase (see Section 5.1), it is important that individuals who discover or suspect an incident know whom to notify. Scenarios for possible incidents should be defined in order to discern which reporting channels are the most efficient for the incidents.,

Structures for incident reporting must be in place to facilitate learning from incidents. A software module for information security incidents is needed to support reporting. Contractors should fill out forms that are registered in an incident reporting tool by some other entity. It is always a challenge when different parts of an organization have different traditions for reporting incidents. For example, control room operators may not report incidents because they only handle the consequences of incidents, not the incidents themselves.

The workshop participants agreed with our recommendation that an information security forum be created for information sharing and transfer in the petroleum industry. However, they felt that industry entities should come up with the goals of such a forum and that different professions should be represented in the forum.

The workshop participants also discussed the relevance of historical data about incidents to IRMA in integrated operations. It was felt that new technology and new ways of organizing work could change the relevance of historical data.

2.2.7. *System dynamics workshops and the AMBASEC project*

In 2005, the IRMA and AMBASEC[3] teams organized two system dynamics workshops. The objective of the workshops was to obtain a deeper understanding of the risks involved when transitioning to integrated operations and the implications for incident handling during a transition. The processes included building a system dynamics model [18] for an integrated operations installation.

The results of the workshops and the collaboration between IRMA and AMBASEC teams are documented in two reports [19,20] and several publications [21–24]. One of the primary areas of discussion involved identifying key indicators to anticipate changes in system state over time.

In the first workshop, a preliminary version of a system dynamics model for the transition to integrated operations was established, and a set of stakeholders[4] and their influences on the possible outcomes for security in integrated operations were identified.

The second workshop focused on the implementation of a new work process in the Brage oilfield. Simulation runs using a system dynamics model in which the parameters were adjusted by industry experts (from Hydro) brought forward a number of hypotheses.

Although little hard data was available, the participants' knowledge of the general structures and behavior in their environment was sufficient for credible and understandable causal modeling. This is a crucial finding in high-threat environments because very little data is made available outside the secure environment of the firm.

[3] The AMBASEC(A Model-based Approach to Security Culture) Project at Agder University College (now the University of Agder) is funded by the Research Council of Norway. AMBASEC and IRMA have a formal collaborative relationship.

[4] Examples of stakeholders are the oil company (system owner), chief executive officer, platform chief, control room manager, incident response team manager, Petroleum Safety Authority, media, etc.

The following were the major findings from the workshops:

- Monitoring changes in risk should be given high priority when developing new industry policies related to incident reporting, creating computer security incident response teams (CSIRTs) and raising awareness.
- Transitions from traditional operations to integrated operations create vulnerabilities and new security issues. The impact of these vulnerabilities and security issues may depend on how well the organization can change its operating processes, train its staff and contractors, and gain acceptance for the transition.
- Successful implementation of collaborative arenas reinforces their effectiveness. On the other hand, limited success slows acceptance of the implementation, increases the resources required for subsequent rollouts, and could possibly derail projects.
- Incident reporting creates a knowledge base of incidents, which contributes to bringing on mature work processes, improves the rate of getting mature technology online, and reduces vulnerabilities, incidents and damage.

The state of information security in this domain is still relatively immature when compared to the state of safety. Numerous reporting systems exist for the safety realm, often mandated by law or, if not directly by law, by political pressure. We may not see well-functioning incident reporting systems for information security unless the government intervenes or threatens to do so. Another reason for the relatively slow adaptation of incident reporting systems may be the singular focus on information security as a technical issue. Non-security personnel are often kept out of the loop and are merely presented with a set of prescribed rules. This is a limited approach to user education. Users must be kept in the loop; only then will they see the importance of following the rules prescribed by information security specialists.

Simulation runs on the system dynamics model illustrate the potential for a successful incident reporting system. However, they also show that the potential exists for partial or even complete failure if important factors, such as investigation quality and motivation, are not handled well.

2.3. *Motivation*

The primary conclusion of this empirical study [8] is that the petroleum industry still does not consider information security to be a matter of sufficient importance. One consequence is that there currently are no systematic security incident handling schemes implemented in the petroleum industry. Incidents are treated in an ad hoc manner. For example, one report [3] notes that virus infections are left untreated for weeks.

Our research confirms that a deep sense of mistrust exists between process control engineers (who are in charge of SCADA systems) and ICT network administrators (who are in charge of office networks). The chasm between the two groups can be illustrated by a quote from an industry representative while conducting a vulnerability assessment: “We don’t have any ICT systems – we only have programmable logic”. This implies that implementing an established incident handling scheme would not work because it would be perceived as something emanating from the “ICT people”. In order for it to be successful, an incident response management scheme has to demonstrate that it is based on the realities faced by process control engineers.

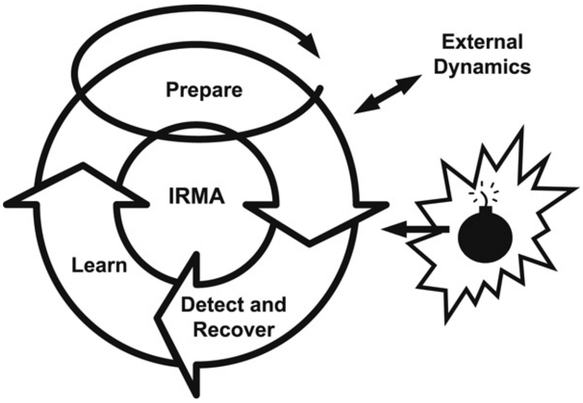

Fig. 1 – IRMA wheel.

3. IRMA phases

The IRMA method combines incident response as described in ISO/IEC TR 18044 [25] and NIST 800-61 [26] with increased emphasis on proactive preparation and reactive learning. The goal is to ensure that incident response procedures are continually improved, and that lessons learned are disseminated to the appropriate parts of the organization. We focus mainly on organizational and human factors, and less on technical solutions, which are covered well in the literature. Fig. 1 illustrates the phases of the IRMA method:

- **Prepare:** Plan and prepare for incident response.
- **Detect and recover:** Detect incidents and restore normal operations.
- **Learn:** Learn from incidents and how they are handled.

An organization is likely to spend most of its time in the *Prepare* phase. The *Detect and Recover* phase and the subsequent *Learn* phase are triggered by an incident (bomb in Fig. 1). Effective detection, recovery and learning from incidents are, however, based on preparation and proactive learning in the *Prepare* phase. Incident response does not operate in isolation within an organization; it has to adjust to external dynamics, both within and outside the organization. The *Learn* phase focuses on learning from single incidents. Learning is important because incident handling experience can be used to improve all phases of incident management. In the following, we discuss three phases of incident response management in more detail.

4. Prepare

In the *Prepare* phase, an organization readies itself to detect, handle and recover from security incidents and attacks. Other proactive tasks such as raising awareness are also part of the *Prepare* phase (see Fig. 2).

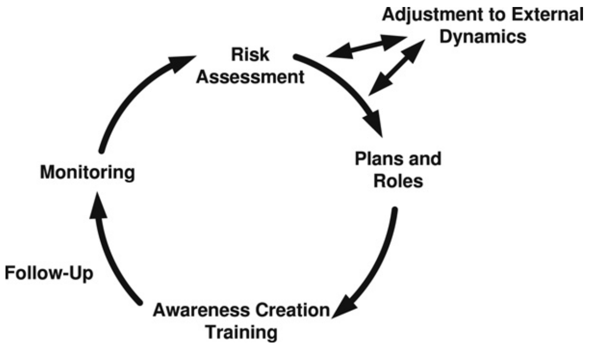

Fig. 2 – *Prepare* phase.

4.1. *Risk assessment*

A risk assessment entails identifying the most important unwanted incidents corresponding to an organization's assets, and determining the probability and consequences of each incident. Risks are often documented in a risk matrix (see, e.g., [3]). If the organization does not know which assets should be protected and from what, it is impossible to prioritize and design the appropriate security measures. This makes periodic risk assessment one of the most important activities related to information security.

To ensure that all relevant risks to SCADA/ICT systems are identified, it is important to engage the various actors who work with these systems in the risk assessment process. This includes representatives from ICT, process control (SCADA systems) and suppliers/contractors.

4.2. *Plans and documentation*

In an emergency situation, tacit knowledge can be the enemy, especially if the individual who has the knowledge is absent. This is why all routines, configurations and systems must be documented in sufficient detail during the *Prepare* phase and they should be continually updated as part of the "*Prepare* cycle".

Plans should exist for the complete incident handling process. In the case of system documentation, there should be a record of all equipment used in an installation. An updated network map showing how all the equipment is connected should be available at all times. For each possible target machine or system, there should be an understanding of whether downtime is acceptable or not.

Incident handlers should have ready access to an incident response toolkit. In addition to the documentation mentioned above, the kit should contain useful hardware and software tools such as cables, storage units, software for capturing images of infected systems, etc.

4.3. *Roles and responsibilities*

The following are the main responsibilities related to incident response:

- **Plan, prepare and train:** ICT security management.
- **Detect and alert:** Anyone who detects or suspects that an incident has occurred must raise an alert.
- **Receive alerts:** Someone or something must be designated to receive alerts. Everyone must know where to send alerts in any given situation.
- **Provide technical expertise:** Someone, either inside or outside the organization, must have technical system/security knowledge, and this knowledge must be available for incident recovery.
- **Handle incidents and recovery:** Someone must be responsible for leading the incident response efforts.
- **Make decisions:** Management must be on hand to make hard decisions.
- **Follow-up activities (including learning):** ICT security management.

Note that the responsibilities of suppliers concerning incidents involving their systems should be explicitly included in business contracts.

4.4. *Awareness creation and training*

The motivation for improving security awareness is twofold: (i) preventing incidents from happening, and (ii) improving the ability to detect and react to incidents. A general problem is that the reason for abnormal behavior of systems is not understood; as a consequence, many incidents are not detected, reported and handled. One of the biggest challenges related to information security incidents is that they are not detected by the users of the affected systems. Regular training exercises have a double impact: in addition to building and maintaining practical incident handling skills, the exercises remind users that abnormal system behavior may be the symptoms of an incident.

Building a security culture in an integrated operations setting comes with special challenges: shift work, multiple organizations and specialist communities (land and platform, ICT and process systems). Management involvement always increases the impact of an awareness campaign.

4.5. *Monitoring*

Feedback mechanisms are commonly used to systematically control a variety of business processes [27] (e.g., financial results, production efficiency, market reputation, quality management and HSE management). The field of safety management has a tradition of using performance indicators for persistent feedback control [28]. We suggest that similar indicators be implemented to measure incident response performance such as the time spent on each incident and the total number of incidents in a given period [29].

4.6. *External dynamics*

Incident response management does not operate in isolation from other parts of the organization and the organizational context. It is also influenced by the general information security management strategy. This influence goes both ways: information security management must be adjusted based on what is learned from incident response management, and vice versa. Both are influenced by information security regulations.

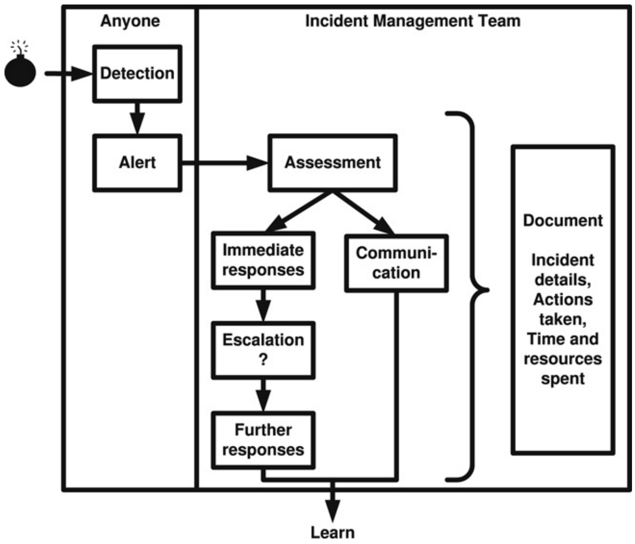

Fig. 3 – Overview of activities in the *Detect and Recover* phase.

5. Detect and recover

The *Detect and Recover* phase covers detecting, alerting, recovering and documenting incidents (Fig. 3). The recommendations made regarding incident detection and recovery are based on recognized publications from ISO/IEC [25], NIST [26] and TERENA [30].

5.1. *Detection and alerts*

Information security incidents are mainly detected in two ways [25]: by coincidence, where someone notices something unusual; or by routine use of technical security measures such as intrusion detection systems and virus scanners. The former is just as important as the latter, which means that every employee must be aware of the responsibility to send alerts whenever irregularities are discovered. Roles and responsibilities are already defined, so everyone knows whom to alert and who is responsible for handling an incident. It is valuable to draw knowledge from incident reporting experiences in the HSE domain [16].

5.2. *Assessment*

Every incident must be assessed with respect to its severity and the way forward. The following actions take place in an assessment [25]:

- **Acknowledge receipt:** The alerter is informed that incident handling has started.
- **Collect additional information:** Additional information is collected if necessary [26]. The goal is to state the severity and scope of incident, who should be involved in handling it, and whether it may affect production and/or safety. At this stage, false alarms are also identified.
- **Further alerts:** Additional personnel needed to handle the incident are alerted.

The ideal incident management team in integrated operations includes experts in ICT security as well as process control systems; this will lead to the best possible trade-offs between security and production. Suppliers may also have to be involved.

5.3. *Immediate response*

In a process control environment, it is imperative to keep systems running as long as possible. However, completely disconnecting the SCADA network from external ICT networks is a reasonable first action. Activating surveillance systems is also prudent as it helps achieve a better understanding of the incident.

During an incident, the best decisions are made when the organization has already prepared for the major types of incidents that can occur and has planned the actions that should be taken in response [5]. In particular, it is important to know which actions are applicable to different types of equipment. In duplicated configurations, infected units may be disconnected from the SCADA network for reconfiguration or restoration of a “known good” backup. This may not be possible for other types of equipment (e.g., components of a safety instrumented system (SIS)), where the removal of a component may trigger massive shutdowns due to integrated watchdog functions. In the latter case, incident handlers must attempt to isolate the infected equipment without disconnecting it or shutting it down. However, HSE always has priority on an offshore installation. Consequently, if HSE is threatened by continued operations, a shutdown is inevitable.

5.3.1. *Escalation*

Escalation requires assistance from outside the team. There are several reasons for an escalation:

- The team does not have the needed expertise.
- The team cannot get the incident under control.
- The incident is more serious than originally anticipated.
- Upper management decisions are necessary.

5.3.2. *Documentation and incident reporting*

Each incident must be documented with respect to what happened, which systems were affected, what damage occurred and how the incident was handled. False alarms should be documented as well.

The documentation of an incident starts when the alert is raised and continues through all steps in incident handling. Documentation must be made easy – otherwise, it will not be performed. The requisite tools should be readily available and easy to use, and personnel should be trained in using them. The actions taken could be described in an unstructured document or in a logbook [26]. However, it is preferable that a reporting form or template be used to ensure that all the important aspects are covered. The British Columbia Institute of Technology (BCIT) has created an excellent reporting form [31] for their (now defunct) Industrial Security Incident Database, which can be used as the basis for developing an installation-specific template.

The incident and the corresponding analysis must be documented in order to inform other actors about the incident and share best practices, as well as to keep a record of the incident that can be used to sustain learning from the incident, and to analyze the incident at a later time. Reporting

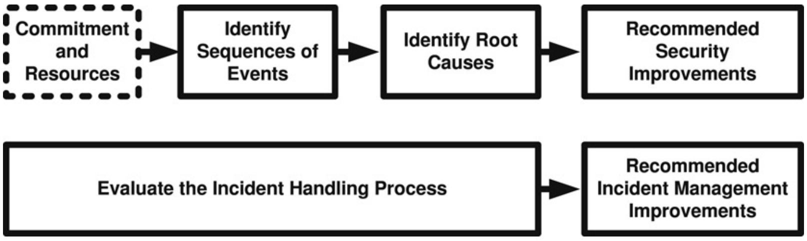
Commitment and Resources
Identify Sequences of Events
Identify Root Causes
Recommended Security Improvements
Evaluate the Incident Handling Process
Recommended Incident Management Improvements

Fig. 4 – Activities in incident learning.

procedures must ensure that this information reaches the designated individuals.

5.4. *Communication plan*

It may be necessary to inform selected individuals from within and outside the organization about the incident:

- Management personnel at different levels may need to comment about the incident in public. Obviously, they should not hear about the incident first from the media or other external sources.
- Individuals affected by the incident must understand what happened and why it happened.
- Media may be informed if the incident is of public interest.

5.5. *Recovering from incidents*

The immediate response to an incident seldom solves the entire problem; it mainly ensures that the incident is under control and limits the damage. Thereafter, actions must be taken to bring the affected systems back to normal operation, i.e., ensure that they are in a safe state and reconnected to external networks. Configuration changes and patches help reduce the vulnerability of the affected systems [25]. However, these should also be performed for other systems that could be targeted by similar attacks in the future. The incident may have led to malware being installed in a system that is hard to detect and remove. The clean up can be performed by reinstalling the operating system and applications or by using backup copies and recovery tools. Integrity checking tools may also be helpful [30]. Where possible, an image of each affected system should be extracted and secured for forensic analysis. If it is not possible to obtain a complete image, audit logs should be secured for later study.

5.6. *Learning from incidents*

When all systems are up and running, the entire experience with the incident should be explored to improve the preparedness of the organization. This is the focus of the *Learn* phase described in Section 6. The *Learn* phase should be initiated when the incident is still fresh in everybody's minds. But first, the individual who raised the alert must be briefed on how the incident was handled. This is an important aspect of raising awareness in incident management.

6. Learn

Cooke [32] describes an incident learning system as "the collection of organizational capabilities that enable the organization to extract useful information from incidents of all kinds and to use this information to improve organizational performance over time". The learning phase of IRMA focuses on learning from an actual incident [32] by following four steps in addition to the parallel activity of learning from the handling of the incident (see Fig. 4).

6.1. *Commitment and resources*

In order for learning to succeed, the organization must be prepared for it. The key issue is the extent of management commitment and the willingness to commit resources to facilitate learning from incidents.

As emphasized in the *Detect and Recover* phase, learning processes are dependent on the documentation of incidents. A structured accident analysis methodology can help identify the immediate and underlying causes, and should cover the organizational, technical and human factors issues. False alarms should also be included in the learning processes to improve incident detection accuracy.

6.2. *Identifying sequences of events using STEP*

The STEP method [33] is designed to conduct detailed analyses of incidents and accidents. It allows for a graphic presentation of the events involved in an incident or accident:

- Actors (i.e., persons or objects that affected the incident) are identified.
- Events that influenced the incident and how it was handled are identified and placed in the diagram according to the order in which they occurred.
- Relationships between the events (i.e., what caused them) are identified and incorporated in the diagram by drawing arrows to express the causal links.

6.3. *Identifying root causes and barriers*

A STEP diagram can be used to understand the root causes and consequences of weak points and security problems. This is done by identifying weak points in the incident description and representing them by triangles in the STEP diagram. A figure illustrating a STEP diagram can be found in [6].

In the example in Fig. 5, four weak points are identified:

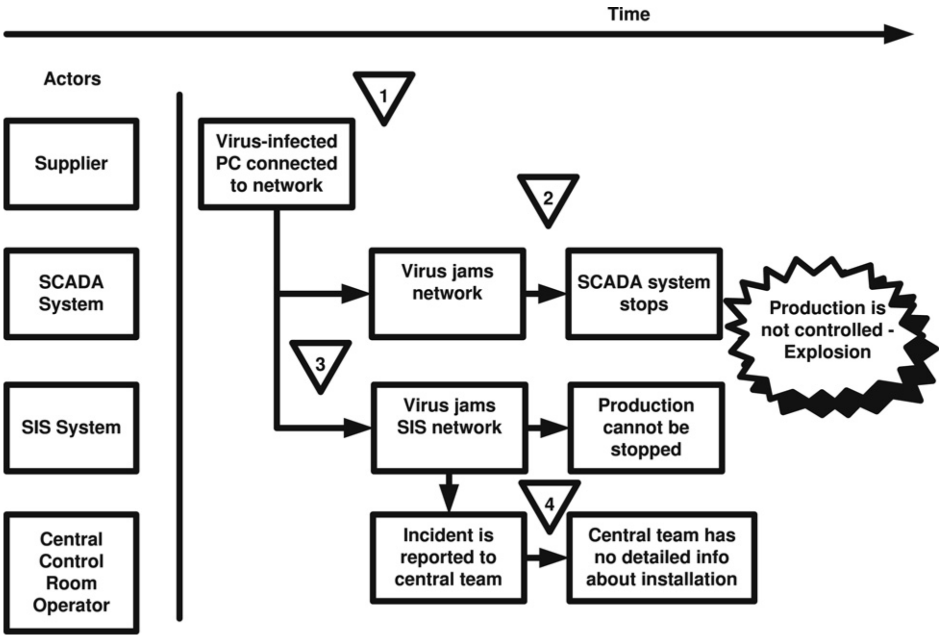
Time
Actors
Supplier
SCADA System
SIS System
Central Control Room Operator
1
Virus-infected PC connected to network
2
Virus jams network
SCADA system stops
Production is not controlled - Explosion
3
Virus jams SIS network
Production cannot be stopped
4
Incident is reported to central team
Central team has no detailed info about installation

Fig. 5 – STEP diagram of a virus attack.

(1) Personal computers are not scanned before connecting them to the network.
(2) The latest patches are not deployed on systems connected to the network, increasing the likelihood of a successful virus attack.
(3) A safety instrumented system (SIS) is integrated with the SCADA system, making it possible to jam the SIS via the SCADA system.
(4) The central technical team does not have detailed knowledge of the local SCADA system and is unable to shut down production.

The weak points are then assessed by performing a barrier analysis, which includes the recommended countermeasures (see, e.g., Johnsen et al. [34]). The barriers may be technical, human or organizational in nature.

6.4. *Recommend security improvements*

The accident analysis, identified weak points and suggested barriers provide the foundation for making security recommendations. It is important to prioritize the suggested actions based on a cost/benefit analysis and to explicitly assign the responsibility for performing the actions.

6.5. *Evaluate the incident handling process*

The *Learn* phase also includes an evaluation of the incident handling process itself. Experience from the incident handling process should be used to improve the management of future incidents. Ideally, all relevant parties should be involved soon after an incident has been handled, when the information is still fresh in their minds [35]. Factors to consider include [25]:

- Did the incident management plan work as intended?
- Were all relevant actors involved at the right time?
- Are there procedures or tools that would have aided incident detection?
- Are there procedures or tools that would have aided the recovery process?
- Were the communications about the incident to relevant parties effective throughout the detection and recovery process?

7. Discussion

This paper has described a framework for incident response management in the North Sea petroleum industry. Several other articles and standards describe approaches for incident handling (see, e.g., [25,26,36,37,44,45]). Our approach follows the same basic ideas, but differs from them in three important ways: (i) it emphasizes socio-technological aspects covering the interplay between individuals, technology and organizations; (ii) it emphasizes reactive as well as proactive learning; and (iii) it covers ICT/SCADA systems used in the petroleum industry.

The former two contributions are discussed in this section. First, we discuss why a socio-technical approach is necessary for incident handling in integrated operations in the petroleum industry. Next, we discuss why learning from incidents is important but also challenging.

7.1. *Socio-technical approach to incident handling*

A socio-technical information security system [38] is created by the interplay of the elements of different information security processes. Traditional incident handling [25,37,26] has mainly focused on the technical aspects of incident response. The framework described in this paper also focuses on individual behavior and organizational processes. This is discerned from the emphasis on organizational roles, awareness training, risk assessment processes and follow-up activities in the *Prepare* phase; roles in the *Detect and Recover* phase; and the involvement of actors in learning activities. In general, the information security domain has failed to focus on socio-technical approaches [39,40]. Our approach to incident response contributes to a wider perspective on information security management because it considers information security as a socio-technical system.

The *Prepare* phase described in Section 4 shows how technological solutions, individuals and organizational structures and processes can be primed to discover and deal with incidents as well as prevent incidents from happening. These assets are important to developing and maintaining a socio-technical incident handling system and to make it more proactive in nature.

The learning processes suggested in this paper emphasize organizational learning, i.e., changes in the organizational interplay between individuals and groups, including modifications of organizational processes and structures [41]. This approach implies that incident learning should emphasize single-loop and double-loop learning [41], i.e., response based on the difference between expected and obtained outcomes (single-loop); and to be able to question and change governing variables related to technology, organization and human factors that lead to the outcome (double-loop). The latter is necessary for socio-technical long-term effects whereas the former is more concerned with technological solutions (e.g., fire-fighting).

Although our empirical findings show that there are few computer security incidents in the petroleum industry, the same findings indicate that systematic analyses of the few incidents that are detected are rarely carried out. Moreover, organizational learning with respect to these incidents is seldom performed [6]. The root causes of incidents are not always documented and there is a focus on technical issues when studying incidents. Organizational and human factors issues are rarely explored. The presence of different professional disciplines poses challenges to implementing learning in an organization because different roles and positions should be involved in incident learning processes.

In our interactions with petroleum industry personnel, we discerned a communication gap between ICT staff and process control staff. These groups have different interests and have traditionally not had to cooperate. However, the increased use and interconnectivity of ICT systems has resulted in increased information security threats to process control systems. The two groups have to cooperate in order to efficiently handle security incidents in SCADA systems. The communication gap between the two groups is taken into account in the IRMA method. Different risk perceptions and situational understanding are best approached by discourse-based strategies [42,43], where the involved actors meet and discuss different viewpoints with the goal of arriving at a common understanding.

7.2. *Learning from incidents*

Incidents are unwanted occurrences. At the same time, they represent invitations to learn about risk and vulnerabilities in the socio-technical systems that are supposed to control these weaknesses. The experience gained from incidents and incident handling processes can be used by an organization to improve its overall security performance. Learning from incidents should thus be a planned part of incident handling and the necessary resources for this activity must be allocated. The incident response management framework proposed in this paper describes such a learning approach, which is both reactive and proactive in nature. It is reactive in the sense that the organization learns from actual incidents and incident handling, and is proactive in the sense that the incident handling system is adjusted based on lessons learned internally and in the context of the organization. Based on the premise of incident response management as a socio-technical system, the learning process emphasizes organizational learning.

In general, there are two obstacles to organizational learning: embarrassing and threatening issues [41]. Information security incidents may be embarrassing (e.g., virus infections caused by unauthorized or unsafe use of the Internet) and threatening in the sense that the incidents are considered to be confidential. These characteristics create individual and organizational behavior that is counterproductive when it comes to learning from unwanted incidents. These defensive routines may, in fact, be the reason that our empirical research indicated relatively few incidents occurred in the petroleum industry. However, the empirical study of incident handling in the petroleum industry showed that several individuals called for more openness about unwanted incidents to enhance learning within an organization as well as across organizations, both of which require much more communication than currently exists.

8. Conclusions

A systematic approach for incident response and learning from incidents is important to the petroleum industry because of the recent trend towards integrated operations. Although the industry sector experiences few incidents at this time, being unprepared for higher risk factors and new and unforeseen threats will be very costly in an industry that depends on virtually no downtime for its production systems.

Our study indicates a weak emphasis on information security in the industry as a whole. Since ICT incident response management is a subset of information security management, it is necessary not only to improve incident response in the petroleum industry, but also general information security functions (technological, human and administrative) in order to improve the overall information security performance. This paper focuses on improving ICT incident response, which is just one component of a general information security strategy. Other components should also be considered, but these are outside the scope of the paper.

The IRMA method is specifically developed for the petroleum industry. Nevertheless, it is applicable to other industries that rely on process control systems and integrated/remote operations. The innovative aspect of the method for incident handling is its proactive nature and the combined focus on technological, organizational and human aspects.

Oil and gas production requires the cooperation of multiple organizations, including operators, suppliers and regulatory entities. This must be taken into account when implementing IRMA. It is not appropriate to only consider the operator because supplier cooperation is indispensable when preparing for, detecting, recovering and learning from incidents. We also recommend that IRMA be implemented for installations rather than organizations; this is because adapting incident response to the context of an installation is very efficient. Finally, a successful implementation of IRMA requires resources. It is, therefore, important that management be convinced of the benefits of incident management and be willing to allocate the necessary resources.

Acknowledgements

This research was undertaken under the IRMA Project (2005–2007), which was supported by the Norwegian Research Council and the Norwegian Oil Industry Association. We wish to thank our colleagues, Stig Ole Johnsen and Irene Wærø, for their contributions to the IRMA Project. We also wish to thank the numerous industry representatives who participated in our workshops and interviews.

REFERENCES

[1] Integrated operations on NCS, 2004. http://www.olf.no/?22894.pdf.

[2] T.O. Grøtan, E. Albrechtsen, R. Rosness, E. Bjerkebæk, The influence on organizational accident risk by integrated operations in the petroleum industry, in: Proceedings of Working on Safety, 2008.

[3] S.O. Johnsen, R. Ask, R. Røisli, Reducing risk in oil and gas production operations, in: E. Goetz, S. Shenoi (Eds.), First Annual IFIP WG 11.10 International Conference, Critical Infrastructure Protection, 2007.

[4] Hackers have attacked foreign utilities, CIA Analyst Says. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html.

[5] K. Stouffer, J. Falco, K. Kent, Guide to scada and industrial control systems security (draft), Tech. Rep. Special Publication 800-82, NIST, 2006.

[6] M.G. Jaatun, S.O. Johnsen, M.B. Line, O.H. Longva, I.A. Tøndel, E. Albrechtsen, I. Wærø, Incident response management in the oil and gas industry, Tech. Rep. SINTEF A4086, SINTEF ICT, 2007. URL http://www.sintef.no/upload/10977/20071212_IRMA_Rapport.pdf.

[7] M.B. Line, E. Albrechtsen, M.G. Jaatun, I.A. Tøndel, S.O. Johnsen, O.H. Longva, I. Wærø, A structured approach to incident response management in the oil and gas industry, in: Proceedings of the 3rd International Workshop on Critical Information Infrastructures Security, CRITIS'08, 2008.

[8] M.G. Jaatun, E. Albrechtsen, M.B. Line, S.O. Johnsen, I. Wærø, O.H. Longva, I.A. Tøndel, A study of information security practice in a critical infrastructure application, in: Autonomic and Trusted Computing, 2008, pp. 527–539.

[9] T. Thagaard, Systematikk og innlevelse: en innfring i kvalitativ metode [Systematics and Isight: Introduction to Qalitative Methods], Fagbokforlaget, Bergen, 2003 (in Norwegian).

[10] S. Kvale, Det kvalitative forskningsintervju. [Interviews: An Introduction to Qualitative Research Interviewing], Ad Notam Gyldendal, 1997 (in Norwegian).

[11] M. Miles, A. Huberman, Qualitative Data Analysis: An Expanded Sourcebook, Sage, Thousand Oaks, CA, 1994.

[12] E. Albrechtsen, S.O. Johnsen, M.B. Line, O.H. Longva, I. Wærø, Irma – Interviews on incident response in the oil and gas industry, Tech. Rep. MEMO, SINTEF, November 22 2007.

[13] Y. Nordby, C.W. Hansen, Informasjonssikkerhet atferd, holdninger og kultur. [Information security behaviour, awareness and culture], Tech. Rep. ROSS(NTNU200504), NTNU-rapport, 2005 (in Norwegian).

[14] S.O. Johnsen, et al., CheckIT – A program to measure and improve information security and safety culture, International Journal of Performability Engineering 3 (1 Part II) (2007) 174–186.

[15] Hazard and operability studies (HAZOP studies) – Application guide, IEC Std. 61882, 2001.

[16] M.G. Jaatun (red.), Arbeidsseminar om IKT-sikkerhet i Integrerte Operasjoner: Referat, Tech. Rep., SINTEF, 2007 (in Norwegian only). URL: http://www.sintef.no/upload/10977/sluttrapport.pdf.

[17] Information Security Baseline Requirements, OLF Guideline 104, 2007. http://www.olf.no/hms/retningslinjer/?50182.pdf.

[18] System Dynamcs Home Page. URL: http://systemdynamics.org/.

[19] E. Rich, D. Andersen, G.P. Richardson, OLF IRMA-AMBASEC group modeling report I, Tech. Rep., University at Albany, 2006.

[20] E. Rich, D. Andersen, G.P. Richardson, OLF IRMA-AMBASEC group modeling report II, Tech. Rep., University at Albany, 2006.

[21] E. Rich, J.J. Gonzalez, Maintaining security and safety in high-threat in e-operations transitions, in: Proceedings of 39th HICSS, 2006.

[22] E. Rich, F.O. Sveen, Y. Qian, S.A. Hillen, J. Radianti, J.J. Gonzalez, Emergent vulnerability in integrated operations: A proactive simulation study of risk and organizational learning, in: Proceedings of 40th HICSS, 2007.

[23] F.O. Sveen, E. Rich, M. Jager, Overcoming organizational challenges to secure knowledge management, Information Systems Frontiers 9 (5) (2007) 481–492.

[24] F.O. Sveen, J.M. Sarriegi, E. Rich, J.J. Gonzalez, Toward viable information security reporting systems, Information Management & Computer Security 15 (5) (2007) 408–419.

[25] Information technology – Security techniques – Information security incident management, Tech. Rep. TR 18044:2004, ISO/IEC, 2004.

[26] T. Grance, K. Kent, B. Kim, Computer security incident handling guide, Tech. Rep. Special Publication 800-61, NIST, 2006.

[27] M. Hammer, J.A. Champy, Re-engineering the Corporation: A Manifesto for Business Revolution, Harper Collins, 1993.

[28] U. Kjellén, Prevention of Accidents Through Experience Feedback, Taylor and Francis, 2000.

[29] M.B. Line, E. Albrechtsen, S.O. Johnsen, O.H. Longva, S. Hillen, Monitoring of incident response management performance, in: International Conference on IT-Incident Management and IT-Forensics, IMF, Stuttgart, Germany, 2006.

[30] A. Cormack, et al. TRANSITS course material for training of network security incident teams staff, Tech. Rep., TERENA, 2005.

[31] Industrial Security Incident Database Reporting Form. http://www.bcit.ca/files/appliedresearch/pdf/security/isid_form.pdf.

[32] D.L. Cooke, Learning from incidents, in: Proceedings of the 21st System Dynamics Conference, 2003.

[33] K. Hendrick, L. Benner, Investigating Accidents with STEP, CRC Press, 1986.

[34] S.O. Johnsen, C. Bjørkli, T. Steiro, H. Fartum, H. Haukenes, J. Ramberg, J. Skriver, CRIOP: A scenario method for crisis intervention and operability analysis, Tech. Rep. STF38 A03424, SINTEF, 2003.

[35] A. Birk, T. Dingsoyr, T. Stalhane, Postmortem: Never leave a project without it, Software, IEEE 19 (3) (2002) 43–45.

[36] Information security management systems – Requirements, ISO/IEC Std. 27001, 2005.

[37] Information technology – Code of practice for information security management, ISO/IEC Std. 27002, 2005.

[38] E. Albrechtsen, Friend or foe? Information security management of employees, Ph.D. Thesis, NTNU, 2008:101, 2008.

[39] G. Dhillon, J. Backhouse, Current directions in is security research: Towards socio-organizational perspectives, Information Systems Journal 11(2) (2001) 127–153.

[40] M.T. Siponen, H. Oinas-Kukkonen, A review of information security issues and respective research contributions, SIGMIS Database 38 (1) (2007) 60–80.

[41] C. Argyris, D.A. Schön, Organisational Learning: A Theory of Action Perspective, Addison-Wesley, 1978.

[42] A. Klinke, O. Renn, A new approach to risk evaluation and management: Risk-based, precaution-based and discourse-based strategies, Risk Analysis 22(6) (2002) 1071–1094.

[43] P. Slovic, The Perception of Risk, Earthscan, London, 2000.

[44] S. Mitropoulos, D. Patsos, C. Douligeris, On Incident Handling and Response: A state-of-the-art approach, Computers & Security 25 (5) (2006) 351–370.

[45] D. Forte, Security standardization in incident management: the ITIL approach, Network Security 2007 (1) (2007) 14–16.