Examining the suitability of industrial safety management approaches for information security incident management

Maria B. Line[1] and Eirik Albrechtsen[2]
[1]Department of Telematics
[2]Department of Industrial Economics and Technology Management
Norwegian University of Science and Technology
N-7491 Trondheim

Abstract

Purpose
This paper discusses whether recent theoretical and practical approaches within industrial safety management might be applicable to, and solve challenges experienced in, the field of information security, specifically related to incident management.

Design/methodology/approach
Literature review.

Findings
Principles, research, and experiences on the issues of plans, training, and learning in the context of industrial safety management would be suitable for adoption into the field of information security incident management and aid in addressing current challenges.

Research limitations/implications (if applicable)
There are a number of reasons why approaches from industrial safety management have something to offer to information security incident management: the former field is more mature and has longer traditions, there is more organizational research on industrial safety issues than on information security issues so far, individual awareness is higher for industrial safety risks, and worker participation in systematic industrial safety work is ensured by law. More organizational research on information security issues and continuous strengthening of individual security awareness would push information security to further maturity levels where current challenges are solved.

Practical implications (if applicable)
This paper shows that the field of information security incident management would gain from closer collaborations with industrial safety management, both in research and in practical loss prevention in organizations. The ideas discussed in this paper form a basis for further research on practical implementations and case studies.

Originality/value
The main audience of this paper includes information security researchers and practitioners, as they will find inspirational theories and experiences to bring into their daily work and future projects.

1 Introduction

Information and communication technologies (ICT) are facing the trend of larger connectivity and increased integration. Dependability on ICT systems is increasing as well; for individuals, organizations, and for society at large. Hence, attacks and/or malfunctioning of ICT systems may have serious consequences for business, in particular societal critical infrastructures. Although many different preventive measures exist, and usually are in place, to protect against information security incidents, such incidents still happen. The number and types of threats are ever changing, creating challenges for protection in such a dynamic risk picture. An efficient incident management process – the ability to appropriately prepare for, and respond to, information security incidents – is thus important to maintain the functioning of systems (ISO/IEC, 2011).

Compared to industrial safety management, information security management is a relatively young field of both practice and research. Albrechtsen and Hovden (2007) describe the development of industrial safety in five stages and compare this with the development of information security management. The two first stages of industrial safety management are about accident prevention by technical barriers and prevention of human errors, while the third stage is the development and application of technical-administrative industrial safety management systems with a focus on documented requirements for organizational behaviour; compliance to rules; auditing and control of irregularities. The fourth stage is the inclusion of ideas from social sciences into industrial safety and the use of leadership and responsibilities, organizational aspects, and organizational culture as a means of improving industrial safety. Finally, the fifth stage focuses on adapting to challenges of dynamic changes in technologies and threats. Albrechtsen and Hovden (2007) claim that traditionally, the field of information security has been preoccupied by the first three stages. However, during the last decade it entered the fourth stage by an increased attention to individual awareness and behavior (Stanton et al., 2005; Möller et al., 2011; Shropshire et al., 2015) as well as the concept of information security culture (Ruighaver et al., 2007; van Niekerk and von Solms, 2010; da Veiga, 2015). In order for information security to reach the fifth step, we claim that there is a need to investigate adaptive management strategies.

In this paper we elaborate what information security incident management can learn from recent industrial safety management approaches in order to deal with expected and unexpected events. Particularly, adaptive industrial safety management approaches are considered. Organizations will need to handle events that were unforeseen and thus not planned for, or they will face situations of expected or unexpected events where there are no formal structures (rules, procedures, technology) that are suited to the situation. To gain control in such situations, adaptation is required. This paper answers the following research question:

What industrial safety management approaches and techniques could be adapted to improve information security incident management?

This question is addressed by a discussion of how industrial safety theories offer new approaches and mind-sets to improve ways of organizing and performing information security incident management.

This paper is structured as follows. Section 2 introduces information security incident management and describes major challenges in current practice. Section 3 compares information security to the field of industrial safety, while Section 4 presents adaptive management approaches for dealing with both expected and unexpected events. Specific theories and techniques from industrial safety management that would address current challenges in information security incident management are discussed in Section 5, before concluding remarks are made in Section 6.

2 Information security incident management

The ISO/IEC 27035 standard on information security incident management (ISO/IEC, 2011) describes the complete incident management process. It complements the requirements stated by ISO/IEC 27001 (ISO/IEC, 2013). The incident management process comprises five phases as illustrated by Figure 1:

- Plan and prepare,
- Detection and reporting,
- Assessment and decision,
- Responses, and
- Lessons learnt.

The first phase runs continuously, as opposed to the next four, which are triggered by the occurrence of an incident. *Plan and prepare* includes activities such as establishing a dedicated response team, defining roles and responsibilities, documenting procedures, as well as training of personnel and awareness raising activities regarding incident management throughout the organization. *Detection and reporting* is the first operational phase and involves detection of what might be an incident and reporting into an incident tracking system. Then it should be decided what kind of response is needed to cope with the registered event, and this activity belongs to the *Assessment and decision* phase. The *Responses* phase describes the actions taken to resolve the incident and prevent further consequences, restore systems, collect electronic evidence and possibly escalate to crisis handling. The final phase, *Lessons learned,* is when the team analyzes whether the incident management scheme worked satisfactorily and considers whether any improvements are needed on any level: the scheme, policies, procedures, security mechanisms, or other. The improvements are then implemented as part of the continuously running *Plan and prepare* phase.

A number of guidelines describe best practice and suggest activities for effective and efficient incident management. NIST (Cichonski et al., 2011), ITIL (Brewster et al., 2012), ENISA (ENISA, 2008 and 2010), SANS (Kral, 2011), and ISACA (ISACA, 2012) are among the most well known providers of such guidelines in addition to ISO/IEC. They have a number of similarities; for example they have all chosen to divide the incident management process into a set of phases. Most of them describe a preparation phase, where an incident management capability is built. Further, all have phases for detection, analysis and incident responses, but the structure of these phases varies. All of them highlight activities related to lessons learned, even though not all describe a separate phase for this. It is worth noting that the guidelines presented by NIST, ITIL, etc., are developed by single organizations, whereas the ISO/IEC standard is based on

international consensus. The development and approval of the ISO/IEC standards are extensive processes with several contributors worldwide and should therefore be widely accepted. In addition to the standards and guidelines, there is a large body of academic literature addressing incident management.

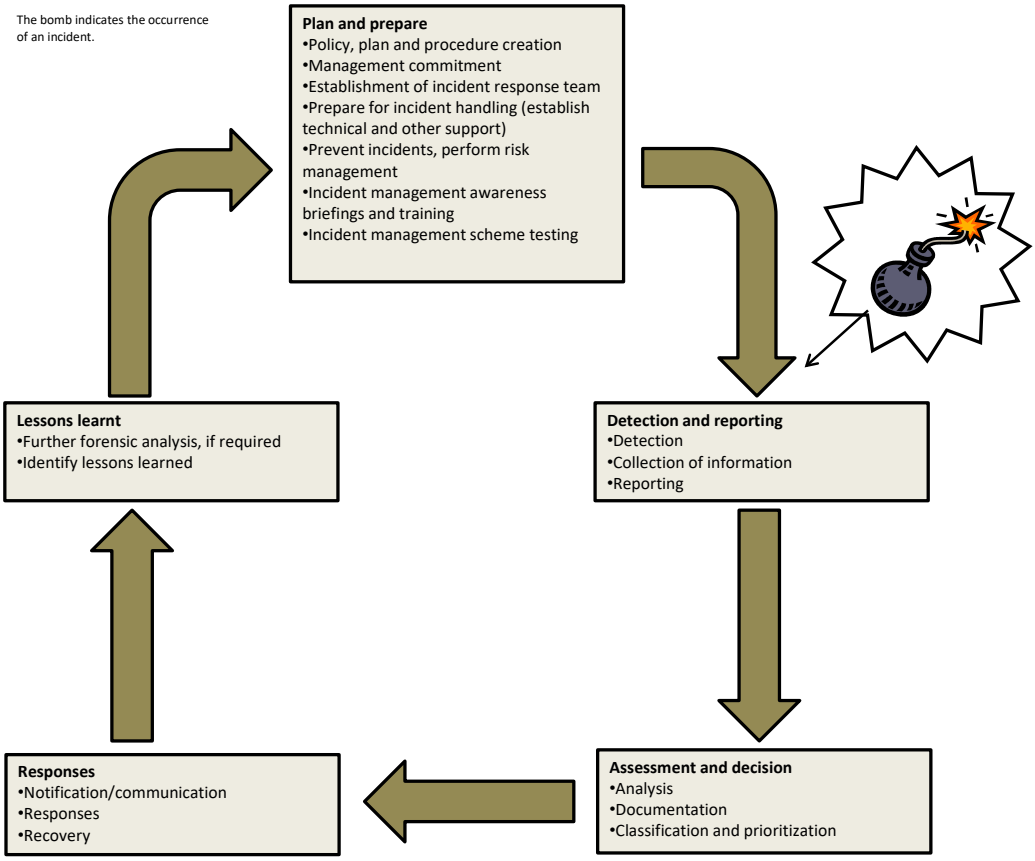

Figure 1: The complete information security incident management process (ISO/IEC 27035)

Tøndel et al. (2014) performed a systematic literature review of empirical studies on information security incident management. These empirical studies were based on data collection in a number of organizations from different industries. Tøndel et al. compared this empirical research with the ISO/IEC 27035 and concluded that current practices and experiences align quite well with this. Besides, they identified a number of challenges that seemed to be present in several of the studies included in their review:

Creating adequate plans for incident handling: Having a simple, short and common plan for incident management was recommended by Jaatun et al. (2009) and Cusick and Ma (2010). This was considered an advantage when present and a need when not present. Without it, the approach to incident management could appear scattered and randomly structured (Jaatun et al., 2009). A lack of plans was reported by Line et al. (2014) to hinder training activities, as a plan was perceived as needed as a basis for training.

Gaining senior management commitment: A low level of awareness among upper management of the importance of cyber security training drills could be explained by a lack of systematic reporting of incidents, according to Jaatun et al. (2009). Rhee et al.

(2012) documented an optimistic bias among senior management; if they do not perceive incidents as a problem, they are less likely to put priorities into incident management.

Involving all employees: Information security awareness is not only an issue for a response team, as current trends show that attacks now target employees, not just technical systems. This requires all employees to be alert and able to detect and report incidents (Hove et al., 2014). ISO/IEC 27035 recommends training activities for the response team, while others, i.e. Wilson et al. (2008), recommend basic security training for all employees. Although automatic detection tools are widely implemented, manual reporting of incidents is still crucial to most organizations (Hove et al., 2014; Koivunen, 2010; Line et al., 2014; Metzger et al., 2011; Werlinger et al., 2010). However, Koivunen (2010) observed that the victims could just as well be the last ones to learn about security incidents, as the incidents referred to in this study were discovered by external parties. Furthermore, according to Hove et al. (2014) it is almost impossible to detect incidents stemming from disloyal employees.

Coping with the existing tools and their lack of usability: Current technical tools suffer from a high number of false positives, the need for precise information that is rarely documented, and a lack of usability (Werlinger, 2010, 2008; Metzger et al., 2011).

Quality of incident registrations: Low-impact incidents tend to remain unregistered, although organizations have systems in place for incident tracking (Cusick and Ma, 2010, Kurowski and Frings, 2011). Cusick and Ma (2010) stressed the challenge of engineers just including a minimum amount of data in such registrations. Existing reporting tools used for Health, Safety and Environment (HSE) incidents were poorly suited to reporting of cyber security incidents (Jaatun et al., 2009).

Collaboration among teams and across disciplines: Jaatun et al. (2009) identified a great deal of mistrust between traditional process control engineers and IT personnel, even though the integrated operations were highly dependent on IT systems. It even seemed that some control system engineers refused to acknowledge that their systems contained vital IT components. Furthermore, collaboration between technical staff and business staff is reported to be challenging, in addition to communication with externals (Hove et al., 2014; Ahmad et al., 2012; Werlinger et al., 2010). Several organizations do not put information security training high up on their agenda (Line et al., 2014), even though experienced incident handlers are considered much more valuable in an emergency situation than plans and procedures (Hove et al., 2014). Ensuring realistic training scenarios and that the training actually provides value in real situations were however identified as challenging. Other pressing tasks are prioritized.

Practicing incident management in outsourcing scenarios: Hove et al. (2014) pointed out the need for defining responsibilities, especially in organizations where IT operations are outsourced or several parties are included in operations and incident response. In complex systems it may be difficult to define such responsibilities, and it may also be difficult to know where a specific incident actually originates and thus determine who is responsible for handling it.

Motivating learning activities: Learning from incidents is important, but some challenges arise due to inadequate involvement of suppliers (Jaatun et al., 2009). Furthermore, the post-incident review process tends to focus more on incidents with high impact than so-called “high learning” incidents that have a potential for being more useful from a learning perspective, according to Ahmad et al. (2012). Learning from low-impact incidents seems not to be given priority (Hove et al., 2014; Ahmad et al., 2012).

Sharing lessons learnt: Scholl and Mangold (2011) claimed that a "well-developed incident response process should be a driver for continuous improvement of enterprise security" (p. 1) and that attending to small security events and early warnings can prevent major security disasters. Ahmad et al. (2012) found that information about incidents seems to be available to a selected few only, even though other parties could find this information useful.

3 Information security management and industrial safety management

Loss prevention is the main purpose of both information security and industrial safety. There are thus many similarities, but still some differences between the two areas. Nevertheless, since both aim at a systematic prevention of loss there should be a potential for learning from each other. One obvious difference is what they aim to protect. Information security is about preserving the confidentiality, integrity, and availability of information, while industrial safety is concerned with controlling hazards of any kind that may lead to losses (humans, material, environment) in the organization. Furthermore, industrial safety and information security have different terminologies. A safety breach may be denoted a *fault* or an *accident*, while security breaches are usually denoted *incidents*. A safety *hazard* may correspond to a security *threat*. Furthermore, there are differences between the two areas concerning the risk picture and management approaches.

Although security efforts, such as protection against competing tribes, have existed since the dawn of time, the first *computer security* efforts happened in the 1960s in the U.S. military sector by the development of time-sharing computer systems (MacKenzie & Pottinger, 1997). Safety, which concerns protection of human lives and health, has been an important part of society as old as civilization. Systematic industrial safety management approaches have existed since the 19th century (Hale & Hovden, 1998). Hence, in a historical perspective, when it comes to systematic approaches, industrial safety is a more mature field than information security. The different historical developments in the two fields have resulted in different views on risk and risk mitigation. Information security is dominated by a focus on technological solutions and problems along with regulation and control of organizational affairs (Albrechtsen, 2008). Industrial safety has, on the other hand, through history developed an integrated technical, human, and organizational approach (Hale & Hovden, 1998).

Albrechtsen and Hovden (2007) describe the development of industrial safety management in five steps:

1. The first step resembled an industrial safety engineering approach where protective measures related to uncontrolled energy release are the main focus. The main means are physical and technical barriers, protective equipment, and automation removing people from danger zones.
2. Then, the focus shifted to the challenge of human errors as the triggering factor in accident processes. In addition to discipline and training as measures, efforts were made on improving the man-machine interface and adaptation.
3. In the third step, technical-administrative industrial safety management systems were developed from the same ideas as quality management with a focus on documentation, auditing, and control of irregularities. Monitoring by key performance indicators was also an important feature of this approach.
4. An approach to industrial safety research and practices based on ideas from the social sciences followed in the fourth step. Main topics on this agenda were leadership and responsibilities, organizational aspects of safety work, and taxonomies of safety culture and climate as means for improved safety.
5. The fifth and most recent step resembles an approach for handling and adapting to the industrial safety challenges of change: changing global economy: fast pace in technology development and the appearance of new threats and hazards, e.g. management approaches aiming at developing and maintaining resilience in systems.

A comparison of the younger field of information security management with these five steps shows that information security is mainly applying the same principles as in steps 1-3. During the last decade there have been more approaches within step 4, related to for example information security culture (i.e. Ruighaver et al., 2007; van Niekerk and von Solms, 2010). Johnsen et al. (2009) and Johnsen (2012) have made the first initial attempts to apply adaptive industrial safety management principles on issues related to information security by discussing how safety and security of control systems can be dealt with. The field of industrial safety is more mature when it comes to applying social science theories (step 4 and 5).

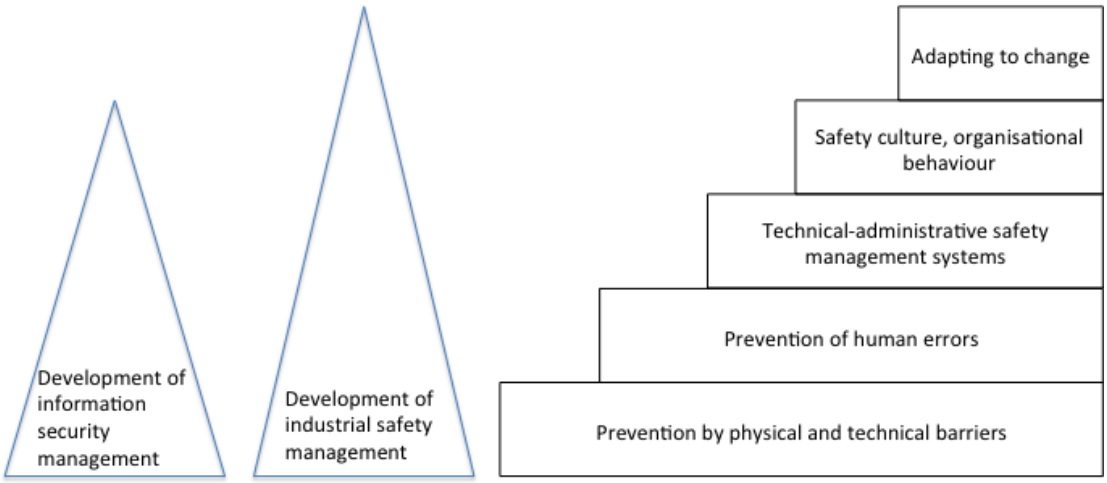

Figure 2: Steps of the development of industrial safety management.

The risks in industrial safety and information security are different regarding both causes, from unintended accidental incidents to intended acts; and consequences, from fatalities, injuries, and physical losses to loss of information and escalating adverse effects that could also harm industrial safety. Albrechtsen and Hovden (2007) claim that, compared to industrial safety risks, information security risks are more:

- uncertain (lack of knowledge),
- complex (difficult to identify and analyse chains of causes as well as consequences), and
- have more ripple effects (information security incidents leading to other incidents).

Furthermore, possible information security incidents and consequences are influenced by technological developments, unforeseen interactions, deliberate threats, non-proximate threats beyond sight, and ripple effects. Adaptive approaches constitute a response to management challenges in complex and uncertain systems (Hollnagel, 2011) and should hence be well suited for information security management.

There are different loss prevention management approaches within the fields of industrial safety and information security. This is partly explained by different characteristics of the risks and also by the historical development of the two fields. Management approaches in both fields have strengths and weaknesses, which means that there should be possibilities for transfer of experience and practices. Information security incident management can learn from the more mature socio-technical perspectives of industrial safety and adopt approaches such as resilience, worker participation, awareness training, handling of globalization, and dealing with socio-technical dynamics in order to cope with current and future challenges of information security.

Another aspect of this comparison is a convergence of information security and industrial safety. In several industries, such as power supply and process industry, safety depends on IT-based control systems. These control systems, commonly denoted as SCADA systems (Supervisory Control and Data Acquisition), are now reliant on adequate information security solutions. As a result, both industrial and societal safety depends on information security management related to both prevention of incidents and incident management.

4 Dealing with expected and unexpected events: Adaptive management strategies

The emergence of adaptive management strategies to industrial safety management is a response to the inadequacy of conventional safety management approaches with regard to complexity and dynamics in socio-technical systems (Woods and Hollnagel, 2006). Such adaptive approaches are thus necessary supplements to conventional approaches. There are mainly two related fields that describe adaptive management strategies: resilience engineering (Hollnagel, 2011) and high reliability organisations (LaPorte and

Consolini, 1991; Weick and Sutcliffe, 2007). In this paper we limit our elaboration of adaptive management strategies to resilience engineering rather than HRO, as the former focuses more on management, action, and control.

Resilience engineering is a new approach to industrial safety management (Woods, 2005; Hollnagel et al., 2006) that focuses on methods, tools, and processes that seek to strengthen and maintain a resilient system that adapts to both expected and unexpected situations in order to maintain its functioning. Resilience can be defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected situations (Hollnagel, 2011:xxxvi). A key ability of a resilient system is thus to adjust to expected and unexpected situations at the same time as it maintains its functioning. This adaptive ability is central to succeed in controlling and minimizing unwanted variability, which depends on the abilities to anticipate, monitor, and learn. These four interdependent main capabilities constitute the four cornerstones of resilience engineering (Hollnagel, 2011):

- Responding to regular as well as irregular variability, disruptions, disturbances, and opportunities either by adjusting performance or by activating response plans.
- Monitoring what changes or may change so much that a response will be required. The monitoring must cover both what is going in the environment as well as own performance.
- Anticipating future developments, threats and opportunities.
- Learning from experiences, both successes and failures.

5 Addressing information security incident management challenges with adaptive industrial safety management approaches

The previous sections described the rationale and purpose of adaptive industrial safety management. In the following we discuss theories and techniques of adaptive industrial safety management that could address current challenges in information security incident management, as presented in Section 2.

5.1 Plans, compliance and situational adaption

Plans for systematic incident management form a necessary foundation for dealing with most incidents and crises, and development of plans is an activity in the first phase, *Plan and prepare* in ISO/IEC 27035. From emergency preparedness, which is a subpart of industrial safety management, it is known that good emergency preparedness planning should (Perry and Lindell, 2003) be knowledge-based, based on risk assessments; provide decision-making support for quick and appropriate responses for emergency managers; support collaboration and coordination; and include people involved in the emergency handling. Perry and Lindell (2003) further reason that planning should involve the same approaches to different scenarios, such as applying the same principles for evacuation of people from flooding as well as from chemical emissions. They argue

that rather than making detailed plans, it is better to focus on the process of planning. Plans that are too detailed go out-of-date faster, they can lead to confusion, and are more difficult to use. Furthermore, they claim that a static emergency preparedness plan is not effective; it must be updated after incidents and exercises. Additionally, changes in technology or work processes should initiate a revision of the plans. The use of short and simple plans should hence be further encouraged for information security incident management, which is also suggested by studies of information security incident management by Jaatun et al. (2009) and Cusick and Ma (2010).

Even though plans are needed, it is impossible to plan for every possible incident due to the dynamic nature of threats as well as complexities in socio-technical systems (Hollnagel, 2011). Plans are thus not everything in incident handling; one also needs the ability to adapt to situations and even improvise (Hale and Borys, 2013). Situational adaptation and improvisation are needed in the operational phases of ISO/IEC 27035, *Detection and reporting, Assessment and decision, and Responses.* With a solid baseline structure in place, the team workers know the boundaries of their work and responsibilities, which also makes them aware of needs and actions of adaption outside the prescribed structures. In a study of improvisation in safety work, Andresen et al. (2008) reason that improvisation can only take place when operators know what they are supposed to do according to governing documents. Improvisation is a thought-through action, not an automatic reflex. It is thus important that a foundation of analysis, plans, and training is in place, as this will make successful adaptations possible.

The successful emergency ditching of a US Airways Flight on the Hudson River in 2009 is an example of an adaption-based response to a situation where the pilots interpreted no formal rules as suitable. Pariés (2011) identifies an important lesson learned from the Hudson River incident, which he calls 'the irony of resilience'. The competence suddenly needed at a sharp end to cope with unexpected or extreme events is lost in the continuous attempt to anticipate all events and pre-determine corresponding responses. Proceduralism and automation aim to reduce uncertainties in the system by reducing variety, diversity and deviations. A side effect is that procedures and compliance also reduce flexibility, creativity, and reactivity.

Hale and Borys (2013) distinguish between two different models that can be referred to regarding the use of safety rules and procedures: Model 1 and Model 2. Model 1 is based on compliance, as rules are considered to describe the best way of carrying out a task. Hale and Borys (2013) point out that in practice, this model often triggers many deviations, as workers tend to find their own way of performing tasks. Model 2, on the other hand, is a bottom-up approach, where the operators at the sharp end are considered to be the experts. Rules are seen as patterns of behavior that emerge from experience. At the same time, the rules are considered a support and guidance for the expert, a template and resource for adaptation, but not something requiring strict compliance and no substitute for competence. Adaptations to the situation, which may imply a violation of rules, are therefore sometimes considered necessary and acceptable.

We would claim that information security incident management has mainly been focused on model 1 approaches. Opening more up for model 2 would be an improvement as a combination of both model 1 and model 2 is appropriate in most organizations. This addresses the need for simple, short, and common plans for incident

management, while at the same time keeping open the possibilities of experts at the sharp end finding the best ways of solving problems through improvisation and use of existing knowledge.

5.2 Training

Plans for emergency handling have low value if they are not rehearsed. An important part of establishing emergency preparedness related to industrial safety is thus training drills (Alexander, 2002). Through emergency preparedness drills, plans will be tested and plans and details might be modified. Additionally, generic skills to deal with any expected or unexpected event will be improved, e.g communication with other actors, and the ability to interpret the situation. An important part of the drill is to practice collaboration between different involved actors (Perry and Lindell, 2003). For emergency drills many parts of the organization are, and should be, involved: not only experts, but also operators. In ISO/IEC 27035 training is included as an activity in the first phase, *Plan and prepare.*

One step to improve the adaptive capability of information security incident management is to establish regular training exercises based on expected and frequently occurring incidents. This would address the challenges of collaborations across teams and disciplines, including outsourcing scenarios, as described in Section 2. Such basic training can be performed without demanding excessive time and resources, and it will pay off quite quickly in leading to more efficient incident management on a daily basis. Training for the expected incidents will also be helpful for dealing with unexpected events (Dekker et al., 2008). Several of the principles applied for dealing with known threats, such as reaction patterns and collaboration patterns, will also be efficient for dealing with unexpected events. Adopting the concept of training generic competencies to information security as described by Bergström et al. (2011) will specifically contribute to developing resilience. Their training framework describes scenario-based training aiming at generic competencies rather than domain-specific skills representing pre-defined response. This is in line with emergency preparedness planning within the industrial safety domain where Perry and Lindell (2003) argue that planning and training should involve similar approaches to different scenarios.

5.3 Learning from incidents

Systematic learning from incidents is a key building stone to industrial safety management including resilience engineering. Even though accidents are unwanted events, they represent a unique possibility for learning when they occur. Systematic reporting of incidents as well as systematic approaches to analyzing causes and establishing countermeasures are essential for learning activities. Systematic learning from unwanted occurrences has a long tradition in systematic industrial safety management with reporting systems, analysis, and accident investigations as a basis for learning (Kjellén, 2000). Learning is described as a separate phase by ISO/IEC 27035, *Lessons learnt,* to be performed after the resolution of an incident, and identified lessons learnt typically trigger improvements to be implemented as part of the continuously running *Plan and prepare* phase.

According to Hollnagel (2011), one of the cornerstones in establishing a resilient system is to learn from both failures as well as successes. The ability to learn will also have an

impact on other abilities (Hollnagel, 2011). Systems and environments change, and pre-defined responses will sooner or later become inadequate. Learning new ways to respond is thus necessary. Similarly, the ability to monitor will improve by learning which indicators to apply. Finally, learning produces relevant understandings of what can happen in the future and will hence improve the ability to anticipate future trends and events.

A thorough literature review of safety literature on learning from incidents by Drupsteen and Guldenmund (2014) describes the learning process and identifies factors that contribute to insufficient learning. Their analysis identifies three main processes in learning from incidents:

1) systematic analysis of the incidents;
2) the use of lessons learned to make a change; and
3) sharing and storing information.

The first process, systematic analysis, is described by the following main steps (Kjellén, 2000): collect information, analyze the information, distribute information to decision-makers, decision-making and implementation of measures, and follow-up. It is important to understand learning as a process, and not as a function reduced to data collection and data analysis. One of the challenges in information security is low quality of incident registrations. Richer registrations are fundamental for further use of the information for learning.

The second main process in learning from incidents, the use of lessons learned, is about implementing change. Learning can be described as a permanent change of behavior due to previous experience; that the lessons learned have been materialized into change of some kind. However, in practice organizations sometimes fail to learn from safety incidents, which is even more often the case for information security incidents as described in Section 2. Argyris and Schön (1996) describe embarrassing and threatening issues as a main obstacle to learning. More openness and transparency of incidents as well as avoiding a focus on blame could thus improve the ability to learn from incidents. Hovden et al. (2011) and Størseth and Tinmannsvik (2012) present other ways to improve learning from safety incidents: to dismiss the question of blame, to aim at understanding the events, to accept learning as a skill that must be maintained, to limit the urge for procedures as the solution to everything, to have a multilevel, socio-technical approach when investigating the event, and involvement from many actors in defining counter-measures and follow-up of these.

The third main process in learning from incidents is related to flow of information, according to Drupsteen and Guldenmund (2014). The information flow must go beyond the ISIRT and include a larger part of the organization. Studies of investigation reports after safety accidents have shown that lack of information or failure of the flow of information is a contributing factor to all accidents (Turner, 1978). In hindsight one can often see that someone somewhere in the organization knew something. Validating the flow of safety-critical information is thus an important contribution to safety, but whistleblowing should also be emphasized. On the other hand, sharing information about information security issues is not always as straightforward as it is for industrial safety, as it may be more difficult to grasp and identify as potential problems, and it may concern sensitive information.

A new trend in resilience engineering is to learn from successes: try to make sure that things go right rather than prevent them from going wrong (Hollnagel, 2014). It is not common practice to pay attention to things that go right in information security. If any statistics are gathered at all, these statistics only cover things that went wrong. These are much easier to both notice and report. It would however be very useful to be able to document how many information security incidents are avoided each month. This would help in justifying investments made on security measures, which is usually a very difficult task, as the success of security measures is based on the absence of incidents.

A systematic approach to learning from information security incidents would aid in sharing lessons learnt, which is one of the challenges mentioned in Section 2. Further, it would be a means of gaining senior management commitment, as documentation of incidents that have already occurred would have greater impact than anticipation of future incidents that may or may not occur. This kind of documentation could also be used as part of awareness raising programs that include all employees. However, informal learning should not be underestimated, as incident response might often be an informal affair, according to Shedden et al. (2011). A remaining challenge would still be to motivate for learning activities, as motivation is a prerequisite for a systematic approach to be implemented.

5.4 Summary of recommendations

The previous subsections discussed how elements from industrial safety management could address information security incident management challenges as presented in Section 2. The table below summarizes our recommendations.

Table 1: Recommendations for improving information security incident handling.

Management element	**Recommendation**	**Challenge addressed (sec.2):**
Plans, compliance and situational adaption (sec. 5.1)	• It is impossible to plan for every possible scenario. Plans and procedures are thus not everything in incident handling, one also needs an ability to adapt to situations. • Plans and compliance reduce flexibility, creativity, and reactivity for dealing with unexpected events. • Incident handling plans need to be short and simple, while at the same time the possibilities of experts at the sharp end finding the best way of solving problems must be kept open.	• Creating plans for incident handling
Training	• Train generic competences for incident management rather than domain-specific skills representing pre-defined responses. This will make the organization more resilient to deal	• Creating plans for incident handling • Involving all employees • Gaining senior

	with both expected and unexpected events. • Training drills should include many parts of the organization, not only experts.	management commitment • Collaboration among teams and across disciplines
Learning from incidents	• Systematic reporting of incidents with rich information • Openness, transparency and dismissing the question of blame will improve the ability to learn from incidents • Limit the urge of more procedures as the solution of everything • Involvement of many actors in an interdisciplinary approach for learning from incidents	• Quality of incident registrations • Motivating learning activities • Sharing lessons learnt • Gaining senior management commitment • Collaboration among teams and across disciplines

6 Concluding remarks

Information security incident management and industrial safety management share several of the same challenges. In Section 2, major challenges for information security incident management were presented: creating plans for incident handling, gaining senior management commitment, involving all employees, coping with existing tools and their lack of usability, quality of incident registration, collaboration among teams and across disciplines, practicing incident management in outsourcing scenarios, motivation learning activities and sharing lesson learning. The same challenges could have been listed for industrial safety management as well. However, the field of industrial safety management has different approaches for addressing these challenges than the field of information security management. In this paper we have examined the suitability of industrial safety management approaches, in particular resilience engineering, for solving challenges for information security incident management. Six out of the nine major challenges could be addressed by the suggested approaches.

We believe that theories and techniques from adaptive management strategies should inspire more organizational research and empirical case studies in information security, rather than updates of the ISO/IEC 27035, as the identified challenges relate more to current practices than they point at deficiencies in the standard.

Why are industrial safety management approaches different from information security approaches? There are four interlinked reasons. First are the historical developments of the two fields. Industrial safety has a longer tradition than information security that was born out of the information technology revolution. This implies that the industrial safety field is more mature than information security. The information security field originates from military organizations with focus on control, compliance, and rules (MacKenzie and Pottinger, 1997; Dhillon and Backhouse, 2001), while industrial safety management is highly influenced by socio-technical studies (Trist and Bamforth, 1951; Trist, 1981).

Formal and informal approaches to industrial safety management are much more mature than those relating to information security management when it comes to the social dimension (Albrechtsen and Hovden, 2007), including adaptive management approaches such as resilience engineering. Second, the individual awareness differs. Individuals care more about their own and their colleagues' health and life than immaterial and material values that information security seeks to protect. Therefore, individuals are more willing to, and able to, contribute to safety, which opens for approaches such as resilience engineering. Further, this implies looking at humans as a resource in loss prevention rather than looking at humans as a threat (Albrechtsen, 2008), which relates to a third reason: worker participation. In the Scandinavian countries worker participation is established by law, which ensures that individuals participate in the systematic safety work. This legal requirement of participation is also related to the strong influence of socio-technical studies and approaches in the Scandinavian countries (Levin and Klev, 2002). A fourth factor relates to the factors above: there is more research on organizational issues in safety than security. This explains why there have been developed adaptive approaches to industrial safety management as well as a high emphasis on socio-technical perspectives.

The field of information security incident management would benefit from adopting management approaches from industrial safety. For incident management this is particularly related to devolving flexible practices and plans for handling incidents, training approaches, and learning practices. Further research should investigate implementations of the suggested management strategies into information security incident management and compare the effects with existing studies from the field of industrial safety.

7 References

Ahmad, A., Hadgkiss, J. and Ruighaver, A. B. (2012), Incident Response Teams – Challenges in Supporting the Organisational Security Function, *Computers & Security,* vol. 31, no. 5, pp. 643–652.

Albrechtsen, E. (2008), *Friend or foe? Information security management of employees*, Doctoral dissertation, Norwegian University of Science and Technology.

Albrechtsen, E. and Hovden, J. (2007), Industrial safety management and information security management: risk characteristic and management approaches. In Aven, T. and Vinnem, J. E. (eds.): Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference (ESREL), pp. 2333-2340, Taylor & Francis.

Alexander, D. (2002), *Principles of Emergency Planning and Management.* Oxford University Press.

Andresen, G, Rosness, R and Sætre, P.O. (2008), Improvisasjon – tabu og nødvendighet. In Norwegian [Improvisastion – taboo and necessity]. In Tinmanssvik, R.K. (ed.) Robust Arbeidpraksis. Tapir, Trondheim, Norway

Argyris, C. and Schön, D. A. (1996), *Organizational Learning II; Theory, method and Practice.* Addison Wesley, Reading, MA.

Bergström, J., Dahlström, N., Dekker, S., and Petersen, K. (2010), Training organizational resilience in escalating situations. In Hollnagel, E., Pariés, J, Woods, D.D. and Wreathall, J. *Resilience Engineering in Practice. A guidebook.* Ashgate, Aldershot, UK, pp. 45-56.

Brewster, E., Griffiths, R., Lawes, A., and Sansbury, J. (2012), IT Service Management: A Guide for ITIL Foundation Exam Candidates, 2nd ed. BCS, The Chartered Institute for IT.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2011), NIST Special Publication 800-61: Computer Security Incident Handling Guide, revision 2 (draft).

Cusick, J. and Ma, G. (2010), Creating an ITIL-inspired incident management approach: Roots, response, and results. In: *Network Operations and Management Symposium Workshops (NOMS)*, IEEE/IFIP, pp. 142–148. doi:10.1109/NOMSW.2010.5486589.

Dekker, S. W. A., Dahlström, N., van Winsen, R. and Nyce, J. (2008), Creating resilience and simulator training in aviation. In Hollnagel, E., Nemeth, C. and Dekker, S. W. A. (eds.): Resilience Engineering Perspectives, Remaining Sensitive to the Possibility of Failure. Aldershot, UK, Ashgate.

Dhillon, G. and Backhouse, J. (2001), Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal,* vol. 11, no. 2, pp. 127–153.

Drupsteen, L. and Guldenmund, F. W. (2014), What is Learning? A Review of the Safety Literature to Define Learning from Incidents, Accidents and Disasters. *Journal of Contingencies and Crisis Management*, vol. 22, no.2, pp.81-96.

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

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

Hale, A., and Borys, D. (2013), Working to rule, or working safely? Part 1: A state of the art review. *Safety science*, Vol.55, pp 207-221.

Hale, A.R. and Hovden, J. (1998), Management and Culture: the third age of safety. In A.M. Feyer & Wlliamson, A. (eds.) *Occupational Injury. Risk Prevention and Intervention*. Taylor & Francis, London, UK.

Hollnagel, E. (2011), To Learn or Not to Learn, that is the Question. In Hollnagel, E., Paries, J., Woods, D.D. and Wreathall, J.: Resilience Engineering in Practice. Ashgate, Farnham, UK.

Hollnagel, E, Woods, D.D. and Leveson, N (2006), *Resilience Engineering. Concepts and Precepts*. Ashgate, Aldershot, UK.

Hollnagel, E. (2011), Prolouge: The Scope of Resilience Engineering. In Hollnagel, E., Pariés, J, Woods, D.D. and Wreathall, J. *Resilience Engineering in Practice. A guidebook.* Ashgate, Aldershot, UK.

Hollnagel, E. (2014), *Safety-I and Safety-II. The Past and Future of Safety Management*. Ashgate, Farnham, UK.

Hovden, J., Størseth, F. and Tinmannsvik. R. K. (2011), Multilevel Learning from Accidents – Case Studies in Transport, *Safety Science*, vol. 49, no.1 pp.98-105.

Hove, C., Tårnes, M., Line, M. B. and Bernsmed, K. (2014), Information security incident management: Identified practice in large organizations, *8th International Conference on IT Security Incident Management and IT Forensics (IMF)*, Münster, Germany, pp. 27–46.

ISACA (2012), Incident Management and Response.

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements (2013).

ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management (2011).

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

Johnsen, S.O. (2012), Resilience at interfaces. Improvement of safety and security in distributed control systems by web of influence. *Information Management and Computer Security*. Vol.20, No.2, pp.71-87.

Johnsen, S., Skramstad, T., and Hagen, J. (2009). Enhancing the safety, security and resilience of ICT and SCADA systems using action research. In *Critical Infrastructure Protection III* (pp. 113-123). Springer Berlin Heidelberg.

Kjellén, U. (2000), *Prevention of Accident through Experience Feedback.* Taylor & Francis, London, UK.

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

Kral, P. (2011), Incident Handler's Handbook, SANS Institute Information Security Reading Room.

Kurowski, S. and Frings, S. (2011), Computational Documentation of IT Incidents as Support for Forensic Operations. In: *6th International Conference on IT Security Incident Management and IT Forensics (IMF)*, pp. 37–47. doi:10.1109/IMF.2011.18.

LaPorte, T. R., & Consolini, P. M. (1991), Working in practice but not in theory: theoretical challenges of" high-reliability organizations". *Journal of Public Administration Research and Theory: J-PART*, Vol.1, no.1, pp.19-48.

Levin, M. and Klev, R. (2002), Forandring som praksis : læring og utvikling i organisasjoner. In Norwegian [Changes in practice: learning and development in organizations] Bergen, Fagbokforlaget.

Line, M. B., Tøndel, I. A. and Jaatun, M. G. (2014), Information security incident management: Planning for failure, *8th International Conference on IT Security Incident Management and IT Forensics (IMF)*, Münster, Germany, pp. 47–62.

MacKenzie, D. and Pottinger, G. (1997), Mathematics, Technology, and Trust: Formal Verification, Computer Security and the U.S. Military. *IEEE Annals of the History of Computing 19(3)*: 41–59,

Metzger, S., Hommel, W. and Reiser, H. (2011), Integrated Security Incident Management – Concepts and Real-World Experiences, in: *6th International Conference on IT Security Incident Management and IT Forensics (IMF)*, pp. 107-121.

Möller, S., Ben-Asher, N., Engelbrecht, K.-P., Engler, R. and Meyer, J. (2011), Modelling the behavior of users who are confronted with security mechanisms, *Computers & Security*, vol. 30, no. 4, pp. 242-256.

van Niekerk, J. F. and von Solms, R. (2010), Information security culture: a management perspective, *Computers & Security*, vol. 29, no. 4, pp 476-86.

Pariés, J. (2011), Lessons from the Hudson. In Hollnagel, E., Pariés, J, Woods, D.D. and Wreathall, J. *Resilience Engineering in Practice. A guidebook.* Ashgate, Farnham, UK, pp. 9-27.

Perry, R. W., and Lindell, M. K. (2003). Preparedness for emergency response: guidelines for the emergency planning process. *Disasters*, Vol.27, no.4, pp. 336-350.

Rhee, H.-S., Ryu, Y. U. and Kim, C.-T. (2012), Unrealistic optimism on information security management, *Computers & Security*, vol. 31, no. 2, pp. 221-232. Available: http://www.sciencedirect.com/science/article/pii/S0167404811001441

Ruighaver, A. B., Maynard, S. B. and Chang, S. (2007), Organisational security culture: Extending the end-user perspective. *Computers & Security,* vol. 26, no. 1: 56-62.

Scholl, F. and Mangold, M. (2011), Proactive Incident Response, *The Information Systems Security Association Journal*.

Shedden, P., Ahmad, A., and Ruighaver, A. B. (2011), Informal learning in security incident response teams. In: *22nd Australasian Conference on Information Systems*, Sydney, Australia.

Shropshire, J., Warkentin, M. and Sharma, S. (2015), Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, vol. 49, pp. 177-191.

Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J. (2005), Analysis of end user security behaviors. *Computers & Security*, vol. 24, no. 2, pp. 124-133.

Størseth, F., Tinmannsvik, R. K. (2012), The critical re-action: Learning from accidents. *Safety Science*, vol. 50, no. 10, pp. 1977-1982.

Turner, B.A. (1978), *Man-Made Disasters*, Wykeham Science Press, London.

Trist, E. (1981), *The evolution of socio-technical systems: a conceptual framework and an action research program*. Toronto, Ontario Quality of Working Life Centre.

Trist, E. and Bamforth, K. W. (1951), Some social and psychological consequences of the longwall method of coal getting. *Human Relations* vol.4, no.1, pp.3-38

Tøndel, I. A., Line, M. B. and Jaatun, M. G. (2014), Information security incident management: Current practice as reported in the literature, *Computers & Security*, vol. 45, pp. 42–57.

da Veiga, A. and Martins, N. (2015), Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, vol. 49, pp. 162-176.

Weick, K., & Sutcliffe, K. (2007), Managing the unexpected: resilient performance in an age of uncertainty. John Wiley & Sons, IncHoboken.

Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P. and Beznosov, K. (2008), 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)*, ACM, New York, USA, pp. 107–118. URL: http://doi.acm.org/ 10.1145/1408664.1408679. doi:10.1145/1408664.1408679.

Werlinger, R., Muldner, K., Hawkey, K. and Beznosov, K. (2010), Preparation, detection, and analysis: the diagnostic work of IT security incident response, *Information Management & Computer Security*, Preparation, detection, and analysis: the diagnostic work of IT security incident response, vol.18, no.1

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D. and Ippolito, J. B. (2008), NIST SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. National Institute of Standards and Technology.

Woods, DD (2005), Creating foresight: Lessons for enhancing resilience from Columbia. In Starbuck, WH, Farjoun, M (eds.) *Organization at the limit. Lessons from the Columbia Disaster.* Blackwell Publishing, Oxford, UK.

Woods, D.D and Hollnagel, E. (2006), Prologue: Resilience Engineering Concepts. In Hollnagel, E, Woods, D.D. and Leveson, N (eds.) *Resilience Engineering. Concepts and precepts*. Ashgate, Aldershot, UK: