A Structured Approach to Incident Response Management in the Oil and Gas Industry

Maria B. Line, Eirik Albrechtsen, Martin Gilje Jaatun, Inger Anne Tøndel, Stig Ole Johnsen, Odd Helge Longva, Irene Wærø

Abstract Incident Response is the process of responding to and handling ICT security related incidents involving infrastructure and data. This has traditionally been a reactive approach, focusing mainly on technical issues. In this paper we present the Incident Response Management (IRMA) method, which combines traditional incident response with pro-active learning and socio-technical perspectives. The IRMA method is targeted at integrated operations within the oil and gas industry.

Key words: Incident Response, Process Control Systems, Learning, Security Culture

1.1 Introduction

Offshore oil and gas installations are increasingly remotely operated and controlled [3], and this has also lead to a situation where the technologies used are changing from proprietary stand-alone systems to standardised PC-based systems integrated in networks. The reliance on Commercial Off-The-Shelf (COTS) operating systems such as Microsoft Windows exposes the operators to more known information security vulnerabilities, and hence increased probability of incidents.

Increased networking between the Supervisory Control and Data Acquisition (SCADA) systems and the general ICT infrastructure (including the Internet) also increases the overall vulnerability. In North Sea operations, it has traditionally been assumed that SCADA systems were sheltered from the threats emerging from public networks [17]. Integration of ICT and SCADA

SINTEF, N-7465 Trondheim, Norway
e-mail: {maria.b.line, eirik.albrechtsen, martin.g.jaatun, inger.a.tondel, stig.o.johnsen, odd.h.longva, irene.waro}@sintef.no

systems makes this assumption void. There has been an increase in incidents related to SCADA systems [1], but these types of incidents and attacks are seldom reported and shared systematically [25] (pp 13-18).

The operating organisation is also changing; integrated operations enable better utilization of expertise independent of geographical location, leading to more outsourcing and interaction between different professionals [3].

A great number of incidents are relatively harmless, mainly causing disturbances, frustration, and reduced work efficiency. More harmful incidents may disable technical equipment, such as sensors, computers or network connections, which interrupts production continuity. Severe incidents may lead to a chain of consequences, where the end result may be large economical losses, environmental damages, and loss of lives. Effective incident handling can minimize consequences, and thereby ensure business continuity.

This paper presents a structured approach to incident management, taking into account technological as well as human and organisational factors. The remainder of this paper is structured as follows: Section 2 gives a brief presentation of the empirical background and motivation for developing the Incident Response Management (IRMA) method. Section 3 presents the three phases of IRMA in brief, with more details presented in Sections 4-6. Section 7 discusses the IRMA method and how to implement the method in industry. Section 8 concludes the paper.

1.2 Empirical Background and Motivation

The development of the IRMA framework for the oil and gas industry is based on a combination of empirical sources. The conclusion from this empirical work [15] is that the oil and gas industry still does not consider that information security is something that they need to be concerned with. One consequence of this is that there currently are no systematic security incident handling schemes implemented in this industry. Incidents that are detected are treated in an ad-hoc manner, and there are reports of e.g. virus infections that are left untreated for weeks [17].

Our research confirms that there exists a deep sense of mistrust between the 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 during a vulnerability assessment: “We don’t have any ICT systems – we only have programmable logic.” This implies that simply implementing an established incident handling scheme would not work, since it would be perceived as something emanating from the “ICT people” – a successful incident response management scheme needs to demonstrate that it is based on the realities faced by the process control engineers. (see Jaatun et al. [16] for details)

1.3 The Phases of IRMA

The IRMA method combines incident response as described in e.g. ISO/IEC TR 18044 [2] and NIST 800-61 [12] with increased emphasis on pro-active preparation and reactive learning. Our aim is to ensure that incident response procedures are continually improved, and that lessons learned are disseminated to the appropriate parts of the organisation. We focus mainly on organisational and human factors, and less on technical solutions. Fig. 1.1 illustrates the phases of the IRMA method:

- **Prepare:** Planning for and preparation of incident response
- **Detect and recover:** Detect incidents and restore to normal operation
- **Learn:** Learning from incidents and how they are handled.

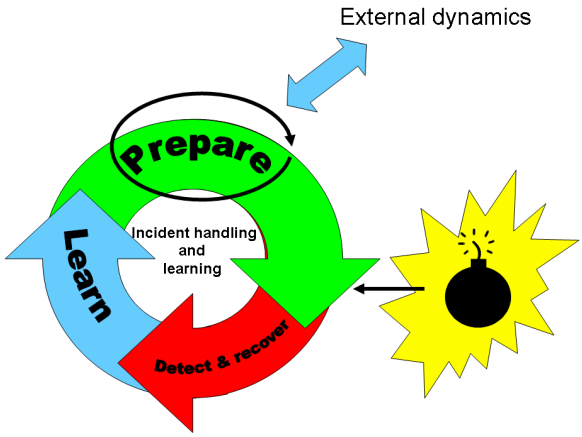

Fig. 1.1 The IRMA wheel

An organisation 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 (the bomb in Fig 1.1). Effective detection, recovery, and learning from incidents are however based on preparations and proactive learning of the *Prepare* phase. Incident response does not operate isolated in an organisation; it has to adjust to external dynamics, both within and outside the organisation. The *Learn* phase focuses on learning from single incidents. This learning is important as it makes it possible to use the experiences from incident handling to improve the incident management work in all phases. In the following, the three suggested phases of incident response management are presented in more detail.

1.4 Prepare

The *Prepare* phase is where the organisation prepares to detect, handle and recover from security incidents and attacks. Other proactive tasks such as awareness raising are also considered part of the *Prepare* phase (see below).

1.4.1 Risk Assessment

A risk assessment entails identifying the most important unwanted incidents to your assets, and determining the probability and consequence of each incident. Risks are often documented in a risk matrix, as shown in e.g. [17]. If you do not know which assets should be protected, and from what, it is impossible to prioritize and design the appropriate security measures; this makes a periodic risk assessment one of the most important activities related to information security.

1.4.2 Plans and Documentation

In an emergency situation, tacit knowledge may be your enemy – if the person with the knowledge is absent. This is why all routines, configurations, and systems must be documented in sufficient detail during the *Prepare* phase – and also kept continually updated as part of the "prepare cycle".

1.4.3 Roles and Responsibilities

The main responsibilities regarding incident response are the following:

- **Planning, preparation and training:** ICT security management.
- **Detect and alert:** Anyone who detects or suspects that an incident has occured must raise an alert.
- **Receive alerts:** Someone (either a person or function) must be appointed to receive alerts. Everyone must know who to alert in any given situation.
- **Provide technical expertise:** Someone, either inside or outside the organisation, must have technical system and/or security knowledge, and this knowledge must be available for incident recovery.
- **Handle incident and recovery:** Someone must be responsible for leading the incident response work.
- **Authority to make decisions:** Management must be on hand to make hard decisions.

- **Follow-up activities, including learn:** ICT security management.

The responsibilities of suppliers in case of incidents involving their systems should be explicitly included in contracts.

1.4.4 Awareness Creation and Training

The motivation for improving security awareness is twofold: *Preventing incidents from happening* and *improving the ability to detect and react to incidents*. A general problem is that the reason for abnormal behaviour of systems is not understood, and hence many incidents are not detected, reported, and handled. Thus, 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 may have a double effect here: In addition to building and maintaining practical incident handling skills, the exercises remind users that abnormal system behaviour *may* be the symptoms of an incident.

Building security culture in the setting of integrated operations comes with some special challenges; shift work, multiple organisations, and several specialist communities involved (land and platform, ICT and process systems). Management involvement will increase the impact of any awareness campaigns or initiatives.

1.4.5 Monitoring

In systematic control of management systems, feedback mechanisms have been utilized in many different business processes [13], e.g. financial results; production efficiency; market reputation; quality management; and Health, Safety, Security and Environment (HSSE) management. The field of safety management has a tradition for using performance indicators for persistent feedback control [19]. We suggest to implement similar indicators to measure how the incident response performs over time, e.g. time spent on each incident, and the total number of incidents in a given period.

1.4.6 External Dynamics

Incident response management does not operate in isolation from other parts of the organisation and the organisational context. It is also influenced by the general information security management strategy. This influence goes both ways, as the two must be adjusted to learning made in the other area. Both are influenced by information security regulations.

1.5 Detect and recover

The *Detect and recover* phase includes detection, alerting, recovering and documenting of an incident. The recommendations made regarding detecting and recovering from incidents are based on various sources [2, 12, 6].

1.5.1 Alerting

Information security incidents are mainly detected in two ways [2]; by coincidence, where someone notices something unusual, or by routine use of technical security measures. The former is just as important as the latter, which means that each and every employee must be aware of their responsibility of alerting when they discover irregularities. Roles and responsibilities are already defined, so everyone knows who to alert and who is responsible for handling the incident. Regarding incident reporting there may be a lot to learn from experiences within HSSE [21].

1.5.2 Assessment

The incident must be assessed with respect to severity and the way forward. The following actions take place [2]:

- **Acknowledge receipt:** The alerter is informed that handling has started.
- **Collect more information:** If necessary, more information will be collected [12]. The goal is to state severity and scope of incident, who should be involved in handling it, and whether it may affect production and/or safety.
- **Further alerting:** Additional personnel needed for handling must be alerted.

The ideal incident management team in integrated operations includes experts on both ICT security and process control systems, which will lead to the best possible trade-offs between security and production. Suppliers may need to be involved.

1.5.3 Immediate Response

In a process control environment it is an imperative goal to keep the systems running as long as possible. Disconnecting them from external networks completely is however a reasonable first action. Activating surveillance techniques

may be prudent in any case, to achieve a greater understanding of the incident.

The best decisions at the time of an incident are made if one is prepared for what major types of incidents may occur and what actions should be taken in response to these incident types [25].

By escalation we mean to get help from outside the team. There may be several reasons for an escalation: The necessary competence is not available in the current team; one is not able to get the incident under control; the incident is more serious than first anticipated; or upper management decisions are necessary.

Each incident must be documented with respect to what happened, which systems were affected, which damages occurred and how the incident was handled. Documentation of an incident starts when the alert is raised, and continues throughout all steps in the incident handling. Documentation must be made easy – otherwise, it will not be performed. Any tools should be readily available and easy to use, and those involved should be trained in using them. Alternatively, one could just describe actions taken in an unstructured document or in a logbook [12]. The incident and the analysis of it must be documented in order to inform other actors about the incident and share good practice, as well as to keep a record of the incident that can be used to sustain learning from the incident, or analyse the incident at a later stage.

1.5.4 Communication Plan

It may be necessary to inform selected persons within or outside the organisation about the incident, such as: Management at different levels – they may need to comment the incident in public, and they should not need to hear about the incident through other channels (e.g. the media); those affected by the incident need to understand what happened, and why; media – if the incident is of public interest.

1.5.5 Recovering

The immediate responses seldom solve the entire problem; they rather ensure that the incident is under control and limit the damage. Thereafter, actions must be taken to bring the affected system(s) back to normal operation; i.e. ensuring that they are in a safe state, and reconnecting to external networks. Configuration changes and patching will help reducing the vulnerability of the system attacked [2]. This should also be done to other systems that may be targeted for similar attacks in the near future. The incident may have lead to malicious code installed in the system that is hard to detect. To clean

up, installation media for operating systems may be an alternative, and/or backup copies and other recovery tools. Integrity checks and investigation tools may also be helpful [6].

1.5.6 The End of Recovery is the Beginning of Learn...

When everything is up and running, the experiences should be explored to improve the preparedness of the organisation. This is the focus of the *Learn* phase that is presented in the following section. The *Learn* phase should be started when the incident is still fresh in people's minds. But first: The person who raised an alert about the incident must be briefed on how the incident was handled. This is an important part of awareness-raising in incident management.

1.6 Learn

The learning phase of IRMA focuses on learning from the actual incident [9] by four different steps in addition to a parallel activity of learning from the *handling* of the incident.

1.6.1 Commitment and Resources

In order to succeed with learning, the organisation must be prepared for it. The key issue is the extent of management commitment and the willingness to spend resources on learning from incidents.

Learning processes are dependent on documentation of the incident, as stressed in the *Detect and recover* phase. A structured accident analysis methodology will help identify immediate and underlying causes, and should cover organisational, technical, and human factors issues.

1.6.2 What Occurred - Identify Sequences of Events using STEP

The STEP method [14] is a tool for detailed analysis of incidents and accidents. It allows for a graphic presentation of the events during the scenario, in the following manner:

- Actors (i.e. person or object that affects 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.
- The relationship between the events, i.e. what caused each of them, is identified and showed in the diagram by drawing arrows to illustrate causal links.

1.6.3 Why - Identify Root Causes and Barriers

The STEP diagram can be used to fully 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 [16].

The weak points should subsequently be assessed by a barrier analysis, including suggestion of countermeasures. (see e.g. [18]). Barriers are here understood to be technical, human, and organisational.

1.6.4 Recommend Security Improvements

The accident analysis, identified weak points, and suggested barriers, represent the necessary background to identify security recommendations. It is important to prioritise the suggested actions based on a cost/benefit analysis, and explicitly assign responsibility for performing the actions.

1.6.5 Evaluate the Incident Handling Process

The *Learn* phase also includes an evaluation of the incident handling process itself. Experiences from the handling process should be used to improve the managing of future incidents. Ideally, all relevant parties should be involved shortly after an incident occurred and was handled, while information is still fresh in people's minds. Factors to consider include [2]:

- Did the incident management plan work as intended?
- Were all relevant actors involved at the right time?
- Are there procedures that would have aided detection of the incident?
- Were any procedures or tools identified that would have been of assistance in the recovery process?
- Was the communication of the incident to all relevant parties effective throughout the detection and recovery process?

1.7 Discussion

This paper has described a framework for incident response management in the North Sea oil and gas industry. There are several other publications describing similar approaches to incident handling, e.g. [2, 12, 5, 4, 22, 11]. Our approach follows the same basic ideas presented in the literature above, but differs from these in three ways: 1) its emphasis on socio-technological aspects covering the interplay between individuals, technology, and organisation; 2) its emphasis on learning in a reactive and pro-active way; and 3) its range of use for ICT/SCADA systems in the oil and gas industry.

The former two of these 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. Then we discuss why learning from incidents is important, but also challenging.

1.7.1 Socio-technical Approach to Incident Handling

A socio-technical information security system [7] is created by elements of different information security processes and the interplay between these elements. Traditional incident handling [2, 4, 12] has mainly focused on technical aspects of incident response. The described framework in this paper has also focused on individual behaviour and organisational processes. This is for example shown by the emphasis on organisational roles, awareness training, risk assessment processes, and follow-up activities in the *Prepare* phase; roles in the *Detect and recover* phase; and involvement of actors in learning activities. In general, the information security domain has lacked focus on socio-technical approaches [10, 23]. Our approach to incident response thus contributes to a wider perspective on information security management as it considers information security as a socio-technical system.

The described *Prepare* phase in Section 1.4 shows how technological solutions, individuals, and organisational structures and processes are primed to be ready to discover and deal with incidents as well as prevent incidents from happening. These assets are important in the development and maintenance of a socio-technical incident handling system, but also to make the system proactive.

The learning processes suggested in this paper emphasise organisational learning, i.e. changes in organisational interplay between individuals and groups including modifications of organisational processes and structures [8]. This approach implies that incident learning should emphasise both single-loop and double-loop learning [8], i.e. response based on the difference between expected and obtained outcome (single-loop) and to be able to question and change governing variables related to technology, organisation, and human factors that lead to the outcome (double-loop). The latter is necessary

for socio-technical long-term effects, while the former is more concerned with fire-fighting and technological solutions.

Although empirical findings show that there are few incidents in the oil and gas industry, the same findings indicate that systematic analyses of incidents and organisational learning are seldom performed in practice [16]. The root causes of incidents are not always documented and there is a main focus on technical issues when studying incidents. Organisational and human factors issues are seldom explored. Different professional disciplines are a challenge for the learning capability in an organisation, as different roles and positions should be involved in incident learning processes.

In our interaction with the oil and gas industry we have experienced the communication gap between the groups of ICT staff and process control staff. These groups have traditionally not needed to cooperate, and have had different interests. The increased use and interconnectivity of ICT systems has resulted in increased information security threats also towards process control systems. For efficient handling of security incidents in SCADA systems these two groups need to cooperate. The communication gap between these two groups has been taken into account in the IRMA method. Challenges regarding different risk perceptions and situational understandings are best approached by discourse-based strategies [20, 24], where involved actors meet and discuss challenges with each other aiming at a common understanding.

1.7.2 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. By using experience from incidents and the incident handling processes in a proper manner, the organisation will be able 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, both in a reactive and pro-active manner. Reactive in the sense that one learns from actual incidents and incident handling, and pro-active in the sense that the incident handling system is adjusted to lessons learned both internally and in the organisations context. Based on the premises of incident response management as a socio-technical system, the learning processes have emphasized organisational learning.

In general, there are two obstacles to organisational learning: embarrassing and threatening issues [8]. Information security incidents may be embarrassing (e.g. virus infections due to incautious use of the Internet) and threatening in the sense that the incidents are considered confidential. These characteristics create individual and organisational behaviour that is counter-productive

when it comes to learning from unwanted incidents. These defensive routines may in fact be the reason that our empirical research indicated so few incidents in the industry. However, the empirical study of incident handling in the oil and gas industry showed that several informants called for more frankness and openness about unwanted incidents to learn both internally in an organisation as well as cross-organisational, which requires more communication on incidents in and across organisations.

1.8 Conclusion

A systematic approach to incident response and learning from incidents is important to the oil and gas industry because of the recent development regarding integrated operations. Even though they experience few incidents at the moment, more technological and organisational changes are still to come, and not being prepared for greater risk and new and unforeseen threats may be very costly to a business that depends on approximately zero downtime in their production systems.

The IRMA method is first and foremost developed with respect to the oil and gas industry, but it should also be applicable to other industries that rely on process control systems and integrated/remote operations. Our method is innovative for incident handling regarding pro-activity and organisational focus.

Oil and gas production requires cooperation between many organisations, including operators, various suppliers, and regulatory authorities. This must be taken into account when implementing IRMA. It is not enough for an operator to consider only the operator organisation, since cooperation of suppliers is highly important when preparing for, detecting, recovering and learning from incidents. We therefore recommend that IRMA is implemented for installations rather than organisations.

Since implementation of the IRMA method will require resources, and ideally preparation before the incident is a fact, success of IRMA requires that management is convinced of the benefits of incident management and willing to spend time and resources on preparation.

1.9 Acknowledgements

This work was carried out in the IRMA project, 2005-2007, financed by the Norwegian Research Council and the Norwegian Oil Industry Association.

References

1. Hackers Have Attacked Foreign Utilities, CIA Analyst Says. URL http://www.washingtonpost.com/wp-dyn/content/article/2008/-01/18/AR2008011803277.html
2. Information technology - Security techniques - Information security incident management. Tech. Rep. TR 18044:2004, ISO/IEC (2004)
3. Integrated Operations on NCS (2004). URL http://www.olf.no/?22894.pdf
4. Information technology – security techniques – code of practice for information security management, ISO/IEC Std. 27002 (2005)
5. Information technology – security techniques – information security management systems – requirements, ISO/IEC Std. 27001 (2005)
6. A. Cormack et al.: TRANSITS course material for training of network security incident teams staff. Tech. rep., TERENA (2005)
7. Albrechtsen, E.: Friend or foe? Information security management of employees. Ph.D. thesis, NTNU (2008)
8. Argyris, C., Schön, D.A.: Organisational learning: A theory of action perspective. Addison-Wesley (1978)
9. Cooke, D.L.: Learning from Incidents. In: Proceedings of the 21st System Dynamics Conference (2003)
10. Dhillon, G., Backhouse, J.: Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal **11(2)**, 127–153 (2001)
11. Forte, D.: Security standardization in incident management: the ITIL approach. Network Security **2007(1)**, 14–16 (2007)
12. Grance, T., Kent, K., Kim, B.: Computer security incident handling guide. Tech. Rep. Special Publication 800-61, NIST (2004). URL http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
13. Hammer, M., Champy, J.A.: Re-engineering the Corporation: A Manifesto for Business Revolution. Harper Collins (1993)
14. Hendrick, K., Benner, L.: Investigating accidents with STEP. CRC Press (1986)
15. Jaatun, M.G., Albrechtsen, E., Line, M.B., Johnsen, S.O., Wærø, I., Longva, O.H., Tndel, I.A.: A Study of Information Security Practice in a Critical Infrastructure Application. In: Autonomic and Trusted Computing, Proceedings (2008)
16. Jaatun, M.G., Johnsen, S.O., Line, M.B., Longva, O.H., Tøndel, I.A., Albrechtsen, E., Wærø, I.: 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
17. Johnsen, S.O., Ask, R., Røisli, R.: Reducing Risk in Oil and Gas Production Operations. In: E. Goetz and S. Shenoi (Eds.) (ed.) First Annual IFIP WG 11.10 International Conference, Critical Infrastructure Protection (2007)
18. Johnsen, S.O., Bjørkli, C., Steiro, T., Fartum, H., Haukenes, H., Ramberg, J., Skriver, J.: CRIOP: A scenario method for Crisis Intervention and Operability analysis. Tech. Rep. STF38 A03424, SINTEF (2003). URL www.criop.sintef.no
19. Kjellén, U.: Prevention of accidents through experience feedback. Taylor and Francis (2000)
20. Klinke, A., Renn, O.: A new approach to risk evaluation and management: risk-based, precaution-based and discourse-based strategies. Risk Analysis **22(6)**, 1071–94 (2002)
21. M. G. Jaatun (red.): Arbeidsseminar om IKT-sikkerhet i Integrerte Operasjoner: Referat (in Norwegian only). Tech. rep., SINTEF (2007). URL http://www.sintef.no/upload/10977/sluttrapport.pdf
22. Mitropoulos, S., Patsos, D., Douligeris, C.: On Incident Handling and Response: A state-of-the-art approach. Computers & Security **25(5)**, 351–370 (2006)
23. Siponen, M.T., Oinas-Kukkonen, H.: A review of information security issues and respective research contributions. Database for Advances in Information Systems 38(1): 60 (2007)

24. Slovic, P.: The perception of risk. Earthscan, London (2000)
25. Stouffer, K., Falco, J., Kent, K.: Guide to industrial control systems (ics) security (2nd draft). Tech. Rep. Special Publication 800-82, NIST (2007). URL http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf