SINTEF

SINTEF ICT

Address: NO-7465 Trondheim, NORWAY
Location: S P Andersens v 15, NO-7031 Trondheim
Telephone: +47 73 59 30 00
Fax: +47 73 59 43 02

Enterprise No.: NO 948 007 029 MVA

SINTEF REPORT

TITLE

Incident Response Management in the oil and gas industry

AUTHOR(S)

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

CLIENT(S)

Research Council of Norway and OLF

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
SINTEF A4086	Unrestricted		
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
Unrestricted	9788214040746	90D205	83
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
20071212_IRMA_Rapport.doc		Martin Gilje Jaatun	Thor Myklebust
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
	2007-12-17	Eldfrid Ø. Øvstedal, Research Director	

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. Incident Response Management (IRMA) combines traditional incident response with a proactive learning loop, thus increasing the focus on organisational learning. The IRMA method is comprised of the following phases:

- **Prepare:** Planning and preparation of incident response
- **Detect and recover:** Detection of incidents and restoration to normal operation
- **Learn:** Experience sharing and learning afterwards.

The IRMA project has focused on the offshore oil and gas industry, but the results should also be applicable to other organisations in the energy sector or process control industry.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Information technology	Informasjonsteknologi
GROUP 2	Information security	Informasjonssikkerhet
SELECTED BY AUTHOR	Integrated operations	Integrerte operasjoner
	Incident handling	Hendelseshåndtering
	Incident response	Hendelsesrespons
	Learning	Læring

SINTEF

Executive Summary

Incident Response (IR) is the process of handling ICT security related incidents involving infrastructure and data. This has traditionally been a reactive approach, focusing mainly on technical issues. Incident Response Management (IRMA) combines traditional IR with a proactive learning loop. IRMA includes the following phases:

- **Prepare:** Planning and preparation of incident response
- **Detect and recover:** Detection of incidents and restoration to normal operation
- **Learn:** Experience sharing and learning afterwards.

IRMA has been developed in the context of the Norwegian oil and gas industry because of the large-scale changes due to implementation of Integrated Operations (IO), and the extreme consequences of unwanted safety and security incidents in this industry. The transition to IO brings along new technologies and new work processes, and the interaction between safety, production and ICT security increases. These changes make the industry vulnerable, and the time is just right for looking at measures that can improve information security in the industry, e.g. by improved incident preparedness and handling. IRMA represents a systematic approach to this task.

This report provides specific advice related to the various phases of incident response. It also gives a step-by-step guide for how to implement IRMA in an oil and gas organisation.

The primary target group for this IRMA report will be administrative personnel, who are responsible for planning and implementing measures regarding information security. They will find help and guidance in this report. Technical personnel will also find useful information in selected areas of the report, and may use it as a reference.

The concept of responding to incidents is not new, and we therefore find it useful to present current good practice from the oil and gas industry. The empirical basis stems from meetings and workshops with industry representatives, and a series of interviews of selected personnel with information security related duties in the oil and gas industry. The new approach introduced by IRMA results in a circular perspective on the incident response management process, where learning from incidents gives input to organisational processes and feedback throughout the *organisation as a whole.* This implies a need for segmenting information to be conveyed, ensuring that the different target groups receive both the type and amount of learning that is appropriate for them. IRMA emphasizes an additional learning loop in the “prepare” phase, facilitating improved information security through learning also during periods without incidents.

The importance of effective incident response management should not be underestimated. Some may have the impression that their systems are not vulnerable, since no serious incidents ever occur. At the same time, many are unaware of possible consequences of incidents, and one can never know in advance when the bad luck, or intended attacks, strike. Furthermore, the vulnerability of offshore process control systems increases steadily due to:

- Increased prevalence of standard PC hardware and software in industrial networks, and increased interconnection between process control networks and office networks
- Extensive inter-organisational collaboration and network interconnection
- Dependency on the technical infrastructure that facilitates the collaboration

It is all about “being ready when the wave hits”. Any major investment should be preceded by a cost-benefit analysis, and Incident Response is no different. There is a balance between being well prepared and accepting a certain level of risk, and every organisation must define this level of balance as it is appropriate for them.

Preface

This report documents the main results of the research project “Incident Response Management” (IRMA), funded by the IKT SoS programme of the Research Council of Norway and The Norwegian Oil Industry Association (OLF). The IRMA project commenced in January 2005, and will be completed at the end of 2007.

The main objective of the IRMA project has been to improve information security in ICT systems in the oil and gas industry by developing and implementing a method for Incident Response Management in the new e-Operations environment.

The research on which this report is based has in part been performed in collaboration with industry representatives through various forums facilitated both by OLF and individual operating companies, in particular Hydro Oil & Energy. IRMA has also had a liaison with the research project “A Model-Based Approach to Security Culture” (AMBASEC) at Agder University College (now: University of Agder) in Grimstad.

Through participation in OLF’s workgroup on information security, the IRMA project has contributed to the development of the Information Security Baseline Requirements (ISBR [1]). The ISBR consist of 16 requirements, the final of which reads: “Procedures for reporting of security events and incidents shall be documented and implemented in the organisation.” This report will hopefully assist organisations striving to fulfil this requirement.

We especially would like to thank StatoilHydro – they have been instrumental in establishing this guideline. In addition thanks to those who participated in our workshop in 2006 [2], and the interviewees who participated in our survey of the state of the art in incident handling and all the other participants in the OLF workgroup for useful collaboration and practical insights: ABB, Aker Kværner, BP, ConocoPhillips, DNV, Halliburton, Hewlett-Packard, IBM, NPD, Oilcamp, Ptil, Schlumberger, Shell, Telenor, UiS.

TABLE OF CONTENTS

Executive Summary ..... **i**

Preface ..... **ii**

1 Introduction **1**
1.1 Proposed incident response management system 2
1.2 Some common terms 3

2 Background **5**
2.1 Information security challenges with integrated operations in the oil and gas industry 5
2.2 Motivation for incident response management 6
2.3 Scenarios to illustrate typical incidents 7
2.3.1 Virus infection 7
2.3.2 Denial-of-service 7
2.3.3 Insider 8
2.3.4 Missing situational awareness 9

3 Methods and findings **10**
3.1 Interviews 10
3.2 A case study of incident response management practice at an oil and gas installation in the North Sea 11
3.3 Risk and vulnerability assessment 11
3.4 Key challenges at an IO installation, identified by the CheckIT tool 12
3.5 Workshop on information security and integrated operations 12
3.6 Workshop on main findings from IRMA 13
3.7 System dynamics workshops and cooperation with the AMBASEC project 14
3.8 OLF-meetings 16

4 Prepare **17**
4.1 External dynamics 17
4.2 Risk assessment with respect to incident response management 19
4.2.1 Monitoring and communicating the risk level 21
4.2.2 Risk assessment examples 21
4.3 Roles and responsibilities 21
4.3.1 Incident response team 21
4.3.2 Responsibilities at interfaces between actors 22
4.4 Planning and documentation 23
4.4.1 Plan for preparation for incident handling 23
4.4.2 Plan for detection and recovery from incidents 23
4.4.3 Plan for learning from incidents 24
4.4.4 Documentation of system information 25
4.5 Developing incident handling awareness 26
4.5.1 Management involvement 26
4.5.2 Communication and cooperation across disciplines and organizational boundaries 27
4.5.3 Education and training 27
4.5.4 Established dissemination channels 28
4.5.5 Utilization of incident experience 28
4.5.6 Review and measure 29
4.6 Monitoring of incident response management 29
4.6.1 Performance indicators for incident response 29

4.6.2 Monitoring threats from insiders 32
4.6.3 How to follow up performance indicators 32

5 Detect and recover 34
5.1 Document and prepare for learning from the incident 35
5.2 Detect and alert 36
5.3 Recover from incident 37
5.3.1 Assessment 37
5.3.2 Immediate responses 38
5.3.3 Escalation 38
5.3.4 Communications 39
5.3.5 Further responses 39
5.4 The end of recovery is the beginning of learn... 39

6 Learn 40
6.1 Commitment - do we want to perform organisational learning? 42
6.2 What occurred - identify sequences of events using STEP 43
6.3 Why - Identify root causes and barriers 44
6.4 Identify safety and security recommendations 48
6.4.1 Document safety and security recommendations and the Incident 48
6.4.2 Documentation and follow up of recommendations 48
6.4.3 Documentation of the incident 48
6.5 Evaluate the incident handling process and identify recommendations 49
6.6 From Learn to Prepare 50

7 Conclusions 51
7.1 What have we accomplished in IRMA? 51
7.2 What will we do further in IRMA? 51
7.3 What did we not accomplish I IRMA, related to the objectives? 52
7.4 Further work after IRMA 52

References 53

Appendix A Abbreviations 57

Appendix B Terms and definitions 59

Appendix C Interview Guide 60

Appendix D Relevant standards and good practice 62

Appendix E Example Incident Reporting Form 66

Appendix F STEP Diagram for Incident Response Planning 70

Appendix G STEP Diagram for Documenting an Incident 71

Appendix H The use of CheckIT 72

Appendix I Proactive and reactive barriers 75

Appendix J Publications from the IRMA project 77

1 Introduction

The development of integrated operations in the oil and gas industry could imply that the possibilities of incidents in ICT and SCADA systems are increasing. In this report such incidents are understood as incidents that could imply loss of availability, loss of integrity and/or loss of confidentiality related to ICT or SCADA systems in production systems, which may generate negative consequences for the production process or create unwanted HSSE (Health, Safety Security and Environment) incidents.

An incident that is allowed to develop may cause consequences on several levels. A great number of incidents are relatively harmless, and a natural consequence of such is that employees perceive their job situation as disturbed, get frustrated, and therefore work with reduced efficiency. More harmful incidents may put out technical equipment, such as sensors, computers or network connections, which interrupt business continuity. Severe incidents may even cause a chain of consequences, where the end of the chain may be large economical losses, environmental damages, and loss of life. By being able to handle incidents in an efficient way, one can minimize consequences, and business continuity can be ensured. Consequently, systematic incident response approaches are needed to cope with the challenges of ICT/SCADA incidents.

Traditionally, incident response work has been an integrated part of overall information security, and it often becomes difficult in any given situation to differentiate between initiatives that are intended to improve incident response and initiatives that are intended to improve security in general. In this report we will focus on incident response, while acknowledging that an interface to preventive measures also is important

The main objective of this report is to present a system for incident response management (IRMA) in the oil and gas industry, i.e. activities conducted in a more or less coordinated way to prepare incident response, handle incidents and learn from incidents. The main target group for this report is the professionals involved in specification, purchasing or operation of the ICT/SCADA equipment used in production or in safety related systems in the oil and gas industry, but the report should also be relevant to other industries..

There are several relevant standards and good practise documents describing incident handling, e.g. ISO/IEC TR 18044:2004 Information Security Incident Management [3]; parts of ISO/IEC 27001[4] and ISO/IEC 27002: Information Security Management Systems [5]; OLF Guideline no. 104 (ISBR#16) [1]; NIST 800-61: Computer Security Incident Handling Guide [6]; and parts of ITIL[7]. Additionally, systems for incident handling are widely described in the literature, e.g. [8-11]. The incident response management approaches described in this report, IRMA, follow the basic ideas as the methods above, but differs since IRMA emphasizes the MTO perspectives (Man, Technology, and Organisation). IRMA focuses both on reactive and proactive learning, thus emphasising the importance of learning and preparing in addition to detection and recovery. Furthermore, IRMA is tailored to the oil and gas industry.

The proposed system for incident response management has been developed in dialogue with and by studies of the Norwegian oil and gas industry. This means that the findings in this report are relevant for the oil and gas industry. However, experience transfer to incident handling in other areas using the same technical infrastructure, such as other parts of the energy sector, should be possible

1.1 Proposed incident response management system

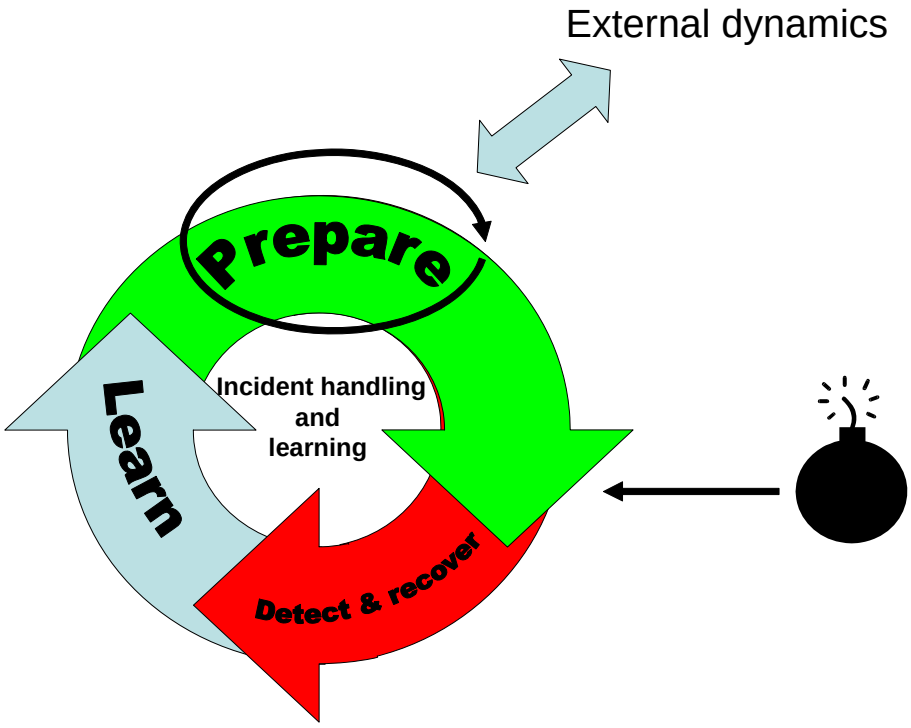


Figure 1-1: The IRMA wheel

Figure 1-1 shows the incident response management system proposed in this report. The proposed management system combines incident response as described in e.g. ISO/IEC TR 18044 [3] and NIST 800-61 [6] with increased emphasis on

- a reactive learning loop, focusing on improving governing variables such as organisational, human and technical factors
- proactive preparation.

These reactive and proactive elements must be included in incident response management in order to ensure that incident response procedures are continually improved, and that lessons learned are disseminated to the appropriate parts of the organisation. Improving incident response will also improve the resilience of integrated operations and reduce the probability of severe incidents due to human errors as well as security incidents influencing safety of personnel, reliability and regularity of production. We have decided to divide incident response management into three phases[1]:

- **Prepare:** Planning for and preparation of incident response
- **Detect and recover:** Detection of incidents and restoration to normal operation
- **Learn:** Experience sharing, and learning from incidents and how they are handled.

The phases are interrelated. The prepare phase makes one ready to detect incidents in the best possible way, thus resuming to normal operation in the most efficient way. The detect and recover phase is triggered by an incident, but the actual detection and recovery work that is performed is based on preparations and proactive learning which have been performed in the prepare phase. The learn phase follows automatically after the actual detection of incidents and the subsequent recovery from them. This learning is important at it makes it possible to improve activities in the detect and recover phase as well as in the prepare phase, and will provide useful input to the

[1] For those who are familiar with Deming's Plan-Do-Check-Act circle, we can mention that the "act" phase ("improve" in TR18044) in our model is divided between the "Prepare" and "Learn" phases in Figure 1-1.

external dynamics that constitute the general security activities such as improvement of technical and organisational barriers. The prepare phase influences the learn phase as well by planning how reactive learning should happen.

Incident response management is the sum of activities conducted in a more or less coordinated way to handle incidents, learn from them and prepare incident response. An organisation is likely to spend most of its time in the “prepare” phase; the “detect & recover” phase and the subsequent “learn” phase is only triggered by an incident. The prepare phase includes continuous learning and interaction with external dynamics. The continuous learning activities are triggered by: A fixed time interval; dynamic environmental stressors (e.g. changes in risks and vulnerabilities; new technology; new working methods; changes in political climate; and changes on competency among worker); and incidences or near-misses in related installations/industries.

Integrated operations imply coordination between many organizations, i.e. operator and suppliers of equipment and services, in a virtual organization. This presents a major challenge to Incident response management. Overall responsibility and authority must be clearly defined and the problems of interaction between different organizations security cultures must be resolved.

1.2 Some common terms

Information Security is most commonly defined as the ability of a system to protect information and system resources with respect to confidentiality, integrity and availability [12], which can be summarized by the acronym "CIA":

- **Confidentiality:** the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** the property that information is not altered by unauthorized persons in a way that is not detectable by authorized users
- **Availability:** the property of timely and reliable access to data services for authorized entity

An incident in an ICT system, i.e. an information security breach, is understood as violation of one or more of these properties.

An incident violating one or more of the CIA properties in an integrated ICT and process control systems in production may influence the production process and lead to unwanted consequences like service disruption, HSSE incidents or financial loss. In this report an incident in an ICT/SCADA system is thus understood as *an incident that could imply loss of availability, loss of integrity or loss of confidentiality related to the ICT or SCADA systems in production systems and thus influencing the production process (leading to a halt or deviation) or lead to an unwanted HSSE incident.*

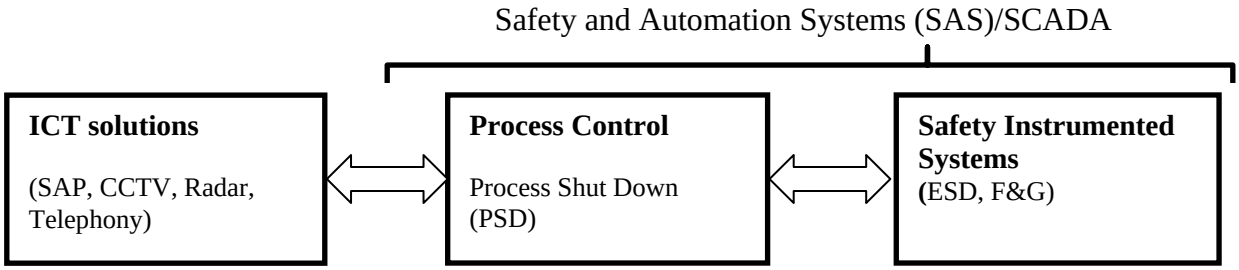


Figure 1-2: Scope of technical infrastructure used during production

The technical infrastructure that is addressed in this report includes three main areas; the ICT infra-structure, SCADA/process control systems (PCS) [13], and the safety instrumented systems (SIS) [14],

as outlined in Figure 1-2. The ICT infrastructure consists of network, supporting systems used in the production process such as SAP, infrastructure as telephone support systems, radar and video systems (closed-circuit television – CCTV). Process control systems are used during regular production and include sensors, OPC and process shut down systems (PSD). The safety instrumented systems are used during emergency shutdowns (ESD) and to prevent fire & gas emissions (F&G). The PCS and SIS systems together are usually called safety and automation systems (SAS)[15] or Supervisory Control and Data Acquisition (SCADA) systems. In the following we will primarily use the SCADA acronym since this is most frequently used internationally, although it has not necessarily traditionally been used in all sectors in Norway.

2 Background

In the following we provide background information on Integrated Operations[2], information security and the motivations for incident response.

2.1 Information security challenges with integrated operations in the oil and gas industry

Integrated Operations covering remote operations and remote control of offshore oil and gas installations is increasing in the North Sea [16]. The main motivations for integrated operations are the potential for operational cost reduction, increased income or yield from the fields, and increased safety. However, initial projects envisioning quick implementation of integrated operations have not been carried through as easily as expected. New technologies and new ways of working have been implemented to increase remote operations and remote control. Many of the projects have been changed or delayed due to a higher degree of complexity than originally envisioned.

The technologies used in integrated operations are changing from proprietary stand-alone systems to standardised PC-based IT systems integrated in networks, which in turn may be connected to the Internet. The reliance on COTS (Commercial Off-The-Shelf) operating systems such as Microsoft Windows on servers increases the vulnerability. The increased networking between the Supervisory Control and Data Acquisition Systems (SCADA), and the general ICT infrastructure also increases the overall vulnerability.

The SCADA systems are fundamentally different from traditional ICT systems. Several challenges become evident when ICT and SCADA systems are integrated, such as the need for antivirus solutions, patching, and awareness of the need for information security in the SCADA systems. There has been an increase in incidents related to SCADA systems – some of them having devastating impact on the operations offshore. These types of incidents and attacks are seldom reported and shared systematically ([13], pp3-18). In North Sea operations the traditional approach has been the assumption that SCADA systems were sheltered from the threats emerging from public networks, such as the Internet [17]. This perception still seems to be widespread within the automation profession. Questions related to security and safety [18] of integrated operations has been raised, i.e. are integrated operations safe and secure? Some of these issues and questions are treated in the OLF work group on information security in integrated operations.

The operating organisation is also changing; integrated operations enable better utilization of expertise independent of geographical location, leading to more interaction between different professionals [16]. Several tasks in operations and maintenance have been outsourced to suppliers and vendors outside the company, and this trend is likely to increase, based on the possibilities given by integrated operations. Outsourcing, the increased use of suppliers and increased connectivity leads to a network of actors, which by accident, negligence, or purpose can inflict unforeseen incidents or accident on an operator, causing large economic loss; and in the worst case, loss of lives. The complexity of integrated operations is illustrated in Figure 2-1, by showing some of the key actors involved in integrated operations, such as:

- the control room offshore
- the operator's onshore operating centre
- service companies' onshore operating centre
- external experts

[2] The terminology and accompanying description varies between the oil companies. Often-used terms have been *remote operations*, *integrated operations*, *e-operations*, *e-field*, *smart field*, and *field of the future*. In accordance with the OLF usage, we will use the term *integrated operations* in the rest of this report.

History shows that personnel involved in projects implementing integrated operations have a tendency to focus too much on technology, often at the expense of human factors, organisational and cultural issues [19, 20]. Virtual organisations and ensuing increased vulnerability create the need for a common risk perception and a common security and safety culture to reduce the risks associated with integrated operations. Incident reporting and learning from incidents among all the involved actors are key issues to reduce the risks.

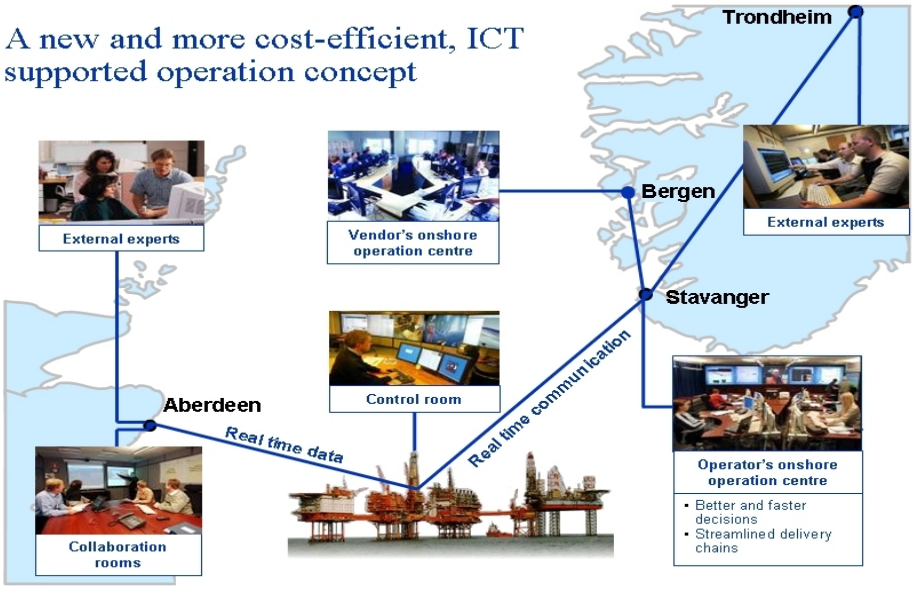


Figure 2-1: Key actors involved in integrated operations [21]

Exploitations of vulnerabilities may lead to the stop of production on oil and gas platforms. The costs of such production stops on the Norwegian Continental Shelf vary greatly, but could typically be losses of 2 to 3 Mill USD, according to NPD [22, 23]. The loss could be larger if a key production facility is affected.

It is widely acknowledged that human errors contribute significantly to casualties and accidents [24]. Figures from 50% to 80% have been found in different industries [24, 25]. When challenges related to remote operations are discussed, the problem with human errors must also be included, and that implies that we must work both with Man, Technology and Organisational issues.

2.2 Motivation for incident response management

A common way to look at incident response is “we fix it when something happens”. This is a reactive approach that may work as long as incidents occur rarely and lead to minor consequences. But for many organisations ‘service disruption’ or ‘loss of information’ are unacceptable consequences, so they need to have a more systematic and proactive approach to the process of handling incidents. In a network of organisations with more complex interactions, it is more important to be proactive, to avoid unforeseen consequences of incidents [26].

It may be difficult to foresee what kind of incidents may occur, and how bad the consequences may be. There is also usually a difference between “most likely consequence” and “worst case consequence”. Planning for incident response is about being prepared and having processes and procedures that will make the job easier when the wave hits, no matter how serious it is. The choice of how well prepared one should be for harmless incidents compared to serious and catastrophic incidents will be an outcome from a risk management process.

2.3 Scenarios to illustrate typical incidents

Based on studies, interviews and workshops conducted with major operators within the oil and gas industry on the Norwegian Continental Shelf, we have identified some of the major risks related to integrated operations. There has been a common perception that the following four scenarios should be explored to reduce their risks and consequences. These scenarios are:

- Virus infection influencing ICT and SCADA systems
- Denial of service incident influencing the SCADA systems
- Insider, e.g. a disgruntled employee
- Missing situational awareness

2.3.1 Virus infection

Incident: A computer virus is being distributed from a supplier to an operator when a supplier's computer is connected to the production network. Based on discussion with the industry, virus from suppliers' computers is perceived to be one of the most common causes of virus infections offshore.

Reason: The rules for security measures and patching differ between the partners. IT components in the production network has not been regularly updated or patched and there is no logical separation or barriers present between the supplier's computer and the production network. This may be due to practical reasons; it makes it easier for suppliers just to connect and fix any problems.

Detection: A computer is set up to log data and print specific reports from a process control component. Nobody is sitting at this computer, but it is checked periodically by people from the instrument department, they walk by and see that everything is ok and that reports are printed. Every time they pass by, the computer is in the middle of a boot process and appears to operate normally afterwards. After a week of several repetitions the helpdesk is contacted, and it turns out that a virus infection had occurred.

Consequence: Service disruption, possible reduced production and reduced profit. Possible disruption of safety instrumented systems that may lead to safety incidents or accidents.

Possible improvements: Increased situational awareness of the virus threat may lead to earlier understanding of the problem among the employees. Scenario training on handling virus and worm attacks in the production systems offshore and onshore will increase understanding on handling and mitigating factors.
Detection mechanisms for virus attacks should be in place.
Stronger barriers between the supplier and production network such as stricter rules and procedures for connecting suppliers' computers to production network in addition to testing of organisational and human barriers in addition to testing of technical solutions.

Implications for incident response: Other systems may become infected, this must be explored. Overview of which systems are connected to the infected system, and which other systems are likely to have been used by the same supplier are needed. Need to consider whether to shut down or isolate the system or accept the infection in a period. Learning from the incident should also take place at the suppliers.

2.3.2 Denial-of-service

Incident: An IT component at an offshore production site is exposed to a denial-of-service (DoS) attack due to a malfunction (this could also be the result of a malicious attack). The system does not have enough capacity to handle the increased traffic load, leading to breakdown of

communication and shut down of production and possible impact on SIS (Safety Instrumented Systems).

Reason: A component malfunctions and continually sends out error packets. At a test at CERN [27], it was discovered that 30% of the SCADA components stopped, if they were subject to DoS or erroneous traffic.

Detection: The attack prevents data communication between onshore and offshore control rooms and jams the production network. This could also jam the network of safety instrumented systems. The incident may be difficult to identify offshore due to poor reporting in the central control room.

Consequences: Missing communication for a couple of hours, preventing optimized production and thus reduced profit. Work hours needed to restore system. Stop of production. Stop of safety instrumented systems, which may lead to safety incidents and accidents impacting HSSE.

Possible improvements: Testing of components prior to implementation. Alert if amount of traffic is above a defined limit. Improved barriers between production network and safety instrumented systems. Establish redundancy of critical IT components and ability to handle larger amount of traffic than expected during normal operation in order to improved resilience.

Implications for incident response: One need to be able to identify DoS incidents fast, and localize and disconnect the attacked component to limit consequences.

2.3.3 Insider

Incident: A disgruntled employee establishes a backdoor in the production environment, enabling a shutdown or creating a critical situation during production.

Reason: This employee has just got the message that he is fired because of workforce reductions. He is not happy with the decision and wants to get back at his employer. The employee has access to offshore production network, and can implement a backdoor or unfriendly software at will.

Detection: The backdoor itself may never be detected, unless it is used to launch attacks that will have visible consequences.

Consequences: The backdoor can be used for tampering with data, leading to reduced or halted production, disruptive services, problems with safety instrumented systems, disconnected communication between on- and offshore control rooms.

Possible improvements: Logging and reporting of changes in the production environment. Establish barriers to avoid, or carefully manage, outside control of critical operations offshore. Access policy based on “need-to-know”, regular updates of access rights, detection mechanisms for violation of access policy

Implications for incident response: It is important to be aware that insiders may cause incidents. When recovering from the consequences of this incident, it may be difficult to detect the root cause. The backdoor may therefore remain in the system. Insiders may also have the possibility to observe the incident response work and react accordingly. Two people should always be involved in incident management to ensure checks and balances.

2.3.4 Missing situational awareness

Incident: An external service provider closing down a valve in production on an offshore oil and gas platform. The service provider believed he closed down a valve in the test environment. Fortunately, the operator in the central control room offshore discovered what had happened and managed to open the valve, thus avoiding a critical situation.

Reason: Poor situational awareness among actors

Detection: Due to vigilance from operators at the central control room, the situation was discovered and mitigated. In general, it is a challenge to detect these kinds of incidents.

Consequences: If not detected: serious accident, possibly loss of life.

Possible improvements: Improved barriers, including permission from the central control room to do testing and changes offshore. Increased focus on scenario analysis/training.

Implications for incident response: It is important to document and learn from these incidents. Incident response must handle organisational, technical and human factors. Incident handlers should plan for incidents that may arise from internal misunderstandings, in addition to traditional external attacks.

3 Methods and findings

In developing an Incident Response Management (IRMA) framework and guide, a combination of different methods was used. Based on the proclaimed aim to improve information security in ICT systems for integrated operations through developing and implementing a method for Incident Response Management, there was a need to study the oil and gas industry's transition to integrated operations. This included both current status and future aims and developments within the industry. Furthermore, current approaches to incident response management as well as the current status for incident response handling in the industry were studied. These empirical findings are interpreted in light of relevant theory in later section of this report in order to develop the IRMA framework.

Several different methods were combined in the development of the IRMA system:

- Interviews with key personnel in the Norwegian oil and gas industry [28]
- A case study of incident response management practice at an oil and gas installation in the North Sea
- A risk and vulnerability assessment of information security breaches on infrastructure and in work processes at an offshore installation
- A study of relevant cultural aspects by the CheckIT tool
- A workshop on information security and integrated operations [2]
- A workshop on the main findings of IRMA in the Norwegian offshore industry
- System dynamic workshops [29, 30]
- Participation in periodic OLF workgroup on information security meetings

These methods and the related findings are described in the following parts of this section.

3.1 Interviews

9 interviews were conducted by phone in the period of March-June 2007. The interviews took about 1 hour each. The interviews aimed at exploring how ICT/SCADA incidents were handled in the Norwegian oil and gas industry. This aim was approached by looking at how incidents were practically dealt with and how the informants believed a best practice for IRMA should look like. See Appendix C for the interview guide. Each interview was made by two researchers from SINTEF. In the analysis of the data, we have taken into account that a few operators are responsible for a majority of the activity on the Norwegian Continental Shelf. .

The interviews showed the following main patterns (see [28] for a detailed result matrix):

In general

- There are very few information security incidents that have impact on production (1-2 years between each incident.)

Plan phase

- There are many plans for different parts of incident response at the studied organizations. These plans have different level of details. A short and common plan, documenting incident response management incorporated in the organization is usually missing. Responsibility is not always clearly defined.
- Scenario training is seldom done (A scenario could be established based on several "Defined hazard and accident situations" (DFUs)).
- There are seldom discussions of defences in breadth; covering organizational and human factors in addition to technical issues. Technical issues are often covered exclusively.
- Awareness and proactive unrest related to information security could be improved. Knowledge and understanding of information security could be improved, especially among suppliers.

Detect and recover phase:
- Time and resources are seldom used to analyze logs from firewalls.
- When an incident is discovered, he who discovers the incident notifies a responsible person (ranging from platform manager to ICT professionals to help desk) about the incident

Learning phase:
- The learning phase is considered to be important. However, some informants were worried whether learning actually had any effect for future activities, and feared that learning was quickly forgotten
- Incident learning is seldom done in depth, Root causes are not always identified, and discussions does not always involve ICT and process professionals together, and lessons learned are not published
- The reporting systems are seldom tailored to information security, and there are often many varying reporting systems
- There is lack of frankness about real incidents. A change of focus is needed in the industry to make experience transfer both inside the organization and to external organizations possible.

3.2 A case study of incident response management practice at an oil and gas installation in the North Sea

In early stages of the IRMA project, a case study at an oil and gas installation was performed. The case study aimed at describing how incident response management was performed in practice in a selected offshore installation. Interviews, meetings and document studies were used in the study, which showed the following main results:

Plan phase:
- There are some awareness creation activities, which among other subjects also includes information security
- There is a procedure for handling virus infections. There are no other relevant procedures for incident response

Detect and recover phase:
- If there is a virus infection in the SCADA systems, it might take weeks before the infection is detected even if the system is not operating normal.
- More research is needed on tools used in the detection phase; warnings; aspects of time; securing evidence; and use of Synergi for reporting incidents.

Learn phase
- There is no communication within the organisation about real incidents
- When incidents happen, there is limited learning in the organization from these incidents
- More research is needed on documenting of the incident handling process; and internal and external learning

In general
- The incident response management at the studied installation has a potential to be more systematic and planned.

3.3 Risk and vulnerability assessment

To gain more insight into the risks involved in IO, a risk and vulnerability assessment was conducted based on the work process of daily production optimization of an offshore installation. Small-scale workshops with managers were performed to identify incidents and assess the risk of these incidents.

This assessment and the knowledge attained by analyzing the coupling and dependencies of ICT-systems, vulnerabilities, responsibilities, possible consequences of various incidents and how incidents are usually detected and recovered gave a basis for further work as well as implications for the assessed installation.

A detailed description of the risk and vulnerability assessment is not included in this report due to confidentiality. However, some generic findings relevant for the IRMA system are presented here.

The most critical incidents identified in the risk assessment were (in generic terms):
- Operation centre goes down jamming SAS/SCADA
- SAS/SCADA goes down
- Virus/worm infects the system from external sources
- Missing situational awareness from central control room operator

The risk assessment suggested the following risk reducing measures relevant for IRMA (in generic terms):
- Monitor the stability of the SAS/SCADA equipment when it is integrated with ICT infrastructure
- External PCs should be scanned and checked prior to being allowed in technical network or offshore network, or supplier should guarantee that the equipment are without viruses
- Incident reporting and learning from incidents should be improved
- The responsibilities related to technical network and the integration of ICT/SCADA systems should be unambiguous and monitored
- Awareness, safety and security culture should be improved onshore and offshore
- Common risk assessment among the actors in the organizational network should be established and sustained
- Emergency response plans should incorporate information security incidents

3.4 Key challenges at an IO installation, identified by the CheckIT tool

The Check IT-tool (see section Appendix H) was used to identify some key challenges related to an IO installation in a half-day workshop with ten managers and staff members in an oil and gas company. The key findings of the CheckIT-study relevant to IRMA were:
- Information Security is not integrated satisfactory in project and new installations
- Suppliers and service providers are not satisfactory involved in incident planning, detection and learning
- Rules and procedures related to information security are sometimes ignored to reach productivity goals
- The identification of critical ICT systems is not satisfactory, and HAZOP analysis of ICT/SCADA systems is seldom done.
- Information security responsibilities on offshore installations should be more clearly defined
- In general, the personnel on offshore installations have a low level of awareness related to information security (e.g. regarding spyware and virus)
- Communication of information security issues could be improved.
- Management is demonstrating their commitment to information security
- Information sharing of information security incidents in the industry is not satisfactory

3.5 Workshop on information security and integrated operations

A workshop on information security in integrated operations was arranged by the Norwegian Petroleum Directorate, the Petroleum Safety Authority Norway, The Norwegian Oil Industry Association and SINTEF in November 2006 [2]. The workshop aimed at 1) creating awareness on information security in integrated operation among different organisational groups (ICT, HSSE, automation and operations); 2) creating an arena for experience transfer and networking; and 3) identifying possible measures. 46 participants from the oil and gas industry, the power supply industry; public agencies and research institutions attended the workshop.

Several information security issues in integrated operations were discussed in parallel group discussions, including IRMA-related topics. The main findings relevant for IRMA (mainly important for the plan phase and reporting of incidents):

- Measurement of information security (indicators) is needed to evaluate whether the security level corresponds to policies and regulations; to evaluate effects of measures and to integrate information security with other business areas.
- Measurement of information security should be done with some kind of reference point, e.g. the OLF-ISBR [1].
- Information about ICT/SCADA incidents must be distributed in the organisation. Experience transfer and narratives should be utilized.
- Encourage incident reporting
- Simplify routines for reporting, including feedback on the reports
- More work is needed to study how to develop a reporting culture; how to inform about incidents; and how to develop a best practise regarding reporting and handling of incidents.
- Defined hazard and accident situation (in Norwegian: DFU, "definert fare- og ulykkeshendelse") scenarios that include training and preparedness for ICT-related incidents is lacking.

Additionally, some findings were relevant as background information for developing a framework for IRMA:

- There is a gap in communication between different groups of professionals offshore, i.e. HSSE, ICT and process
- ICT-routines are not adjusted to the offshore reality.

3.6 Workshop on main findings from IRMA

In October 2007 some of the main findings on IRMA in the offshore industry were discussed at a workshop. About 15 participants from the industry, governmental agencies, consulting companies and research institutions participated at the workshop. The main discussions at the workshop were about the following subjects:

Plan phase:

- One needs to perform risk analysis in the plan phase of IRMA as a decision support for how IRMA should be planned and performed. The plan phase of IRMA must appear as a proactive management approach, in which risk analysis should be a central part
- There are no requirements to report information security incidents

Detect and recover phase:

- It is important that those who discover an incident or suspicion of an incident know who to notify
- One must define possible incidents and then see which channels for reporting that is the most efficient for those incidents, e.g. perform a risk analysis

Learn phase:

- A module for information security is needed in Synergi[3]. Contractors fill out a form, which is registered in Synergi by someone else. It is a challenge that different parts and of the organisation have different traditions for reporting incidents. For example, our experience is that control room operators do not report incidents, since they only handle the consequences of incidents, not the incident itself.
- An information security forum for the oil and gas industry is an interesting idea, but the industry must decide what such a forum should be used for. It is important to include different professions in such a forum.

[3] "Synergi® is an integrated business solution, which provides your organisation with the tools you need to manage and reduce operational and business risk." http://www.synergi.com/

General:
- There are different views on what an ICT incident is
- Some participants doubted that there were so few incidents that the IRMA project had uncovered in the industry by the empirical studies.
- Is historical data on incidents relevant for IRMA in integrated operations? New technology and new ways of organizing work may change the relevance of historical data.
- If it is difficult to make a list of incidents, another possibility is to use scenarios.

3.7 System dynamics workshops and cooperation with the AMBASEC project

In 2005 the AMBASEC[4] project, in collaboration with the IRMA project team, carried out two Group Model-Building Workshops, also referred to as System Dynamic Workshops, The objective was to reach a deeper understanding of:
- The information security risks in the transition to integrated operations within the oil and gas industry. The processes included building a System Dynamic Model.
- The implications of the transition to integrated operations for incident handling

Participants in the workshops were representatives from Hydro and the research teams in AMBASEC (AUC), IRMA (SINTEF) and NTNU. During the workshops experts from the University of Albany (UA) acted as facilitators. The Brage oil field, operated by Hydro was in the forefront of the transition to integrated operations and was used as a pilot case.

The results from the workshops and the collaboration between IRMA and AMBASEC are documented in two reports [29, 30] and several scientific publications [31-34]. The areas of discussion included identifying key indicators and dynamic system stories to anticipate change in a system's state over time.

In the first workshop in May, a first version of a system dynamics-model for the transitions to integrated operations was established. and a set of stakeholders and their influences on possible outcomes for security in IO were identified. [5]'Two dynamic stories were developed with the intent to show the relationship between operational change, security and the stakeholders "Virus exposure in virtual organizations" and "The effect of the introduction of compliance mechanisms to suppliers and contractors."

During the second workshop in September the attendees discussed a risk and vulnerability analysis for the work process "daily production optimization", and came up with different views on how work processes will develop in the future of IO.

Findings from the first workshop in May included;
- Monitoring risk change should be given high priority when developing new policies in the industry related to incident reporting, creating CSIRTs[6] and raising awareness.
- Transitions from traditional to integrated operations create vulnerabilities. The timing of these vulnerabilities may depend on how well the organization is able to change its operating processes, train its staff and contractors, and gain acceptance of the transition.
- Successful implementation of collaborative arenas reinforces their effectiveness. On the other hand, limited success will likely slow acceptance of this innovation, and increase the resources required for subsequent rollouts, or possibly derail the project.

[4] AMBASEC (A Model-based Approach to Security Culture) is a project, anchored at Agder University College (AUC), sponsored by the Research Council of Norway and in collaboration with IRMA
[5] Examples of stakeholders are oil company (system owner), chief executive officer, platform chief, control room manager, incident response team manager, Ptil, media etc
[6] Computer Security Incident Response Team

- The transition from existing to new work processes will introduce new security issues and potential for security lapses. These problems, if not detected and mitigated, are expected to increase the resistance to further change and adoption.
- Delays in learning and reflection may reduce the migration to integrated operations. Development of a capacity to detect problems and learn from them may facilitate future transitions. Conversely, a limited capacity to detect problems as they occur will obstruct change and delay corrections, increase risk, and put the project at greater peril.

The second workshop in September was focused on the implementation of a new workprocess in the Brage oilfield. Simulation on the SD-model where the parameters were adjusted by the experts from Hydro brought forward a set of hypotheses:

- Maturation and adoption of technology enables work processes and transformation.
- Introduction of new technologies and work processes can create knowledge gaps and vulnerabilities.
- More communication off-platform reduces resistance to change, which enables adoption of mature processes.
- Incident reporting creates a stock of knowledge of incidents, which allows us to bring on mature work processes and improves rate of getting mature technology online, reducing vulnerabilities, incidents and damage.

Several papers on the system dynamic model combined with findings from other studies created more insight;
While the effects of this work on the proposed e-operations migration are not by any means clear, the group model building process achieved several important outcomes for the participants.

- The qualitative models identified several problematic areas in the transition. The potential for a Knowledge Gap and a Work Process gap reinforced the importance of timing and knowledge sharing.
- The long-term effectiveness of CSIRT activity on the ability of the firm to develop a strong security culture is dependent upon a move beyond damage repair and into active learning.

From a methodological perspective, the results had two additional important outcomes:

- Group model building engaged and focused a diverse set of experts and modellers to develop a holistic, systems view of a problem. This was particularly gratifying given the initial scepticism expressed during the planning of the meeting.
- Through the feedback models, a wide set of interrelationships emerged that influence the success or failure of both the e-operations and the CSIRT initiatives.
- Though little hard data was available, the participant's knowledge of the general structures and behaviours in their environment was sufficient for credible and understandable causal modelling. This is a crucial finding in high-threat environments, as little data is ever made available outside the secure environment of the firm.

On the importance of an incident reporting system: The state of information security is still relatively immature when compared to the state of safety. In the realm of safety there are numerous reporting systems, often mandated by law or if not directly by law, by high political pressure. Perhaps we will not see well-functioning incident reporting systems for information security before 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 completely out of the loop and are instead presented with a set of prescribed rules. However, this is a limited approach to user education. Users must be kept 'in the loop'; only then will they see the necessity and usefulness of following the rules prescribed by information security specialists.

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

3.8 OLF-meetings

The IRMA project team has been represented in OLF's workgroup on information security for the entire duration of the project. IRMA has thus contributed to the development of OLF guidelines 104 [1] and 108 (to be published). The OLF workgroup meetings have provided the IRMA project with important background information and firsthand access to operator and contractor personnel who are actively involved with offshore safety and security work. The workgroup meetings have also been used to discuss preliminary results from IRMA, and have provided us with useful feedback. Furthermore, the fact that we had contributed to the workgroup meetings made it significantly easier to recruit participants for our workshops and interviews.

4 Prepare

The *prepare* phase is where the organisation prepares to detect, handle and recover from attacks and other incidents. We have determined that there is a need for documented incident management plans which are founded on a risk analysis. The risk level that is determined by the risk analysis and external information should be communicated to all relevant employees, and this should include information on unwanted incidents that have taken place in the past. The incident management plan should consider organisational and human factors as well as technical issues, and must be designed to cope with the complex situation with operators and multiple contractors found on all offshore installations.

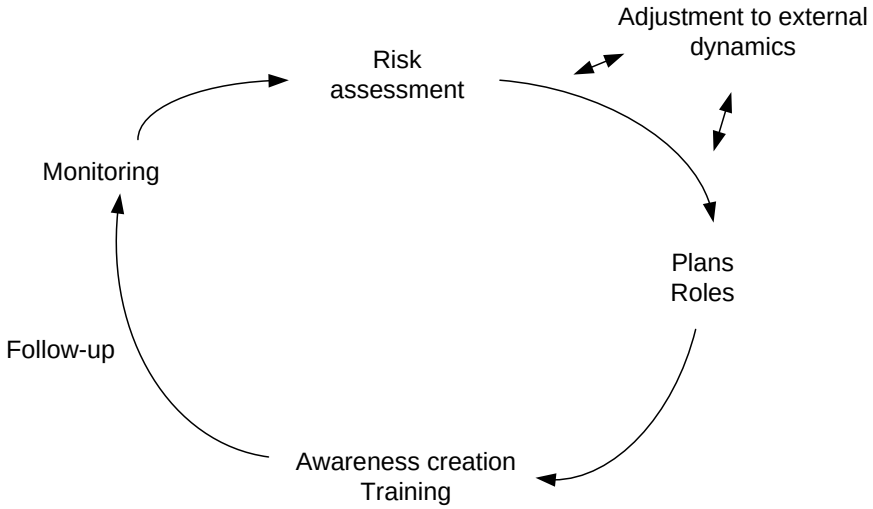


Figure 4-1: Graphic representation of the prepare phase

Figure 4-1 shows how different activities in the plan phase relate to each other. We argue that plans and roles should be based on a risk-based approach. Plans and defined roles must be implemented and followed up by awareness-creating activities at individual and organisational level as well as training activities. Monitoring procedures and key performance indicators are also important inputs to decisions regarding how incident response plans and roles are designed. All the activities in the plan phase must furthermore be adjusted to external dynamics, e.g. changes in competency, the risk picture (se section 4.1).

4.1 External dynamics

Incident response management does not operate isolated from other parts of the organisations and the organisational context. This is illustrated in Figure 4-2, which is inspired by Rasmussen's model of a socio-technical risk management system [35].

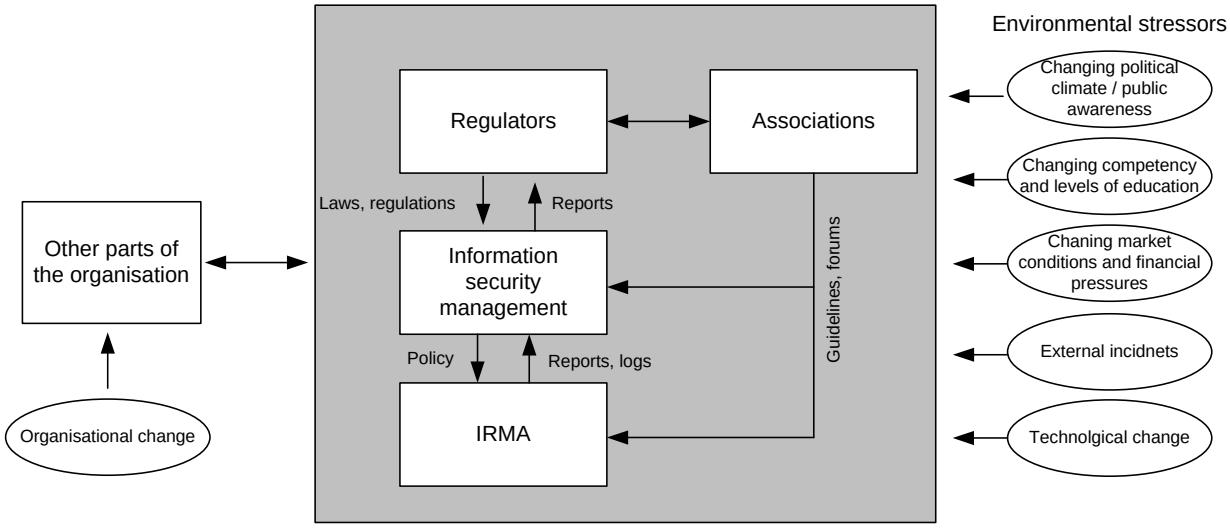


Figure 4-2: Incident Response Management in an organisational context.

The grey box in the figure illustrates the information security organisation, which includes incident response management, and its information security context. Incident response management is of course influenced by the general information security management strategy of an organisation. At the same time, information security management is influenced by incident response management, as information security management approaches must be adjusted to learning made in incident response management processes. Both information security management and incident response management are influenced by information security regulations. At the current moment there four cross-sectoral regulators on information security in Norway (the Norwegian National Security Authority; The Data Inspectorate; The Directorate for Civil Protection and Emergency Planning; and the Norwegian Post and Telecommunications Authority), in addition to several sectoral regulators, including the Petroleum Safety Authority Norway [36]. Various member associations also influence how information security management and incident response management is performed. In the oil and gas industry, the Information Security Baseline Requirements [1] developed by The Norwegian Oil Industry Association is of particular importance as a guideline for management

In addition to information security management approaches, incident response management must operate together with other organisational processes and structures, e.g. HSSE, economics, quality management, process and productions, etc. This is illustrated in the figure above as a mutual influencing arrow between the information security organisation and the box ‘other parts of the organisation’. Integrated operations imply that organisations change, so the box ‘organisational change’ has been added as an influencing factor. The change to integrated operations will also have implications for how incident response management is performed, as offshore activities become dependent on an adequate information security level and emergency preparedness.

The model also illustrates how environmental dynamics in society influence information security work at all levels in society. These are factors outside the organisation that influence the incident response management processes. Incidents at other organisations have high potential of experience transfer, and thus learning for incident response management. Technological change is of course an essential dynamic of information security: use of new software and hardware; new vulnerabilities in software; trends of use; converging technologies; and coupling of systems. Differences in competency are also creating changes, in particular the difference in experience,

knowledge and skills between e.g. old and young employees and offshore and onshore personnel. Market conditions and financial pressures also generate environmental stressors: e.g. technology-driven organizational development and automation. Public awareness and the political climate also influence risk management in society, e.g. by emphasis on terrorism but also on vulnerabilities in technology regarding for example air traffic control or the power supply.

Technical mechanisms such as Intrusion Detection Systems, firewalls and anti-virus software are vitally important in any modern computer network, and can detect (and often prevent) a large number of incidents in an automatic fashion. These mechanisms in themselves are outside the scope of IRMA, but it is important that alerts and warnings that they generate are handled in the appropriate manner, and followed up by the incident response team. The main task in the prepare phase is thus ensuring that there are routines that facilitate the information flow, taking both organisational/human and technical aspects into account.

Furthermore, the incident handling process must interact with changes in the global threat picture, technological change and innovation, and increased available information. This is a two-way street, in that the handling of incidents facilitates learning that is important to the general information security work in an organization. The information flow routines must therefore also ensure that system administrators and other relevant personnel become party to information (e.g. regarding new attacks and misconfigured equipment) from the learn phase.

4.2 Risk assessment with respect to incident response management

It is important to assess the probabilities and consequences of potential incidents that may occur, in order to prioritise activities and to identify if the mitigation represented by incident handling procedures is sufficient for a given incident type.

A risk assessment of the relevant ICT/SCADA systems should be performed regularly. To ensure that all relevant risks are identified, it is important to involve resources from ICT, process control (SCADA systems) and supplier/contractor. The usual activities in such a risk assessment are:

- Organisation and planning of the risk analysis
- Description of scope - defining object and relations to be analyzed
- Identifying possible unwanted incidents (and if relevant – frequencies and consequences)
- Description of risks and assessment of risk
- Identify actions to reduce probabilities and reduce consequences of incidents – including contingency plans
- Perform periodic assessment of the plan, and analyse relevant incidents to identify when the risk assessment should be updated

Risk analysis is a key activity to identify what can go wrong during integrated operations, and is important in the general security work that focuses on building barriers to reduce probability and consequences. For the work on incident response it is important to know what incidents to prepare for and focus on in e.g. plans and the work on awareness rising. Establishment of common risk perceptions is very important in a virtual environment such as in Integrated Operations.

Because every organisation has a limited set of resources, organisations should prioritize risk analysis of the systems based on potential impact. The organisation should perform a detailed vulnerability assessment for the highest-priority systems and assessments for lower-priority systems as resources allow. The vulnerability assessment will help identify any weaknesses that may be present in the systems that could allow the confidentiality, integrity, or availability of systems and data to be adversely affected, along with the related cyber security risks and safety risks.

The first activity is to identify the applications and computer systems within the scope of interest (e.g. ICT/SCADA), as well as the networks and interfaces. In addition, organisational and human factors should be included in the assessment: Which organisations are involved in the operations of the ICT/SCADA systems; what are the key Human Factors issues? The tool CheckIT (see Appendix H) can be used to identify organisational and human factors issues.

Identifying the vulnerabilities within an ICT/SCADA system requires a different approach than in a typical ICT system. In most cases, devices on an ICT system can be rebooted, restored, or replaced with little interruption of service to its customers. A SCADA system controls a physical process and therefore has real-world consequences associated with its actions. Some actions are time-critical, while others have a more relaxed timeframe. This will have implications for how to respond to incidents in these systems.

A risk matrix is commonly used to evaluate risks. Ideally all risks should be in the lower left quadrant (low impact and low probability). In the real world however, many of the risks will be in the upper right quadrant (high impact and high probability). These risks are not acceptable to the organisations, and by implementing security controls and measures the organisation will seek to reduce the probability or the consequence – or even better; both, i.e. move the risk in the direction of the arrow, into the acceptable zone.

In Figure 4-3 we have plotted the example scenarios described in section 2.3 in terms of their perceived risk – see section 4.2.2.

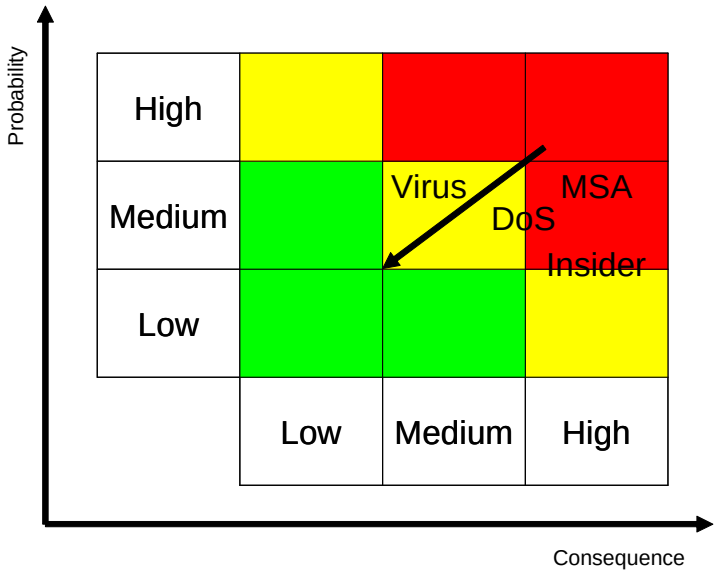


Figure 4-3: Example Risk Matrix

Example of a Probability (Frequency) scale:
P-Low: once every 10 years and upward
P-Medium: Between 1 to 10 years
P-High: Several times a year

Example of a Consequence Scale:
C-Low: Up to $1,000
C-Medium: $1,000 - $100,000
C-High: $100,000 and upward.

4.2.1 Monitoring and communicating the risk level

To ensure a proactive attitude, it is important to have a realistic perception of the risk level related to integrated operations. Monitoring of the risk level can be done by information from:

- Suppliers of ICT solutions such as Symantec or Norman
- The authorities, NorCERT see http://www.cert.no
- Breached barriers, activity logs from breached firewalls, or by utilizing Intrusion Detection Systems or "Honey pot" solutions (the specifics of such technological measures fall outside the scope of this report, however).

4.2.2 Risk assessment examples

The incident scenarios described in section 2.3 can also be used as risk assessment examples (more examples of risk assessment of real cases in a process control environment are described by Johnsen et al. [17]). For each incident scenario, the consequence of a manifest incident and the probability of an incident occurring must be estimated. For security incidents, determining the probability of occurrence may frequently be difficult, since it depends on active intent on behalf of unknown attackers. This is in direct contrast with safety incidents, where the components involved have clearly defined "mean time to failure" rates. However, the probabilities for security incidents will be influenced by the general threat picture and expert opinion (see section 4.2.1).

Scenario	Consequence	Probability
Virus infection	Medium	Medium
Denial of service	Medium to high	Medium
Insider	High	Low to Medium
Missing situational awareness	High	Medium

Table 4-1: Risk assessment of incident scenarios

Any incident that causes stop of production will most often result in a "High" consequence, since any stop in production causes large losses. It can be noted that all the scenarios presented in section 2.3 appear in proximity to the upper right quadrant; but this only to be expected, since the scenarios were selected for their relevance and importance.

4.3 Roles and responsibilities

The work on incident response must be organised in a way that fits the organisation. This means that who is assigned responsibility for the different tasks may vary. The important thing is that responsibility is assigned and that the responsible for each task has the requisite authority. In this section we outline who should be involved in the work on incident response management. We will focus mainly on the roles and responsibilities when it comes to incident response. It is important to have clearly defined beforehand who to involve when an incident occurs. However, one must also make sure that responsibilities are defined when it comes to the work defined for the Prepare and Learn phases.

4.3.1 Incident response team

With an incident response team we mean the group of people involved in handling an incident. The members of the team may vary with different types of incidents. The consequences and the technical expertise needed are important factors when determining who to involve in the incident handling.

In the following we list the main responsibilities when it comes to incident response:

- **Detect and alert:** Anyone who detects or suspects that an incident has is responsible for raising alert. Everyone should be aware of this responsibility and its importance.

- **Receive alerts:** Someone must be responsible for receiving alerts and, if applicable, who to alert next. Everyone must know who to alert in case they detect an incident.
- **Provide technical expertise:** Someone, either inside or outside the organisation, must have technical system and/or security knowledge, and this knowledge must be available in incident recovery.
- **Handle incident and recovery:** Someone must be responsible for leading the incident response work.

...and then we need somebody with

- **Authority to make decisions:** At least for incidents with potential serious consequences, management decisions will be necessary. Management must therefore be available.

The following is an example of roles that will be involved in handling of incidents:

- Platform manager
- Technical network manager (Process/SCADA)
- ICT/Telecom person
- Central control room operator

Although it would have been ideal to have a dedicated incident response (IR) team on a platform, practical realities mandate that incident handlers have to perform other duties between incidents. Thus, the IR team will be an ad-hoc organisation, and it is therefore important to define the priorities of the IR team members in case of an incident. It is likely that the team will consist of internal personnel with SCADA and ICT competence, and suppliers. Team members may be stationed both onshore an offshore.

Though the actual incident handlers will vary between incidents, there must always be a defined point of contact for raising security incident alerts (including both process control and ICT incidents). Two main options are available:

- **Alerting line management:** Line management will then be responsible for alerting those responsible for incident response handling.
- **Alerting a central support centre**; In most cases it will be sensible to integrate this with the normal helpdesk/support centre that is used for computer support

No matter which option is found to best suit the needs of the organisation, the important thing is to have a clear and unambiguous line of reporting in the event of an incident. Everybody should know who to turn to. The reporting point must be available 24 hours a day, 7 days a week. It may be advantageous to utilize the alerting routines available for safety incidents.

4.3.2 Responsibilities at interfaces between actors

For some incidents, the competence of the suppliers of the equipment affected will be necessary to deal with the incident. At least for important systems, suppliers' responsibilities in case of incidents involving their systems should be included in contracts. Preferably, this responsibility should be part of standard-form contracts. A list of contact persons [6] that can be called during incident handling should be available.

The responsibilities of contracted personnel and suppliers in case they detect or suspect an incident should be clearly stated and communicated. The responsibility for raising incident alerts should not only apply to internal employees, but everybody on platform.

To improve incident preparedness, openness about incidents is important. If companies share incident experience, everybody will be better able to learn from others successes and failures. A coordinating body that can facilitate information sharing between all involved actors should be

established. This body should be administered from an industry organsation like OLF, and should maintain close communication with national bodies such as NorCERT and Ptil.

4.4 Planning 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 a part of the "prepare cycle".

A risk analysis will result in knowledge of the most important systems, the most likely incidents, and the incidents that may result in high consequences. This is important input when it comes to what to focus on in the planning process.

Some plans are directed towards people with special responsibilities. Examples are plans for preparing for, recovering from and learning from incidents. Incident handling is however also dependent on the general employees' ability to detect incidents, and every individual in the organisation must be familiar with the practical details involved with raising incident alerts. This is partly an awareness issue (see section 4.5), but also a matter of documentations – the procedures must be documented at the required level of detail, and the documentation must be available in a well-known repository.

In the following we will recommend plans for preparing incident management activities, plans directed towards detection and recovery from incidents, and plans for learning from incidents that have happened. We will also recommend that documentations of the important systems that may be affected by incidents are kept continually updated. This will ease the work on recovering from incidents.

4.4.1 Plan for preparation for incident handling

Chapter 4, of which this section is a part, describes activities that are important when preparing for incident handling. These activities should be described in a plan with a focus on:

- Who is responsible for the different activities
- When and how to perform the different activities

The IRMA wheel in Figure 1-1 and the overview of the prepare phase in Figure 4-1 both focus on continuous learning and interaction with external dynamics. This means that the activities that are part of the Prepare phase should be revisited, either periodically or because of incident learning, changes in risk, new working methods, etc., to ensure that preparations are continuously improved. The continuity of the Prepare phase should be described in the plans with a focus on what triggers the different activities.

A plan for the prepare phase should be closely linked to any security policies of the organisation.

4.4.2 Plan for detection and recovery from incidents

Interviews and workshops performed as part of the IRMA project has shown that clear and simple guidelines for how to detect and respond to incidents often are missing. As a response to this IRMA recommend to create a plan for incident response, which consists of three main parts:

1. **A plan on what to do if being the one that detects or suspects that an incident has occurred:** This plan is directed towards all employees, including contractors and suppliers. It should be readily available (e.g. intranet, posters) and easy to understand, meaning that it should be short, precise and follow common terminology and common perceptions. The plan should describe:

- What is an incident, with examples of when to react
- How and where to raise an alert, and the importance of doing so
- What to expect, e.g. what will typically happen with the alert and what information to expect back

2. **A plan for how to detect incidents with the help of tools, routines and information sharing:** This plan is directed towards those responsible for the work on security, and should describe:
   - What tools are available and how and when to follow up those tools (e.g. checking of logs, IDS alerts)
   - What external sources to follow up (e.g. mailing lists, suppliers, other organisations) to get information on new threats and attacks that may be on the way
   - Who is responsible for all tasks described
3. **A detailed plan for how to respond to different types of incidents:** This plan is directed towards those responsible for recovery from incidents, and should describe:
   - What information to collect and document during incident handling
   - The main steps of incident handling (in chapter 5 we suggest the steps Assessment, Immediate responses, Escalation, Further responses, and Communication)
   - A plan for how to respond to different main types of incidents, including severity scale, who to involve, main steps that should be taken
   - How to balance the need for information security and the need to keep up production also when minor incidents has occurred
   - Who is responsible for the different tasks

Part of the plan can take the form of STEP diagrams or similar that graphically show the steps involved in handling specific types of incidents. This will ensure consistency in handling common incidents. An example STEP diagram that describes a plan for handling a virus incident can be found in Appendix F. More detailed recommendations on how to detect and recover from incidents are provided in chapter 5. The contents of that chapter can be used as inspiration for creating a plan that fits the needs of the organisation. The plan should be revised based on:

- Experiences made during incident handling (see chapter 6 for how to learn from incidents)
- Results from monitoring of the incident management work (see section 4.6)
- Changes in the priority of and/or the organisation of incident management
- New threats

4.4.3 Plan for learning from incidents

Interviews and workshops performed as part of the IRMA project has shown that systematic analysis of incidents to achieve organisational learning is often not done. Learning should be a natural part of incident handling that should be planned beforehand and that should be allocated necessary resources. It is important that management understand the learning potential represented by incidents and support learning activities, and the benefits the community as a whole can gain from openly sharing information about incidents.

Chapter 6 describes the Learn phase of IRMA. A plan for learning from incidents can use the steps presented in that chapter. That will assure focus both on what happened and what led to the incident, as well as a focus on how to improve incident handling. Important elements are:

- **Team based approach;** open discussions including representatives from ICT, SCADA, management, contractors, other relevant organisations, etc. onshore and offshore.
- **Structured incident analysis;** identify the circumstances of which the incident was an outcome, as well as the process involved in handling the incident. Cover organisational, technical and human factor issues. Make recommendations.

The resources spent on learning should depend on the seriousness of the incident, as will be further discussed in chapter 6. An important part of a plan for incident learning is to state the criteria that shall be used to decide who to involve and the time that should be used for learning from a particular incident. It should also be clearly stated who is responsible for the different learning activities.

As important as developing a plan for incident handling is to assure that the organisation is willing and able to accomplish learning:

- **Management commitment:** Is management committed and willing to use resources on incident learning?
- **Learning culture:** Is there a culture that supports reporting and learning? What is most important: learning how to improve management of incidents or allocating blame? Do employees feel obliged and empowered to report promptly and accurately all incidents, and are they confident that they will be valued for doing so? Do HSSE performance targets tend to act as a disincentive to reporting accidents and incidents?
- **Capabilities:** Do key persons have necessary knowledge, training, guidance and support?
- **Willingness to change:** Is there a clear link between the outcome of the learning phase and the work on preparing for incident handling and implementing preventive measures? Are there effective means in place to communicate conclusions back to stakeholders and to track closure? Is the implementation of recommendations managed to an agreed timetable?

The CheckIT methodology (see Appendix H) can be used to aid in reflection on the level of possible organisational learning and to establish necessary meeting arenas. The suggested key question from CheckIT to be discussed related to organisational learning are:

4 - To what extent are unwanted incidents analyzed and used as a learning experience?
5 - To what extent are reporting of unwanted incidents appreciated?
7 - To what extent are experience transferred between your company and other companies?
8 - How is experience feedback used in the organisation?

Use of CheckIT represents an assessment of the security and safety culture, going from denial culture (Score 1), rule based culture (Score 3) to learning/generative culture (Score 5). Organisational learning is a challenge if the score is close to the denial culture, but it is an integral part of the way things are done, if the level is around the learning/generative culture.

4.4.4 Documentation of system information

When recovering from incidents, there will be a need for technical competence and an overview of the technical equipment that is or may be affected by the incident. The ISBR [1] mandates that there shall be a record of all equipment used on an installation. It is important to maintain a list of all computing equipment with the following information:

- Type of equipment
- Name (if any)
- HW address(es)
- Network address(es)
- Physical location
- Software version(s)

In addition, there must be a network map which shows how the various parts of the network are interconnected. Since the configuration changes frequently, this information must be maintained electronically, and it must be convenient and hassle-free to add or update information.

For each possible target machine or system there should be an understanding of whether downtime is acceptable or not. For some components in a process network, downtime is not acceptable unless keeping them running may have serious consequences regarding life and health. Just the installing of patches that is not yet tested completely, is not an acceptable action. This is a big difference from traditional IT systems where downtime is more common and is hardly regarded as that serious.

4.5 Developing incident handling awareness

The motivation for increasing security awareness is twofold:

- Preventing incidents from happening
- Improving the ability to detect and react on incidents

Both these aspects are important. Our focus is on the last bullet – detection and reaction. The measures suggested will be directed towards achieving this last aim, though it is likely that increased awareness will also result in incidents being prevented. As an example: In Section 2.3 some typical incidents were outlined. One of them was a virus finding its way to the production system via the computer of a supplier. This incident could have been detected, and thereby reacted to, earlier if those who observed the infected computer had reacted to the abnormal behaviour of the computer and filed a report. For this to happen, the general knowledge of and awareness of virus attacks need to be on a sufficient level. But then again, awareness of the danger of virus attacks could have prevented the supplier from connecting an infected computer to the network, thereby preventing the incident to happen in the first place.

Building security culture in an IO setting comes with some special challenges:

- Shift work
    - Awareness campaigns need to have a long duration to reach all workers
    - It is easy to forget the new things learned – especially when one is away from work for several weeks
- Several organizations involved
    - Different security cultures
    - Need to address the whole virtual organization
- Several specialist communities involved (land & platform, ICT & process systems)
    - Need practice on how to work together
    - Different views on what is most important (confidentiality, integrity vs. no stop in production)
    - Speak different “languages”

ICT security incidents related to IO are also seldom reported, and the risks related to such incidents are therefore not very visible. As pointed out in one of the workshops arranged by the IRMA project [2]: Maybe one of the biggest challenges related to information security incidents is that we do not see them?

4.5.1 Management involvement

It takes effort and patience to build a security culture. Management needs to understand the importance of information security, and be aware of its role in building a security culture (see section 3.3 and [37]). Any policies should be signed by senior management. In the same way, management involvement will increase the impact of any awareness campaigns or initiatives, for instance by a statement saying that this is important for the corporation and why. The statement need not be written by the manager – but his/her signature is required.

4.5.2 Communication and cooperation across disciplines and organizational boundaries

When an incident occurs, several people from different disciplines (HCE, ICT, automation) placed on different locations (onshore and offshore) and possibly from different organizations need to cooperate (see section 3.3). As an example, a mechanic may be the one that detects some abnormality, reports this to the control room on platform which again reports to a central control room onshore. The equipment involved may be controlled by suppliers – resulting in a need to cooperate also with them. In an incident situation it is important that all those involved are able to communicate and cooperate efficiently. It is however unlikely that this will happen if one has not prepared for such communication and cooperation beforehand.

Issues that are probable to lead to communication and cooperation problems are [2]:

- Different skills and expectations when it comes to writing reports – the mechanic that detects the abnormality may for different reasons not be able to write reports of some minimum quality
- Different views of what is most important – e.g. minimizing the number of systems infected by a worm vs. prevent halt in production
- Differences in culture and technical competence.

The complexity of the systems involved makes it necessary to have people that are experts on different fields. It is however possible to prepare for cooperation between selected groups of people by e.g.:

- Establish meeting places
- Train on incident handling together
- Reserve some time to discuss incident response related topics like what to prioritize in case of an emergency – with a focus on “why we think like we do”.

Regarding the last bullet point, representatives from different groups should be involved in the risk analysis work (see section 4.2) to reach a common understanding of risks and how to react on these risks.

It is also important that those being “experts” on incident handling are aware of the importance of handling all reports in a serous matter – as viewed by those filing the reports. Reporting should be rewarded, and one should not risk looking foolish if the matter reported is not related to an incident.

4.5.3 Education and training

To be able to respond to incidents in an adequate way it is necessary to have knowledge of what to react on and how (see section 3.3). Different groups need different levels of knowledge. The system and security experts responsible for handling the incident need completely different knowledge than those using the systems in question to perform their different tasks – and that through their work with these systems may detect abnormalities that results from information security incidents [3].

Any education and training initiatives must be directed towards the different target groups to be successful. Based on risk analysis and knowledge of the organisation one should develop a communication plan that for each group describes what is required knowledge and how one plans to spread this knowledge [37]. There are several ways to proceed:

- Face-to-face training in small of middle sized groups is effective since it opens up for discussions and questions, but may be costly.
- Information on an internal website is less costly, but its effectiveness depends on the number of visitors of the page.

- Quizzes can result in increased interest and engagement.
- Posters with a simple clear message can be put up in areas where incidents may be detected – e.g. posters close to where computers are used that remind of the dangers of virus infections and what to do if one detects something suspicious.
- Screen savers
- Leaflets
- Regular email or newsletter
- Information to all new employees.

In all training and education it is important not only to spread knowledge on what to do when, but also to communicate why this is important [2].

Training related to incident response can profitably be combined with other training initiatives in the organisation. Incident response and security should be a natural part of the business, not something separate [3]. A possible way to build awareness is to define a relevant scenario to be explored between offshore and onshore installations. This could be done by using a DFU (A set of scenarios with defined dangers and emergencies, used in offshore training) involving unwanted ICT/SCADA events. Research indicates that scenario training (exploration of a DFU scenario) is important especially when implementing new technologies – such as integrated operations.

Information security aspects could be integrated in the DFUs already used, or new information security incident DFUs could be created. The following scenario can be explored together with other issues as a basis for a DFU:

> *As an example of how important it is to have common risk perceptions; in august 2005 the ZOTOB.E worm attacked a major Norwegian oil and gas company. As of the 15th of September, 157 PCs were infected, many of these were located on offshore networks. The probable cause of the attack was a portable PC that had been connected to the network by a third party supplier. One of the challenges facing the production company was poor understanding of the security consequences on safety critical production issues. The ICT staff had to explain the consequences to the operational staff at some length before suitable and adequate mitigating actions were taken - in this case patching and restarting PCs used in safety critical operations. Fortunately no accidents happened as a consequence of the infected systems* [17]

4.5.4 Established dissemination channels

Security awareness and security culture is not something you can build in one day. Changing culture takes time – and it is therefore necessary to establish long-term dissemination channels where information related to incident handling can be spread [2]. Preferably one should utilize dissemination channels that are already in place and used because these are more likely to work – at least in the short run. Examples of dissemination channels can be intranet pages, status meetings, e-mail, etc.

When an incident occurs it can be desirable to spread information related to this incident in order to facilitate organizational learning. In such a situation it is important that the dissemination channel to use is established and working.

4.5.5 Utilization of incident experience

Real incidents are more likely to be of interest than fictional examples. Experience from real incidents should therefore be utilized in education and other awareness initiatives. Incidents should be described as short stories that clearly show the importance of each and every employee in handling incidents (see section 3.3 and [2]).

In the “learning phase” of incident handling one will identify specific issues that should be learned from an incident. Long term learning from these incidents will only be achieved if the information is repeated. One should also utilize aggregated incident information [3] that is not spread to the organization right away.

4.5.6 Review and measure

Every corporation is different, also within IO. Measures that work perfectly in one setting may therefore be less effective at another time in another place. It is therefore important to periodically review which initiatives are working as intended, and which are not [37]. CheckIT (see Appendix H) is important in this setting – to be able to measure the security culture at a given point in time and identify the areas most important to work with.

4.6 Monitoring of incident response management

Monitoring the performance of incident response management is an important part of both the total incident response system as well as the general information security management system. Performance measures or indicators are well-suited for monitoring as they make incident response management visible for decision-making, communication, comparison and learning. Indicators even play an important motivational role, both at higher management levels and among the workforce. Additionally, indicators are used to show compliance with company security policy, industry standards and best practices, and public regulations and requirements (see Appendix D).

Performance indicators have been utilized for monitoring a variety of different business processes [38], e.g. financial results; production efficiency; market reputation; quality management; and HSSE (health, safety, security and environment) management. The field of safety management, particularly the oil and gas industry, has a tradition for using performance indicators for persistent feedback control [39]. Both information security management and safety management aim at loss prevention, thus experiences of performance indicators within the safety field has been utilized as background information for developing indicators for incident response management.

The principles for establishing norms for different indicators may vary. There might be a fixed goal established for a specific period of time, e.g. average time of response during a month should not be more than four hours. Another norm might be that an indicator must show continuous improvement from one period to the next. Furthermore, performance indicators might be used to evaluate whether a process is stable, by using control charts for several periods of time.

A set of performance indicators, which assists monitoring the incident response management scheme, is presented below. According to the requirements given in an overall security policy a proper subset of performance indicators should be selected. These indicators are discussed in more detail in [40].

4.6.1 Performance indicators for incident response

The table below shows the derived indicators, covering the three phases of IRMA. Each indicator is then described in more detail. The majority of the indicators presented should be derived from a reporting system. For the rest other monitoring tools must be used.

Phase of IR management	Performance indicator[7]
Plan and prepare	*1. Rating system for the quality of the IR management system*
	2. Assessment of information security culture with respect to IR
	3. Average order of feedback
Detect and recover	*4. Number of incidents responded to*
	5. Average time spent on responding pr incidents
Learn	*6. Total consequences of incidents*
	7. Number of incidents of high loss
	8. Downtime of SCADA systems due to incidents
	9. Total costs related to incident response

Table 4-2: Performance indicators

Indicator 1: *Rating system for the quality of the incident response management systems.*
This quality, i.e. how well-prepared the management structures are for handling incidents, is measured by looking at management elements such as feedback system, goals, documentation, management commitment, and education. It should also be considered to what extent necessary security mechanisms are in place. This indicator supports decision-making by specifying to what extent the planned incident response management system is appropriate for the context of the organisation.

Indicator 2*: Assessment of information security culture with respect to incident response.*
The concept of information security culture deals with the shared values and beliefs of the members of an organisation, which states the members' commitment to the organisation's information security management systems and performance, including incident response. This performance indicator will, among other things, identify whether employees are well prepared regarding incident handling. It may for example show that employees are not willing to report unwanted incidents. Consequently, one should develop measures such as training and awareness campaigns in order to increase the members' commitment to the planned incident response management system.

CheckIT (see Appendix H) is an example of a tool for measuring this indicator and improving information security culture. The focus of CheckIT is on security and safety culture in a network of cooperating companies performing integrated operations in the oil and gas industry.

Indicator 3: *Average order of feedback.*
It is of outmost importance to communicate the lessons learned from each incident to all parts of the organisation – to management, employees, operators, suppliers, contractors, and others. The order of feedback is an indicator of the degree of learning from previous experience. It also reflects what kinds of measures are taken after an incident. Is the organisation mainly doing fire fighting, i.e. correcting deviations, or is the whole organisation learning from the incident.
The indicator is measured be classifying the follow-up of each incident regarding five orders of feedback. Then it is possible to quantify the average order of feedback during a period of time, which can be periodically compared.

This indicator has been limited to learning within an organisation. At the same time, experience exchange to other organisations should happen as well. For a more sophisticated analysis of learning, this inter-organisational learning should be monitored as well.

Indicator 4: *Number of incidents responded to.*
An incident is being responded to when it is discovered, the responsible party is informed, and some kind of action is taken to deal with the problem. This indicator must be considered with

[7] All performance indicators are aggregated and the results tallied for a given period, e.g. once every 6 months.

care. For example, a major decrease in this number from one period to the next does not necessarily mean that the quality of the incident response management has changed radically, but may be due to external factors such as a change in the overall risk picture, or a few serious incidents that required the highest priority over other, less serious incidents.

Indicator 5: *Average time spent on responding pr incidents.*
This indicator says something about the efficiency of the incident response management. The time span goes from an incident is detected until the handling of the incident is finished. As an example, if the incident caused an abnormal situation for systems in operation, the handling of the incident is finished when the systems are recovered and again running in normal operation.
A trend analysis will show if this indicator significantly decreases or increases over time, which will give a more accurate picture of the efficiency of the incident response management, than just a comparison between two successive periods.

Indicator 6: *Total consequences of incidents.*
One of the ultimate goals of improving incident response management is to reduce the total consequences of all incidents. To compute the total consequences, one needs to sum up the consequences of every single incident one has responded to. One may rate the loss of each incident regarding different types of losses using a severity scale. To this scale one should add a money value scale, such as saying that for a consequence to be negligible the direct financial loss should be less than $10.000 or that injury to people should be limited to first-aid injuries. The table below shows a way to structure the assessment of each incident.

	Direct financial loss	Injury to people	Damage to the environment	Loss or damage of assets	Immaterial loss
Catastrophic					
Critical					
Serious					
Marginal					
Negligible					

Table 4-3: Total consequences of incidents

To estimate the total consequences of all incidents, one should sum up the matrices for each incident to see which types of losses have the highest occurrences. For simplicity, one may look only at the degree of loss. Improvement is indicated by a reduction in the possible loss of all incidents summed up.

Indicator 7: *Number of incidents of high loss.*
The incidents one wants to avoid the most are the ones resulting in the most severe loss. This indicator measures the number of incidents with the most severe losses, i.e. those incidents that are categorized as catastrophic or critical in the matrix in the table above. This indicator is very useful for risk communication to different stakeholders, will draw attention to the need of high-quality incident response management and will communicate the importance of awareness and willingness to react to incidents among employees.

Indicator 8: *Downtime of SCADA systems due to incidents.*
A SCADA system may be down due to an incident or due to planned maintenance. The former is relevant in connection to incident response. An incident does not necessarily result in downtime. This is why it is meaningful to use both this indicator and indicator 4 ‘time spent on responding to incidents’.

Indicator 9: *Total costs related to incident response.*
Responding to incidents requires investments, both for preparations in advance and when incidents actually occur. The total cost should be seen in connection with the total consequences of all incidents. A risk analysis must create the foundation for determining a reasonable balance between these two; so that investments on incident response are in proportion to the acceptable level of risk for consequences of incidents.

4.6.2 Monitoring threats from insiders

A significant portion of incidents are caused by insiders [9], by those who are authorized to use computers and networks. The indicators presented above do not distinguish between attacks from outside or inside. Obviously, indicators giving more specific information on insider attacks would be very useful for incident response management. Intensive studies in the last years have resulted in a suggestion for such indicators; implementation of security event management technology. In practice, this means:

1. Introducing dynamic and persistent policy control and activity tracking on document accesses. Users are constrained in their privileges (copy, print, edit, read. etc.) with documents and portions of documents even though the documents reside on the users' workstations.
2. Providing a detailed audit trail that tracks which documents, and portions of documents, are being accessed by whom and for how long.
3. Establishing alert levels for policy breaches

Thus users can be monitored on activities as

- Showing unusual interest in information outside the scope of their job, i.e. who violate the need-to-know principle, or who repeatedly make inquiries about projects to which they no longer have access.
- Collecting/storing classified material outside approved facilities.

The introduction of semantic technologies in retrieving and sharing information will enable even more sophisticated indicators of insider misuse.

4.6.3 How to follow up performance indicators

The performance indicators are aggregated incident information. The quality of the indicators depends on a properly functioning system for monitoring and reporting each incident. In turn the functioning of a reporting system depends on an active follow-up and use of the reports, clearly visible to those in the organization who has filed a report or could expect to do so.

Combining two or more indicators will produce better support for decision-making as it increases the understanding of how incident response management functions and the effects of implementing new measures. Examples are:

- The ratio of number of incidents with high loss to total number of incidents. This combination gives an indication of the change in the overall severity of the incidents.
- Comparing the consequences of incidents and the costs of incident response management. This will show the elasticity of the resources used to minimize the consequences. This is important input for cost-utility analysis deciding the amount of incident response management efforts.
- Average loss per incident of high loss can be created by the ratio of the consequences of high loss incidents to the number of incidents with high loss. A rise in this ratio signals higher loss per incident and thus the need to improve incident handling in general and particularly for high loss incidents.

There are lots of possible combinations of indicators that can be utilized. The main reason for combining indicators is to perform a more sophisticated and detailed analysis of the results the single indicators provide.
The indicators described above are specific for each organization. They should be supplemented with updated information on threats and vulnerabilities from external sources, in particular those applicable to the business areas of the organization.

This ensemble of information from the indicators should be used for several purposes:

- As important input to risk analysis and risk management
- To identify vulnerabilities in the technical security system
- To identify deficiencies in the security organization
- To monitor the efficiency of the incident response capabilities

5 Detect and recover

When incidents occur it is important to be prepared and have a plan for how to detect and handle the incident. In interviews and workshops performed as part of the IRMA project we have identified that incidents frequently are detected by coincidence. We have also identified that procedures are not always clear enough on how to deal with incidents, and that simple guidelines are needed. These guidelines should take into account that e.g. a virus should be treated differently in a process environment than in an ICT environment.

A plan for detection and recovery should be created as part of the prepare phase (see section 0). In this section we make recommendations as to what the contents of this plan should be. An overview of the activities we suggest as part of detection and recovering from an incident is shown in Figure 5-1. As can be seen from this figure, anyone in the organisation can be the one that detects an incident and is thereby responsible for raising an alert. This is further elaborated in subsection 5.2. When the incident is reported, someone in the organisation will be responsible for reacting to and handling the incident. These are referred to in Figure 5-1 as the incident management team. Who should be part of this team can vary depending on the type and seriousness of the incident, as will be further discussed in subsection 5.3. The main activities that should be part of recovering from an incident are also described in the same subsection. An important part of all activities is to document the judgements made and the actions taken. This is further addressed in subsection 5.1.

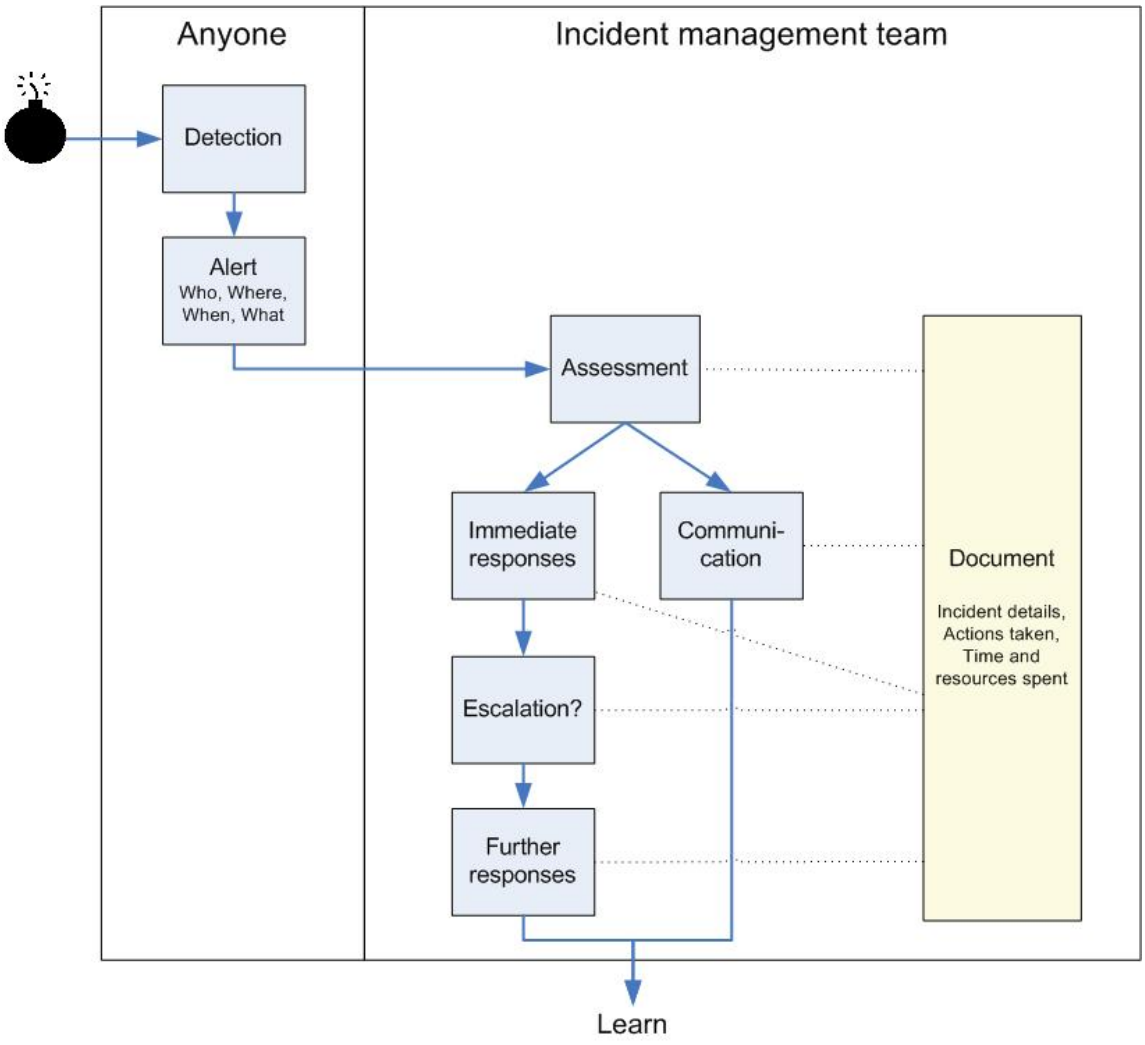


Figure 5-1: Overview of detect and recover

The recommendations made regarding detection and recovering form incidents are largely based on the "use" phase of ISO/IEC TR 18044:2004 [3]. Main differences are:

- The number of steps has been reduced. Forensics is not part of our model. We have also not included steps that depend on a special organisation of the incident management work.
- The special needs of IO have been given more consideration.

Recommendations are also based on TRANSITS course material for training of network security incident teams staff [41], and the NIST Computer Security Incident Handling Guide [6].

5.1 Document and prepare for learning from the incident

To be able to learn from incidents it is important to document any incidents that take place. This includes details on the incident itself and information on how the incident is handled. This way incident information can be shared between staff and one is able to look back and learn from earlier experiences [6, 41] and measure whether the work on incident handling is successful (see indicators in section 4.6.1).

Documentation of an incident starts when an alert about the incident is received, and continues throughout all steps in incident handling. Alerts can be communicated in different ways, e.g. orally (face-to-face or via telephone), via e-mail or some form on the intranet, or written on a piece of paper. Either way the one receiving the alert should make sure that important information is documented:

- **Who;** contact information of the one detecting the information unless he/she wants anonymity.
- **Where;** the system affected
- **What occurred when;** description of the incident and how it was detected

At this stage it is however more important to alert about incident than to provide adequate documentation, as stated in ISO/IEC TR 18044: "It is not good practice to delay the submission of a reporting form in order to improve the accuracy of its content." Raising an alert should be easy. Although all information on the incident ultimately may be registered in a database, it is probably not practical to raise alerts by providing input directly into this database – since this may increase the knowledge level necessary.

Documentation of the incident continues throughout all steps that are part of incident handling. The following information should be documented:

- **Incident details;** consequences, systems affected, reason behind, etc.
- **Actions;** actions taken and the reasons behind these actions
- **Time and resources spent**

Documentation should be made easy – the focus during incident handling will and should be on getting on top of things, and not on documentation. Any tools used for documentation at this stage should be readily available and easy to use, and those involved in incident handling should be trained in using them. Alternatively one could just describe actions taken in an unstructured document or in a logbook [6]. Structuring of documentation is part of the learn phase.

Synergi[8], which currently seems to be the established system for documenting HSE incidents, is probably not a good system for documenting an incident during detect and recover. If one wants to use a computer tool for documentation, Request Tracker[9] is one of several alternative systems.

[8] http://www.synergi.no/
[9] http://bestpractical.com/rtir/

5.2 Detect and alert

Information security incidents are mainly detected in two ways [3]:

- **Coincidence:** Someone notices something unusual – either technical, physical or procedural related – and becomes concerned.
- **Routine:** Equipment like firewalls, intrusion detection systems and anti-virus tools detects the incident automatically, or the incident is detected as part of the work of information security experts, e.g. by examining logs.

As mentioned above, interviews and workshops performed as part of the IRMA project shows that many incidents are detected by coincidence. This however does not reduce the importance of making an effort to detect incidents that occur:

- **Reports from suppliers:** Suppliers should be asked to report on incidents in their systems that may have consequences for your organisation. Responsibility for reporting incidents should preferably be part of contracts.
- **Regular controls of logs:** Error logs, logs from firewalls and intrusion detection systems, and other logs showing incidents of some kind should be checked regularly. Even though minor incidents have no direct impact on target systems or network, a collection of such may be of a certain degree of seriousness. It is important to act proactively in this respect.

A main challenge is the potentially high volume of signs of incidents[10]. Intrusion detection systems do have problems regarding false positives, it can be a difficult to identify what is an abnormal log entry and problems reported by users will in many cases be false alarms. Skills and experience are needed to be able to identify the real incidents [6].

No matter how the incident is detected, the person detecting the incident or the person that is notified by automatic means is responsible for raising an alert. This could be anyone in the organization – whether permanent or contracted personnel, or suppliers. The person's knowledge on ICT security can be limited. Yet, timely alerts are of high importance. It is therefore essential to build awareness and minimise the skills needed for raising alerts [3]. Each and every employee (including contractors, etc.) needs to know what to do if detecting irregularities in a system:

- **When to react;** everybody needs to understand what system behaviour is not normal and may be due to an information security incident (awareness, see ...)
- **What to do;** everybody needs to know who to alert if they detect something that may be a security incident.
- **Appreciation;** every incident alert should be appreciated, and no punishment should be risked. It must also be recognised that raising alerts take time [2] – and that this is a natural part of the job.

It is essential to clearly define who should receive incident alerts, and if applicable, who to alert next. Typical entities that may be involved are user support, incident response team, and management like e.g. platform manager. Some may prefer to have central user support (a telephone/-hotline) that is operated 24 hours a day, 7 days a week, and which further alerts an expert group and/or management. Others may prefer to alert line management and make them responsible for directing the alert to those responsible for handling the incident. No matter what approach is taken, the important thing is that everybody knows who to alert and how to do it.

[10] The NIST Computer Security Incident Handling Guide (sections 3.2.2 and 3.2.3) provides more examples on indications on incidents.

Who that in the end will be responsible for dealing with the incident may vary depending on the type of incident, the system involved and the seriousness of the incident. One can however not expect anyone that detects an incident to be able to direct alerts based on such judgements. We recommend raising alerts in the same way regardless of the type of incident, and leave it to the step assessment (5.3.1) that is part of incident recovery to take such considerations.

Regarding incident reporting there may be a lot to learn from the experiences within HSSE [2].

5.3 Recover from incident

In order to recover successfully and effectively from an incident, it is important to be well prepared, meaning that a plan and the necessary skills are in place. Important factors are [3]:

- **Clear responsibilities;** "distributing the responsibility for incident management activities through an appropriate hierarchy of personnel, with assessment decision making and actions involving both security and non-security personnel"
- **Clear procedures;** "providing formal procedures for each notified person to follow, including reviewing and amending the report made, assessing the damage, and notifying the relevant personnel (with the individual actions depending on the type and severity of the incident)"

The importance of this has already been stated in the Prepare phase (see section ?), and we will further return to these points throughout this section.

5.3.1 Assessment

When the incident alert reaches someone that is responsible for handling the incident, the incident should be assessed to determine the severity of the incident and the way forward. Important activities are [3]:

- **Acknowledge receipt of the alert:** Those reporting the incident should be informed that it is now taken care of.
- **Collect more information:** If necessary more information on the incident should be collected[11] in order to be able to state:
    - Whether it in fact is an incident
    - The scope of the incident, e.g. the number of machines affected
    - Can we handle this, and who need to be involved
    - The seriousness of the incident – is this a crisis situation, can it affect safety?
- **Alert those that need to be involved in handling the incident**

Who will be part of the incident management team may vary with the type and severity of the incident – and possibly with the time of the day. It is important to include both experts on ICT security and process control systems, so as to better be able to make good tradeoffs between e.g. security and production. Possible candidates are ICT security experts, system experts, management, and representatives from users of the system affected. Resources may be internal or external to the organisation, and it may be advantageous to involve suppliers. An important part of the preparation for this activity is to create a pre-determined severity scale or evaluation criteria for incidents [2]. Who to involve in the different types of incidents should as far as possible be planned beforehand, and the role and responsibilities of each team member defined (e.g. in a STEP diagram as described in Appendix F). Note however that planning for all eventualities is not practical, and one should rely on the team's ability to improvise if necessary.

[11] The NIST Computer Security Incident Handling Guide (sections 3.2.4 and 3.2.6) gives advice on preparations that will improve the ability to analyse incidents and help prioritise them.

Some incident alerts will report on situations that are not security related, and therefore does not require any recovery activities to take place [6]. Nevertheless, all incident alerts should be treated seriously, meaning that the one raising an alert should get the impression that the alert is appreciated and that it is treated appropriately. An important part of this is to report back on the actions taken [2]. Chris Johnson [42] calls this to keep the staff in the loop. They "see that their concerns are treated seriously and are acted upon by the organisation".

In the following we will not consider forensics. If forensics is important it needs to be part of incident handling from the start, and this should be decided at this stage. For more information on forensics, see e.g. RFC 3227 [43].

5.3.2 Immediate responses

One of the main things on one's mind during at least serious incidents is to "make it stop" and to limit further damage resulting from the incident. TR 18044 suggests several immediate responses, the main ones being:

- To disconnect from the Internet
- To shut down the information system, service and/or network, or isolate the relevant part and shut it down
- To activate surveillance techniques

The above responses are very much IT related. In a process control environment more specific immediate responses may be:

- To isolate the ICT part of the system (if this is where the problem lies), and continue with operations of the process system in order to avoid process shut down
- Disconnect the SAS from Internet and external networks completely
- Enhance the control of incoming and outgoing traffic on the target network (segment)
- Perform Process Shut Down (PSD)
- Perform Emergency Shut Down (ESD)
- Remove power from ESD system and restore, to ensure that the ESD system has not been inactivated

To be able to make good decisions at the time of an incident it is important to be prepared on what major types of incidents may occur and what actions to take in response to different incident types. The NIST Computer Security Incident Handling Guide [6] provides general information on how to respond to some major types of incidents, Specific incidents related to process systems are documented in the NIST Guide to SCADA and Industrial Control Systems Security [13].

5.3.3 Escalation

Deciding who should be part of incident handling has been described as part of the assessment step. During later steps it may however be that one finds that the judgements made initially is not yet valid. By escalation we mean to get help from outside the team. This may include:

- Involve additional technical experts from own organisation
- Involve experts from suppliers of equipment affected
- Involve external experts
- Involve management or crisis organisation

There may be several reasons why an escalation may be necessary:

- 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 and must be handled accordingly
- Need upper management decision

Guidelines on when to involve e.g. management or external experts should be available beforehand.

5.3.4 Communications

Depending on the incident, it may be necessary to inform selected persons within or outside the organisation of the matter, e.g. when the incident is confirmed as real, when it is under control and if escalated [3]. Persons that may need to get such information can be:

- **Management** at different levels; they may need to make decisions, and they should not first hear about the incident through other channels (e.g. the press).
- **Those affected** by the incident; people affected need information to understand what happens, how to behave and what to expect.
- **Press**; if the incident is serious.

Guidelines for whom to communicate with when should be available, and one should plan for how to effectively communicate during an incident. Note that electronic communication channels in some cases may not be fully available. Existing plans, for instance on how to communicate with the press, should be utilized. In stead of creating new plans, communication in case of security incidents should be added to these existing plans.

5.3.5 Further responses

When an incident is under control it should be identified what further responses are required to bring the system back to normal operation. This is the time for restoring systems, assuring that systems are in safe condition, reconnecting to external networks, etc. In this process it will often be necessary to:

- **Take immediate actions to reduce the vulnerability of the system**[12]**;** install necessary patches or improve the configuration of the system by changing passwords or disabling unused services [3].
- **Utilize tools;** installation media, backups and recovery tools, and possibly also integrity checks and investigation tools [41].
- **Be aware of malicious code;** trojans, rootkits and kernel modules can be maliciously placed in the current system, and are hard to detect [41].

Often it is considered that loosing some data is better than a (still) insecure system [41]. In a process control setting it is however important to balance the need for improved security and the need to keep the system up and running. It is therefore important that representation from both IT and process control are involved in decisions that will result in a shutdown of the system, or that may render the system unstable.

5.4 The end of recovery is the beginning of learn...

When everything is up and running and the incident handled it is important to use the experiences made as an opportunity for improvement. The documentation created during incident detection and recovery, and the experiences made by those involved in handling the incident can be used to improve the preparedness of the organisation to prevent and handle incidents in the future. This is the focus of the Learn phase that is presented in the next chapter. The activities of the Learn phase should be started when the incident is still fresh in peoples mind. But first: Remember to provide status information to the one that raised an alert about the incident. This is an important part of the work on awareness rising when it comes to incident management.

[12] Other improvements, like increasing the monitoring of the system and improve plans are identified as part of the learn phase.

6 Learn

This phase covers the learning process that follows an incident that has happened. Proactive learning related to anticipation - knowing what to expect - are treated in the prepare phase.

Incidents should be used as an opportunity for learning and improvement. Learning from incidents should be a planed part of incident handling, and the necessary resources must be allocated. The learning process we are suggesting is focused on organisational learning. Our aim is to change the incident response based on the difference between expected and obtained outcome (single loop learning) in addition to be able to question and change governing variables related to technology, organisation and human factors that lead to the outcome (double-loop learning). This is described by Argyris and Schön [44] and in the Check-IT method in Appendix H. Cooke [45] describes an incident learning system as "the collection of organisational 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" [46] [47] [26]. In the learning phase IRMA focuses on what lead to the incident, what happened, and how the incident was handled, by:

- Understanding how the incident happened and analysing barriers by using the STEP method
- Understanding how the incident was handled and analysing improvements by using a post-mortem analysis

Interviews and workshops performed as part of the IRMA projects has shown us that systematic analyses of incidents and organisational learning is a challenge in an IO environment, and is often not done:

- **Different organisations:** The IO-environment consists of personnel from different organisations onshore and offshore performing varying tasks. Learning among the involved organisations is not always performed.
- **Different background:** Related to the ICT/SCADA systems the involved ICT personnel have a very different background from SCADA/automation experts and a team consisting of ICT and SCADA professionals are not always collaborating when analysing the incident. Operators from the central control room (CCR) are seldom involved in the handling of the incident, or have any knowledge of ICT/SCADA incidents.
- **Limited causal analysis:** The root cause is not always documented.
- **Limited focus:** There is a focus on technical issues, organisational and human factors issues are seldom explored.

We have also learned that many different systems are used to register the unwanted incidents.

As a response to these challenges we suggest a form that can be used for all ICT related incidents (see Appendix E). This form will be completed as part of a systematic approach to analysing incidents and support organisational learning, as shown in Figure 6-1. For analysing the incident and suggesting barriers, four steps are suggested (further described in Sections 6.1 - 6.4):

1. **Commitment** and resources (do we commit to organisational learning and use necessary resources?)
2. **What occurred** – identify sequences of events using STEP
3. **Why** – identify root causes and barriers, and
4. **Document** safety and security recommendations

As a parallel activity we suggest evaluating the incident management process by performing a post mortem review and suggesting improvements (Section 6.5).

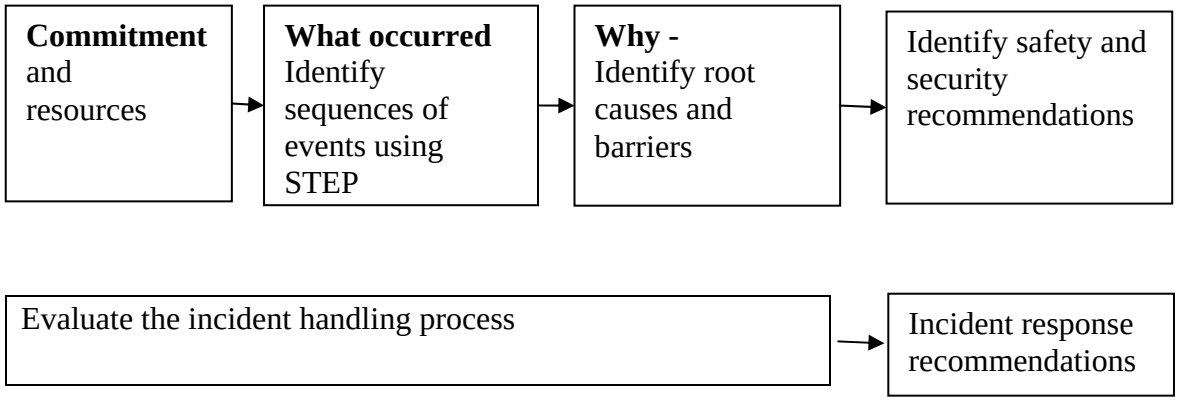


Figure 6-1: Team discussion and common agreement to increase organisational learning

The challenges identified above are addressed by:

- Including people from all involved organisations in the learning process
- Emphasising the need for both ICT security and SCADA experts in all meetings
- Focusing on identifying why the incident happened, in step 3.
- Focusing on organisational and human factors in the barrier analysis, performing analysis of the incident handling process, and including the detection and handling of the incident in the STEP diagrams.

The process of analysing the incident and identifying barriers should be performed in a team setting to improve organisational learning – focusing on agreement among the participants. Participants should be key actors such as management, control room operators and ICT and SCADA professionals, see Figure 6-2 inspired Mitropoulos et al [10]. Personnel from the team handling the incident should participate. If possible, all actors should participate in all meetings.

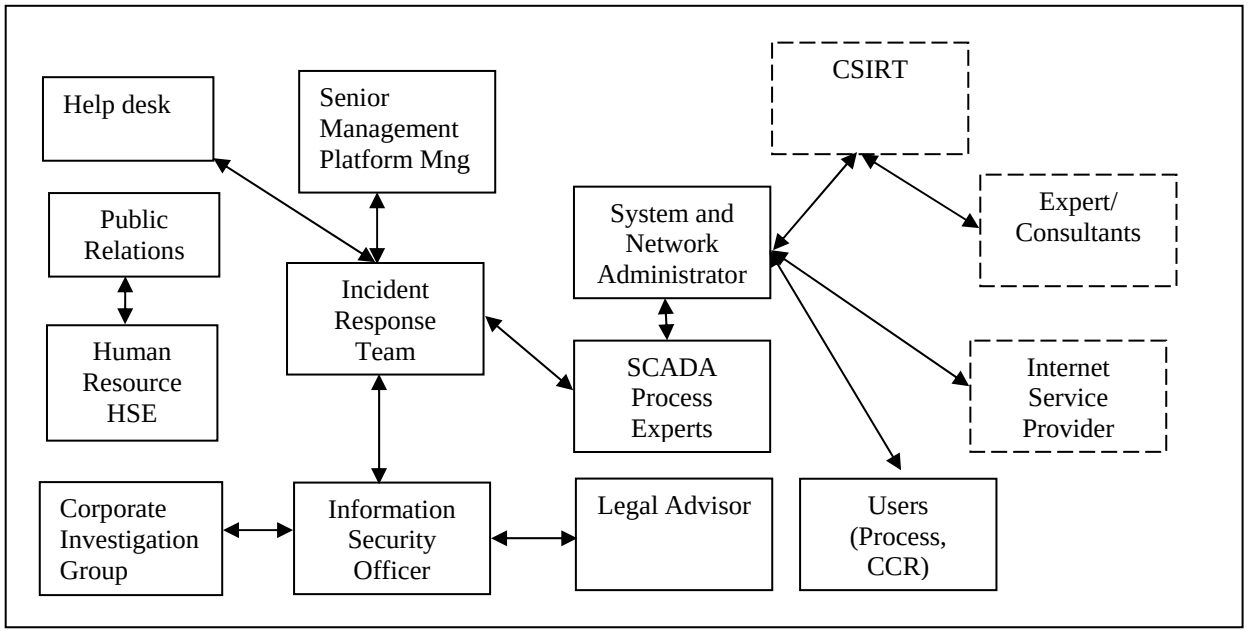


Figure 6-2: Incident response contacts and actors

The number of meetings (or workshops) needed is dependent on the severity and scope of the incidents and must be decided (see Figure 6-2). For a serious incident we suggest to arrange three key meetings focusing on:

- Meeting #1-**What has happened**; discussion in open setting to ensure that all participants do agree on the sequential steps describing the incident
- Meeting #2- **Why it did occur**; ensuring that there is agreement on all root causes
- Meeting #3-**Recomendations**; ensuring that there is common agreement on all recommendations and that the relevant actors accept responsibility of the proposed actions.

This process has the ability to improve organisational learning by involving resources with different background, enabling us to get a more complete picture of what has happened and possible improvements. By using a graphical representation such as the STEP diagram, it is easier to create a common understanding of what has happened among all the involved participants. By involving the management and ensuring that they agree on what should be done, it is easier to identify mitigating actions that need to be implemented.

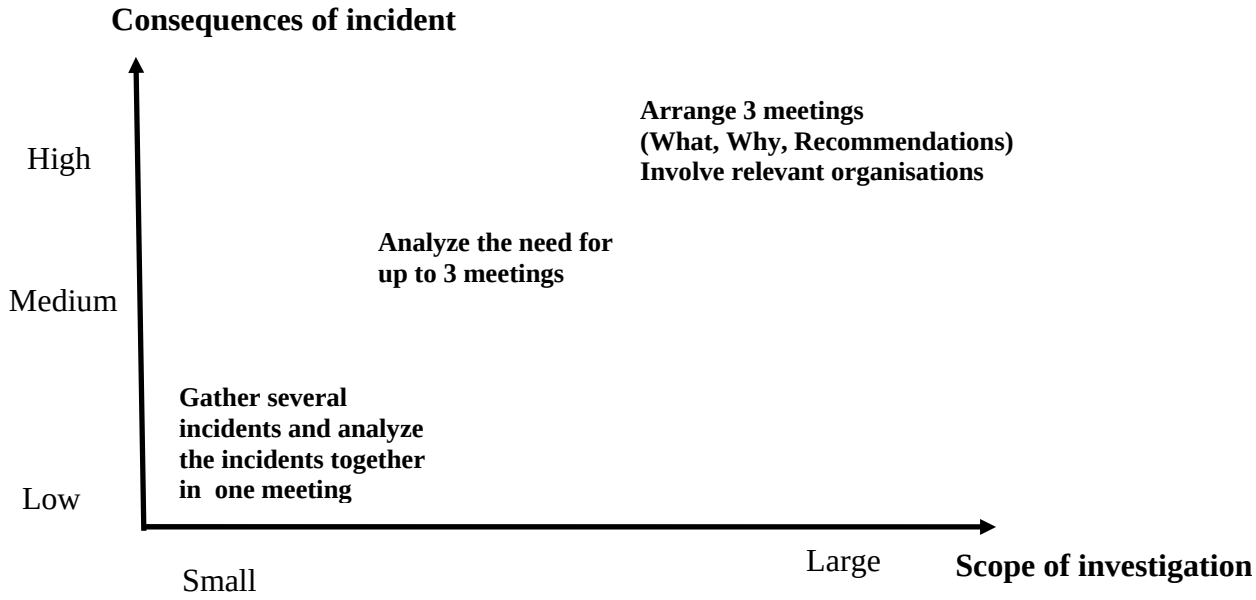


Figure 6-3: Scope of incident/accident investigation

The lessons learned should be used to improve the work on information security and the incident handling (by providing input to the work in the Prepare phase). Lessons learned should as far as possible be published openly and shared. To ensure good organisational learning it is suggested to describe each incident as a short story, that are collected in a common repository (on the web). These stories can then be utilized in the awareness work, as described in Section 4.5.

6.1 Commitment - do we want to perform organisational learning?

In order to be able to succeed with organisational learning, the organisation must be prepared for learning – as pointed out in section 4. The management must decide on the resources to be used. The key issue is the extent of management commitment to learning and the willingness to use resources in learning from this type of incidents. For each incident, a consideration should be made regarding to what extent one is able and willing to learn from this incident. This is highly related to the seriousness of the incident, and will decide the amount of resources that will be used on learning from the incident, as shown in Figure 6-3 above.

The ability to involve all relevant actors is also of special importance. Questions to ask include:

- To what extent do we want to have an open reporting culture related to this incident?
- To what extent is it possible to adopt an open, team based approach to investigation, with effective involvement of operative employees (from ICT, SCADA), HSSE representatives, and management?
- Is the team led by a manager with appropriate seniority?
- Are all the relevant organisations in the network involved in the learning process, e.g. onshore/offshore?
- Are suppliers involved?
- Have all team members received necessary training and guidance to enable them to play their part effectively in the investigation and learning process?
- Does the team have knowledge of both organisational, human factors and technical issues?
- Is practical guidance and support available to the team from professionals?

The willingness to learn, and possibly change fundamental issues related to this particular incident is also a main factor that should be considered:

- Do investigations seek to identify and discriminate between immediate and underlying causes?
- Are there effective means in place to communicate conclusions back to stakeholders and to track implementation of mitigating actions?

To be able to learn from the incident, one is dependent on documentation of the incident, as stressed in section 4.4 in the Detect and recover phase. One is also dependent on a structured accident analysis methodology to help identify immediate and underlying causes. Such an analysis method should cover organisational, technical and human factors issues. The following sections describe one such analysis method.

6.2 What occurred - identify sequences of events using STEP

We are proposing to base our methodology on the “Swiss cheese” model from Reason [48], e.g.:

1. Document the causal relationships using a step diagram and
2. Discuss barriers to prevent and protect

This section focuses on the first step.

The STEP method [49] was originally developed for detailed analysis of incidents and accidents. (What happened and why did it happen.) It provides a common framework for the analysis group in the form of a graphic presentation of the events during the scenario, see figure 6.3.

The method is conducted in the following manner:

1. The actors who are involved in the incident are identified. The term actor denominates a person or object that affects the incident “by his or her own force”. The actors do not only react in a passive manner to outside influence, they are actively involved in the incident leading up to the accidents and afterwards by e.g. their own actions, decisions or omissions. The actors are drawn under each other in a column on the left side of the STEP diagram.
2. Identify the incidents and events that influenced the accident and how the incident was handled. The events are described by”whom”,”what” and”how”, and are placed in the diagram according to the order in which they occurred. There should only be one event in each rectangle. A mental event (i.e., what the actor perceives or interprets, or actions she or he intends to conduct) should be included in the diagram.
3. Place events in the correct place on the time-actor sheet. If the exact time of an event is not known, attempts should be made to identify the correct order of events. In some

situations it is better to identify the sequence of events first. This is not a problem as long as the investigator remembers to identify all the involved actors afterwards.

4. Identify the relationship between the events, what caused each of them, and show this in the diagram by drawing arrows to illustrate the causal links. For each event the previous events leading to this event are assessed. This is done by the use of a logic test. The logic test consists of a necessary and a sufficient test. The logic tests address whether one event is sufficient to cause the following event. If not, then other events that are necessary in order to cause the following events are identified. Finally the connection between the events is shown using arrows. This will also ensure that the events are in correct order with regard to the time line.

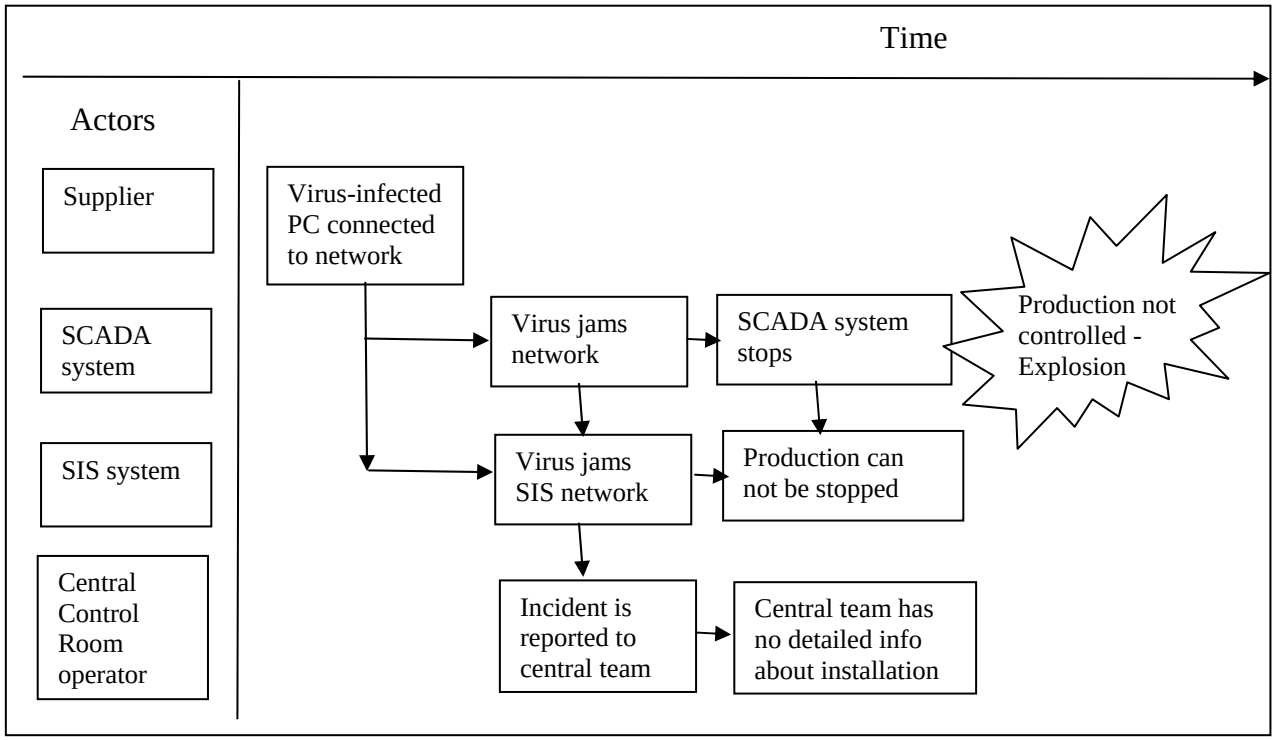


Figure 6-3: Schematic STEP diagram of virus attack

We have made a step diagram as an example to illustrate a virus attack, influencing the SCADA system and the SIS network. The example is inspired by an actual incident described by Johnsen, Ask and Røisli [17].

It is practical to use yellow post-it notes and large pieces of paper when the incident is constructed. The text is written on the post-it notes, which are placed in the presumed correct position and moved when needed. The connecting lines should be drawn with pencil, so that they can be altered easily.

6.3 Why - Identify root causes and barriers

The safety and security philosophy of offshore installations is generally that *multiple* technical safety and security devices are installed to prevent escalation of deviations into adverse consequences. This implies that offshore processes are designed to be self-contained in the event of disturbances. If the process control system or the operator fails to keep process parameters within predetermined limits, the process equipment is designed to shut down and prevent adverse development of the situation.

With these redundant safety and security devices, how can accidents occur? It is evident that in order to reach a critical situation, safety and security barriers must be missing or not function as intended. Barriers can be put out of function intentionally or unintentionally, due to errors or slack in operating procedures on the installation, as well as insufficient component reliability ore due to targeted attacks.

When constructing scenarios for the analysis, the following hypothesis must be kept in mind "Accident scenarios involve failures in several safety and security barriers"

The HSSE philosophy on the installations implies that if all barriers function as intended, the safety systems and security systems would handle or contain abnormal situations. Experience shows that major incidents typically are caused by a combination of instrument failures, incorrect operator actions and inadequate organisational communication systems. Therefore, barriers can be technological, human or organisational.

To fully understand the root causes and consequences of weak points and safety and security problems found in the Scenario Analysis, the analysis team should evaluate the existing and missing barriers. One way of evaluating the barriers and their relation with the weak point is to carry out the three steps shown in Figure 6-4.

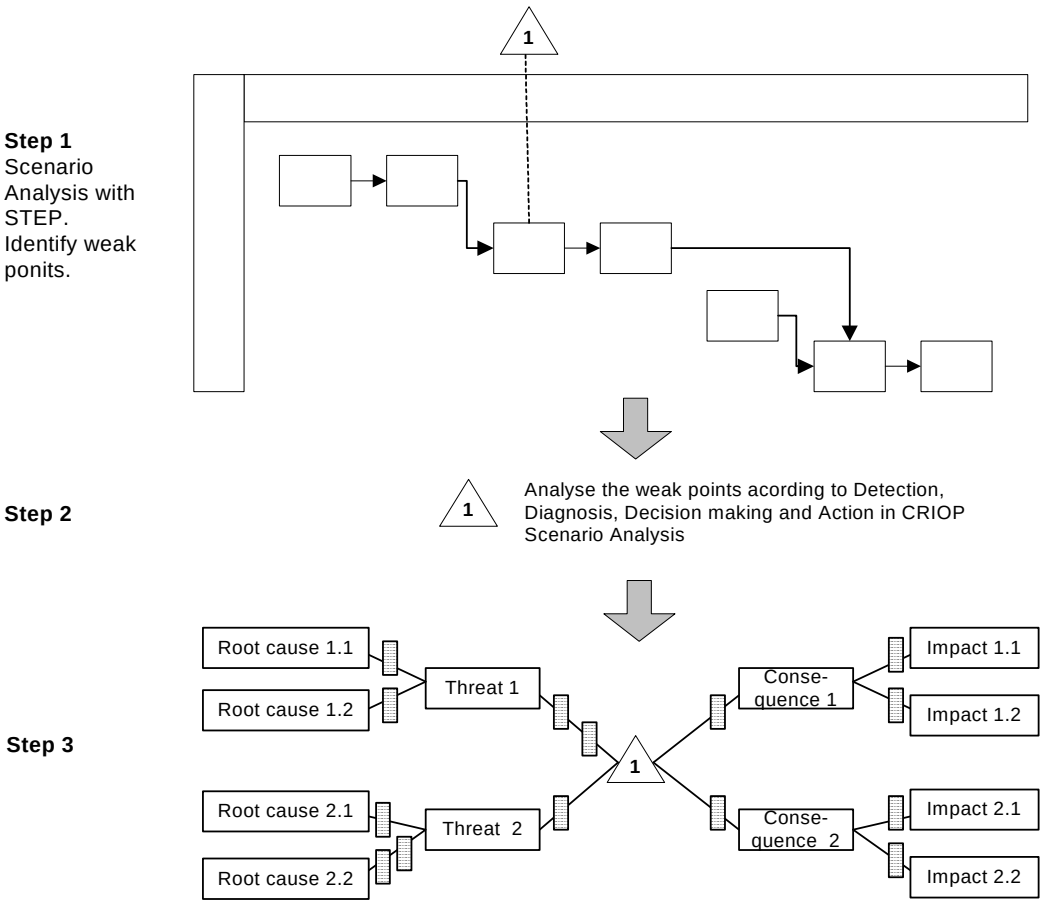


Figure 6-4: : Evaluating the weak points in combination with safety barrier analysis [50]

Step 3 in the figure comprises (paraphrased from CRIOP [50]):

- Evaluate the threats which can lead to a weak point
- Identify root causes leading to the threat

- Identify the consequences and Impacts of the weak point (use results from step 2)
- Identify the existing and missing barriers to hinder root causes and threats
- Identify the existing and missing barriers to reduce negative consequences and impacts
- Summarise weak points, root causes, safety and security barriers and impacts in a table showing their relations to one another

NB! The triangle represents the weak point. The shaded vertical blocks represent safety and security barriers.

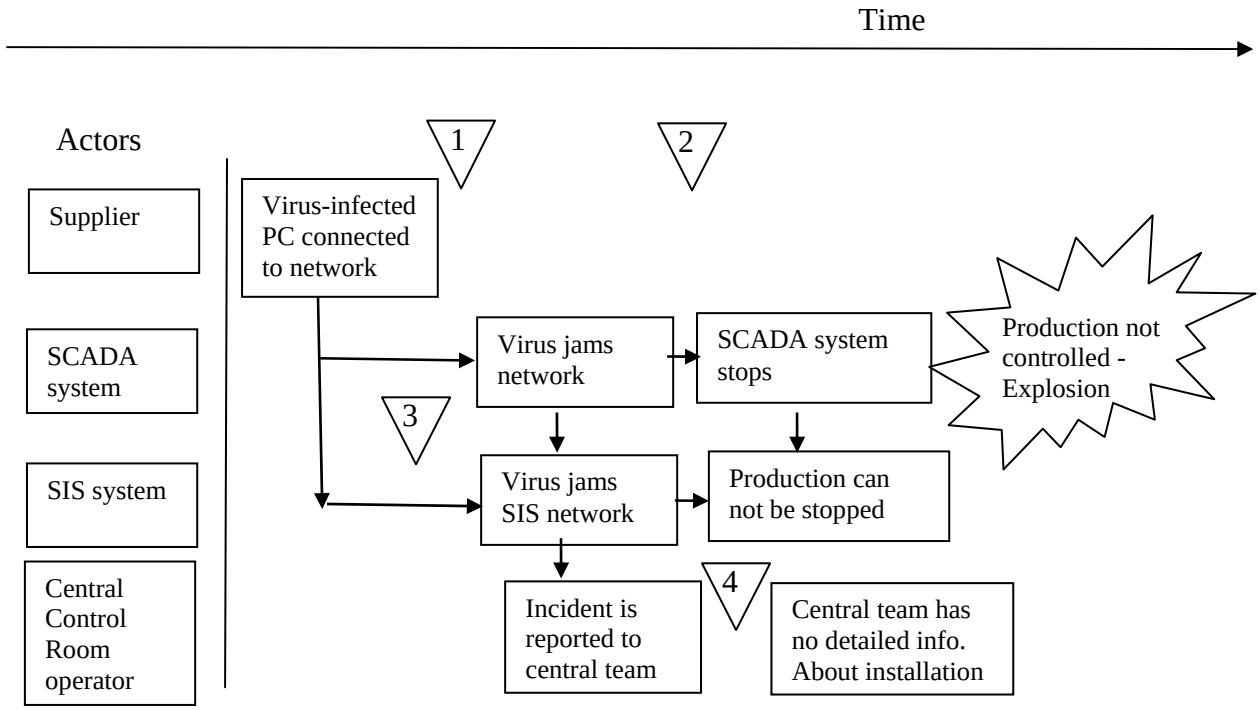


Figure 6-5: Case evaluating the weak points in combination with safety barrier analysis

Weak Points:

1. No scanning of PC prior to connection to network
2. Latest patches not deployed to network and systems connected to network, making a successful virus attack more probable
3. SIS network integrated in SCADA system, the SIS/SCADA network are common, making it possible to jam the SIS trough the SCADA system
4. The technical central team has not sufficient detailed knowledge of the local SCADA system and does not manage to stop or shut down production

Suggested barriers to be attached at the weak points:

B1-1) Supplier must guarantee that all PC's to be connect to the network should be scanned prior to connection
B1-2) Uses a staging facility to scan PC prior to connection to the network
B1-3) Awareness training of supplier (PC owner) – ensuring that no virus are established at the PC
B2-1) All components attached to the network have latest patches, ensuring that the virus attack is not successful.
B3-1) Firewall between SCADA system and SIS

B3-2) Separate isolated and independent network between SIS and SCADA systems
B4-1) Better documentation of SCADA systems or more standardised solutions

We have identified that organisational and human factors issues seldom are assessed. Based on our interviews and collaboration with the industry we have suggested important barriers that should be explored during the accident analysis (see Appendix I). We describe both proactive and reactive barriers to be used in the accident analysis (see figure 6-4).

The barriers are based on our interviews, and we suggest that the list should be used as a starting point as an aid to identify the necessary barriers in a given organisation.

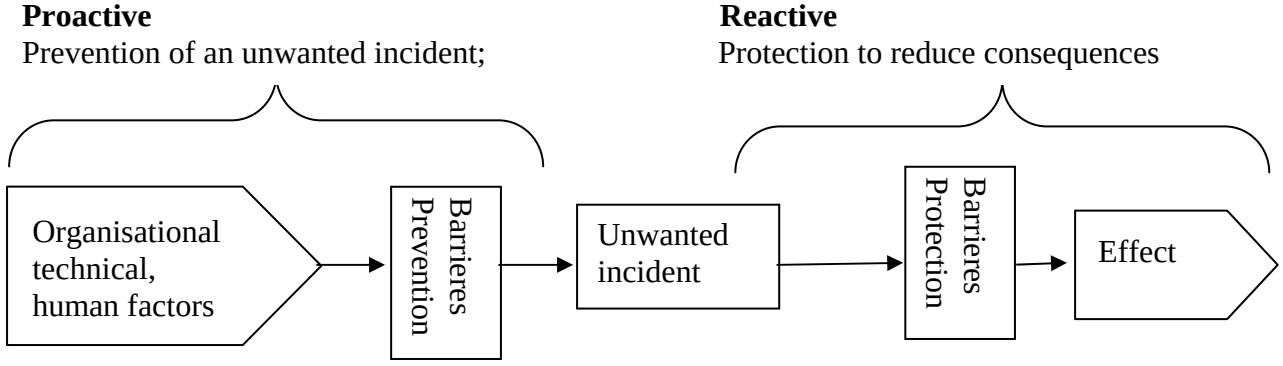


Figure 6-6: Barriers based on organisational, technical and human factors issues to prevent and reduce consequences.

Examples of proactive barriers for incident handling are:

- **Organisational barriers** – Has an incident handling team been established and has a short and precise incident handling plan been established? Is there precise responsibility related to operations of the ICT/SCADA network, has good practice been for remote access (such as the HYDRO SOL solution) been established, has a risk assessment been performed for process control, safety, and support ICT systems and networks? Are there procedures for reporting of security events and incidents, has an open reporting culture been established among operators and suppliers? Has a DFU scenario analysis been performed between operator and suppliers?
- **Technical barriers -** Have firewalls been implemented based on a good practice scheme, are the firewall logs analysed systematically? Has an IDS and/or Honey-Pot solution been established, to act as a proactive indicator related to incident handling? Has the interconnection between ICT and SCADA systems been tested and certified, and have the SCADA network been tested and certified for ICT traffic? Do the process control, safety, and support ICT systems have adequate, updated, and active protection against malicious software?
- **Human Factors barriers** - Have the participants from suppliers and other operators been educated in the information security requirements, do they know how an incident should be handled and do they know about acceptable use and operations of the ICT systems? Has a CheckIT analysis been performed? (We suggest performing a CheckIT analysis annually, to ensure that no complacency is setting in.)

Examples of reactive barriers include:

- **Organisational barriers** – A clear responsibility related to incident handling and that an Incident Response Team is available. Performing an accident analysis and performing an evaluation of the incident handling process, e.g. a “post mortem analysis”.

- **Technical barriers** – Good practice firewalls are established and the firewalls are updated with the most relevant patches.
- **Human Factors barriers** – The organisation is informed about the incident in an open manner and organisational reflection and learning is taking place. Have the users of process control, safety, and support ICT systems been educated in the information security requirements and acceptable use of the ICT systems?

6.4 Identify safety and security recommendations

Based on the accident analysis, the identified weak points and suggested barriers, we have established the necessary background to identify the safety and security recommendations. It is important to prioritise the suggested actions based on a cost/benefit analysis. The responsibility for the action should be placed.

6.4.1 Document safety and security recommendations and the Incident

The usual HSSE reporting systems, such as Synergi is used in general to follow up the HSSE incidents, but Synergi is not structured or used to record ICT incidents. Synergi should however also be used to record ICT incidents.

6.4.2 Documentation and follow up of recommendations

The results from the accident analysis, the safety and security recommendations, should be documented in an action list, consisting of:

- A short description of the identified weak points
- Suggestions for remedial measures and recommendations (such as barriers) based on the identified weak points, as agreed in group meeting
- Cost/benefit analysis
- Responsible person for the weak point/suggested recommendation and target date

6.4.3 Documentation of the incident

There is a need to document the ICT incident in order to inform other actors about the incident and share “best practice”; and in order to keep a record of the incident that can be used to sustain learning from the incident, or analyze the incident at a later stage.

We feel the need to document some sort of best practice form to be used in incident reporting. We have based our work on the BCIT form, but have adapted this form to our MTO perspective, adding issues related to human factors (Man) and Organization. In addition we have tried to document proactive and reactive issues. It is suggested to use such a structured form to document the incident, and the suggested form can be used as a starting point. The form should be filled out by the expert technical group being involved in the incident handling.

The form (see Appendix E) includes the following items:

- **Who,** is reporting the incident
- **Incident information**
- **Barriers in place prior to the incident- technical, organizational or human factors**
- **Remedial action taken after the incident - technical, organizational or human factors**
- **Result of incident**
- **Equipment involved**
- **Incident description in free form, not covered earlier in the form**
    - STEP diagram with a general description of the incident
    - Description of impact on the organization
    - Suggested barriers to ensure that the incident will not happen again

- References to the incident (Web, articles, publications)

6.5 Evaluate the incident handling process and identify recommendations

We would like to establish a collective learning activity to analyse how the incident was handled, and this is called our "post mortem" analysis. The STEP diagram is an important document in this post mortem analysis.

There are most often lessons to be learned from the handling of an incident that can be used to improve the managing of incidents and the way incidents are documented. Ideally, all relevant parties should be involved shortly after an incident while information is still fresh in peoples' minds. Factors to consider include [3]:

- Did the incident management plan work as intended?
- Were all relevant actors involved at the right time?
- Are there any procedures or methods that would have aided the detection of the incident? (if the incident was detected by someone outside the incident management team, any lessons learned should be explored and communicated to the relevant actors as part of awareness-building.)
- 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 & recover process?

The key participants in the evaluation process are:

- Facilitator, group leader
- Incident response team (ICT, SCADA professionals)
- Other participatory organisations – suppliers or contractors

The main motivation is to reflect on what happened during the analyses in order to improve future practise – for the individuals that have participated and for the organisation as a whole. The physical outcome of a meeting is a post mortem report. The key activities are:

1. *Introduction*. First, the facilitators introduce the agenda of the day and the purpose of the post mortem review.
2. *Session 1*. Facilitators hand out post-it notes and ask people to write down what went well during the Incident/accident analysis, hear presentations, group the issues on the whiteboard, and give them priorities.
3. *Session 2*. Facilitators hand out post-it notes and ask people to write down problems during the accident analysis, hear presentations, group the issues on the whiteboard and give them priorities.
4. *Root cause analysis*. The facilitator leading the meeting draws a diagram for the main issues both from the things that went well and the things that were problematic (e.g. using fish-bone diagrams as illustrated and described in [51]).

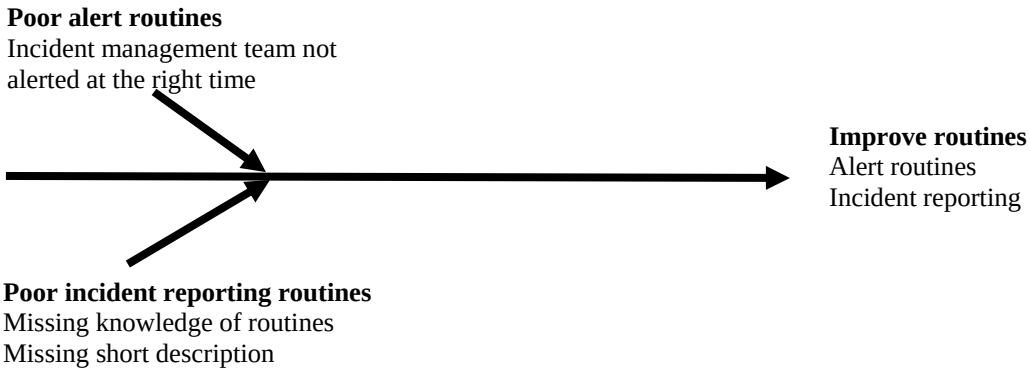


Figure 6-5: Example fishbone diagram for root cause analysis

6.6 From Learn to Prepare

The result from the STEP analysis and post mortem analysis should be explored both in the prepare phase and in the other phases. It is important to sustain the open reporting culture, spreading information about the incident in an open and participatory way.

The main actors in receiving information are management, the general users in the organisation and the technical experts. The information flow routines must ensure that the technical experts (system administrators and other relevant personnel) become party to information regarding new attacks and misconfigured equipment. Management and the general users should ideally learn by hearing (pedagogic) stories from the incidents. The technical experts involved in preparation and detection of incidents should go trough the detailed step analysis and barrier analysis.

Some of the key results from the learn phase is:

- Identified new barriers to be implemented – both technical, organisational and related to human factors (To management and technical experts)
- The process identifying what and why the incident happened, creating understanding, awareness and improved attitudes among the participants in the accident analysis (To management and technical experts)
- Information from the accident analysis, such as the STEP analysis, creating understanding, awareness and improved attitudes among the people receiving the information. The information must be targeted to the user group, i.e. information to the general user must be formed as a pedagogic story, while the technical experts should explore the step analysis.
- The “post mortem” analysis improving the whole incident management process (To management and technical experts, including incident response team)
- Responsibilities for mitigating actions, creating new power relations in the organisation (To management)

7 Conclusions

Traditionally, incident response work has been an integrated part of overall information security, and it often becomes difficult in any given situation to differentiate between initiatives that are intended to improve incident response, and initiatives that are intended to improve security in general. In this report we have focused on incident response, while acknowledging that an interface to preventive measures also is important

The main objective of the IRMA project has been to improve information security in ICT systems in the oil and gas industry by developing and implementing a method for Incident Response Management in the new e-Operations environment.

The main target group for this report is the professionals involved in specification, purchasing or operation of the ICT/SCADA equipment used in production or in safety related systems in the oil and gas industry. However, the IRMA method is not limited to the oil and gas industry. Due to its normative nature it should be possible to transfer the IRMA system to other industries and businesses as well.

7.1 What have we accomplished in IRMA?

Incident Response (IR) has traditionally been a reactive approach, focusing mainly on technical issues. Incident Response Management (IRMA) combines traditional IR with a proactive learning loop, with emphasis on organisational, technical and cultural aspects. IRMA includes the following phases:

- **Prepare:** Planning and preparation of incident response
- **Detect and recover:** Detection of incidents and restoration to normal operation
- **Learn:** Experience sharing and learning afterwards.

In this report we have presented IRMA as a detailed approach to IR.

The approach includes findings from a number of interactions with the oil and gas industry such as workshops, system dynamic modelling workshops, interviews with key personnel, a case study, a risk and vulnerability assessment, a study of relevant cultural aspects by the CheckIT tool, participation in periodic OLF workgroup on information security meetings. It also includes identification of a number of performance indicators for monitoring of incident response management.

A particular aspect of the transition to IO-operations in the oil and gas industry is the integrated involvement of a number of actors such as operators and suppliers. This implies a virtual organization with several security cultures in cooperation. This important aspect must be taken care of in incident response management.

7.2 What will we do further in IRMA?

We will publish a short IRMA Guide that will provide specific advice related to the various phases of incident response. It will also give a step-by-step guide for how to implement IRMA in an organisation in the oil and gas industry.

The primary target group for this IRMA guide will be administrative personnel, who are responsible for planning and implementing measures regarding information security. They will find help and guidance in this report. Technical personnel directly involved in incident response handling will also find useful information in selected areas of the report, and may use it as a reference. And finally technical personnel directly involved in support or operative work may use the guide to attain insight and competence in incident handling.

7.3 What did we not accomplish in IRMA, related to the objectives?

One of the goals in the project was to implement the results in the industry and thus have a large scale testing of the method. This was not accomplished. The pilot case was Brage, operated by Hydro. We underestimated the challenge of doing this in parallel with the transition to Integrated Operations, and the practical problems related to getting access to qualified operator personnel who were already overtaxed with other responsibilities could not be resolved.

7.4 Further work after IRMA

During the IRMA project several areas for future work to improve incident response management have been identified:

- *Indicators*.
  There is a lack of empiricism on the use of indicators in this area. Large scale/long time trials are needed access which indicators are most effective.
- *There are few incidents*.
  Registration and analysis of “near misses” could provide a better data base.
- *Interlinking of information security and safety.*
  The interlinking of information security incidents and safety incidents should be studied in detail.

References

[1] "Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems," 2007, http://www.olf.no/hms/retningslinjer/?50182.pdf.

[2] M. G. Jaatun(red.), "Arbeidsseminar om IKT-sikkerhet i Integrerte Operasjoner: Referat " 2007, http://www.sintef.no/upload/10977/sluttrapport.pdf.

[3] "ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management.," 2004.

[4] "Information Security Management Systems - Requirements," ISO/IEC 27001, http://www.27000.org/iso-27001.htm, 2005

[5] "Information technology - Code of practice for information security management.," ISO/IEC 27002, http://www.27000.org/iso-27002.htm, 2005

[6] T. Grance, K. Kent, and B. Kim, "Computer Security Incident Handling Guide," NIST Special Publication 800-61, 2004.

[7] "IT Infrastructure Library (ITIL)," http://www.best-management-practice.com/IT-Service-Management-ITIL.

[8] N. Brownlee and E. Guttman, "Expectations for Computer Security Incident Response," IETF, 1998.

[9] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security*, vol. 21(6), pp. 526-531, 2002.

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

[11] D. Forte, "Security standardization in incident management: the ITIL approach," *Network Security*, vol. 2007(1), pp. 14-16, 2007.

[12] "Information security risk management (Draft)," ISO/IEC 27005, http://www.27000.org/iso-27005.htm, 2007

[13] K. Stouffer, J. Falco, and K. Kent, "Guide to SCADA and Industrial Control Systems Security (draft)," NIST Special Publication 800-82, 2006.

[14] "Functional safety - Safety Instrumented systems for the process industry sector," IEC 61511, 2003

[15] "Safety and automation system (SAS)," NORSOK I-002 Rev.2, http://www.standard.no/pronorm-3/data/f/0/01/34/3_10704_0/I-002.pdf, 2001

[16] OLF, "Integrated Operations on NCS," Norwegian Oil Industry Association 2004, http://www.olf.no/?22894.pdf.

[17] S. O. Johnsen, R. Ask, and R. Røisli, "Reducing Risk in Oil and Gas Production Operations," presented at First Annual IFIP WG 11.10 International Conference, 2007, Critical Infrastructure Protection, E. Goetz and S. Shenoi (Eds.), ISBN: 978-0-387-75461-1.

[18] S. O. Johnsen, et al., "Trusler og muligheter knyttet til eDrift," SINTEF T&S, Trondheim STF38A04433, 10.01 2005.

[19] S. Andersen, "Improving Safety through Integrated Operations," Master of Science thesis, NTNU 2006, http://www.criop.sintef.no/Participants%20and%20projects/MasteroppgaveSiriAndersen.pdf.

[20] A. K. Solem, "Experience transfer as a contributor to increased HSE level in Integrated operations," Master of Science thesis, NTNU 2007

[21] OLF, "Integrated Work Processes: Future work processes on the Norwegian Continental Shelf," Norwegian Oil Industry Association 2005, http://www.olf.no/?51638.pdf.

[22] "The NPD's fact pages," Norwegian Petroleum Directorate 2005, http://www.npd.no/engelsk/cwi/pbl/en/index.htm.

[23] T. Larstad and Ø. Dretvik, "FAKTA Norsk Petroleumsverksemd 2005," *Norwegian Petroleum Directorate*(March), 2005.
[24] D. B. McCafferty and C. C. Baker, "Human Error and Marine Systems: Current Trends. ," presented at IBC's 2nd Annual Conference on Human Errors, London. , 2002
[25] G. B. Chadwell, F. L. Leverenz, and S. E. Rose, "Contribution of Human Factors to Incidents in the Petroleum Refining Industry," presented at American Institute of Chemical Engineers 33rd Annual Loss Prevention Symposium, Houston, Texas, 1999
[26] S. Jones, C. Kirchsteiger, and W. Bjerke, "The importance of near miss reporting to further improve safety performance," *Journal of Loss Prevention in the Process Industries*, vol. 12(1), pp. 59-67, 1999.
[27] S. Lüders, "CERN tests reveal security flaws with industrial networked devices," 2006, http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=1490.
[28] E. Albrechtsen, et al., "IRMA - Interviews on incident response in the oil and gas industry," SINTEF MEMO, November 22. 2007.
[29] E. Rich, D. F. Andersen, and G. P. Richardson, "OLF IRMA-AMBASEC Group Modeling Report I," University at Albany, Albany, NY 2006.
[30] E. Rich, D. F. Andersen, and G. P. Richardson, "OLF IRMA-AMBASEC Group Modeling Report II," University at Albany, Albany, NY 2006.
[31] E. Rich and J. J. Gonzalez, "Maintaining Security and Safety in High-threat in E-operations Transitions," presented at 39th Hawaii International Conference on System Sciences, Hawaii, 2006
[32] E. Rich, et al., "Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning," presented at 40th Hawaii International Conference on System Sciences, Hawaii, 2007
[33] F. O. Sveen, E. Rich, and M. Jager, "Overcoming organizational challenges to secure knowledge management," *Information Systems Frontiers*, vol. 9(5), pp. 481-492, 2007.
[34] F. O. Sveen, et al., "Toward viable information security reporting systems," *Information Management & Computer Security*, vol. 15(5), pp. 408-419, 2007.
[35] J. Rasmussen, "Risk Management in a Dynamic Society: A Modelling Problem," *Safety Science*, vol. 27(2/3), pp. 183-213, 1997.
[36] E. Albrechtsen, T. Onshus, and L. Bogen, "Oversikt over forskningsmiljøer, offentlige og private aktører innen informasjonssikkerhet med relevans for petroleumsnæringen," SINTEF T&S STF50F06115, 2006.
[37] I. Santa, "Information security awareness initiatives: Current practice and the measurement of success," ENISA 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf.
[38] M. Hammer and J. A. Champy, *Re-engineering the Corporation: A Manifesto for Business Revolution*. New York, NY: Harper Collins, 1993.
[39] U. Kjellén, *Prevention of accidents through experience feedback*: Taylor and Francis, 2000.
[40] M. B. Line, et al., "Monitoring of Incident Response Management Performance," presented at International Conference on IT-Incident Management & IT-Forensics (IMF 2006), Stuttgart, Germany 2006
[41] A. Cormack, et al., "5th TRANSITS Training Workshop course materials," TERENA, Chantilly, France 2005.
[42] C. W. Johnson, *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*: University of Glasgow Press, Glasgow, Scotland, 2003.
[43] D. Brezinski and T. Killalea, "Guidelines for Evidence Collection and Archiving," IETF RFC 3227, February 2002.
[44] C. Argyris and D. A. Schön, *Organisational learning:A theory of action perspective*: Addison-Wesley, 1978.

[45] D. L. Cooke, "Learning from Incidents," presented at 21st System Dynamics Conference, NYC, New York, 2003
[46] D. L. Cooke and T. R. Rohleder, "Learning from incidents: from normal accidents to high reliability," *System Dynamics Review*, vol. 22(3), pp. 213-239, 2006.
[47] J. Hadgkiss, "Computer Security Incident Response Teams: Exploring the Incident Learning Capability," BSc (Hons) thesis, The University of Melbourne, Melbourne, Australia November 2006, http://www.dis.unimelb.edu.au/future/research/theses/2006/JustinHadgkiss.pdf.
[48] J. Reason, *Managing the Risk of Organisational Accidents*: Ashgate, 1997.
[49] K. Hendrick and L. Benner, *Investigating accidents with STEP*: CRC Press, 1986.
[50] S. O. Johnsen, et al., "CRIOP®: A scenario method for Crisis Intervention and Operability analysis.," SINTEF 2004, www.criop.sintef.no.
[51] T. Dingsøyr, "Postmortem reviews: purpose and approaches in software engineering," *Information and Software Technology* vol. 47 pp. 293-303, 2005.
[52] ACSN, "Third report of the Advisory Committee on the Safety of Nuclear Installations - Organizing for Safety " 1993.
[53] T. Helokunnas and R. Kuusisto, "Information security culture in a value net," presented at Engineering Management Conference (IEMC '03), 2003, published in "Managing Technologically Driven Organizations: The Human Side of Innovation and Change" pp. 190-194.
[54] S. O. Johnsen, A. Askildsen, and K. Hunnes, "Challenges in remote control and co-operation of offshore oil and gas installations," presented at ESREL, Poland, 2005, ISBN 0-415-38340-4.
[55] "Information security management measurement (draft)," ISO/IEC 27004, http://www.27000.org/iso-27004.htm, 2007
[56] E. Chew, et al., "Guide for Developing Performance Metrics for Information Security (Draft)," NIST Special Publication 800-80, 2006.
[57] "Information Security Baseline Requirements," 2007, http://www.olf.no/hms/retningslinjer/?50182.pdf.
[58] "Information technology - Service management," ISO/IEC 20000, http://www.itgovernance.co.uk/iso20000.aspx, 2005
[59] "Sarbanes-Oxley Act of 2002," in *H.R. 3763, U.S. Congress*, 2002.
[60] "Industrial Security Incident Database Reporting Form," British Columbia Institute of Technology, http://www.bcit.ca/files/appliedresearch/pdf/security/isid_form.pdf.
[61] S. O. Johnsen, et al., "CheckIT – A program to measure and improve information security and safety culture," *International Journal of Performability Engineering* vol. 3(1 Part II), pp. 174-186, 2007.
[62] E. H. Schein, *Organisational Culture and Leadership*: Jossey-Bass, 1992.
[63] R. J. Westrum, "Cultures with Requisite Imagination," presented at NATO Advanced Study Institute on Verification and Validation of Complex and Integrated Human-Machine Systems, Vimeiro, Portugal, 1992, published in Wise, Stager and Hopkin (Eds.) "Verification and Validation of Complex Systems: Human Factors Issues", Springer 1993.
[64] C. Argyris and D. A. Schön, *Organisational learning II:Theory, method and practice*: Addison-Wesley, 1996.
[65] S. O. Johnsen, "Norwegian CheckIT web page," 2005, http://www.sintef.no/content/page1____6775.aspx.
[66] T. R. LaPorte and P. M. Consolini, "Working in Practice But Not in Theory: Theoretical Challenges of 'High-Reliability Organizations'," *J Public Adm Res Theory* vol. 1, pp. 19-48, 1991
[67] J. P. Kotter, *Leading Change* Harvard Business School Press, 1996.
[68] S. O. Johnsen, "CheckIT web page," 2007, http://www.checkit.sintef.no.

[69] "21 Steps to Improve Cyber Security of SCADA Networks," US Department of Energy, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

[70] S. O. Johnsen, et al., "From Incident Response to Incident Response Management," presented at PSAM 7 / ESREL '04 International Conference on Probabilistic Safety Assessment and Management, Berlin, Germany., 2004

[71] S. O. Johnsen, et al., "From Incident Response to Incident Response Management," presented at 16th Annual FIRST Conference on Computer Security Incident Handling, Budapest, Hungary, 2004

[72] S. O. Johnsen, M. B. Line, and A. Askildsen, "Towards more secure virtual organisations by implementing a common scheme for incident response," presented at PSAM8, New Orleans, USA, 2006, ISBN: 0-7918-0245-0.

[73] S. O. Johnsen, et al., "Measurement and improvement of Information security and safety culture," presented at Asia Pacific Conference on Risk Management and Safety – Challenges in Engineering Applications and Advances in Technologies, Hong Kong, 2005

[74] S. O. Johnsen, et al., "How to measure and improve IT security and safety culture (CheckIT)," presented at 8th SPE International Conference on Health, Safety & Environment in Oil and Gas Exploration and Production, Abu Dhabi, 2006

[75] S. O. Johnsen, et al., "Check-IT - measurement and improvement of information security and safety culture " presented at PSAM 8 – The eight international conference on Probabilistic Safety Assessment and Management, New Orleans, USA, 2006

Appendix A Abbreviations

AMBASEC:	A Model-Based Approach to Security Culture (project)
CC:	Common Criteria
CCR :	Central control room
CCTV:	Closed Circuit Television
CERN:	Organisation Européen pour la Recherche Nucléaire (French: European Laboratory for Particle Physics; Geneva, Switzerland)
CheckIT:	Tool for measuring security culture
CIA:	Confidentiality, Integrity, Availability:
COTS:	Commercial Off-The-Shelf
CRIOP:	CRIOP®: “A scenario method for Crisis Intervention and Operability analysis.," SINTEF 2004
CSIRT:	Computer Security Incident Response Team
DCS:	Distributed Control System
DFU	Defined hazard and accident situation (Definert Fare og Ulykkeshendelse)
DoE :	The Department of Energy (US)
DoS:	Denial of Service
ESD:	Emergency Shutdown Device
ESD:	Emergency Shutdown System
F&G:	Fire & Gas
FW:	FireWall
HAZOP:	Hazard Operational Analysis
HCE:	Human Caused Error
HMI:	Human Machine Interface
Honey pot:	A computer system set up as a trap for attackers
HSSE:	Health Safety Security and Environment
HW:	Hardware
ICT:	Information and Communications Technologies
IDS:	Intrusion Detection System
IEC:	International Electrotechnical Commission
IFEA:	Industriens Forening for Elektroteknikk og Automatisering (The Association for Electrotechnics and Automation in Industry)
IKT SoS:	ICT Security
IO:	Integrated Operations (e-Operations)
IP:	Internet Protocol
IPsec:	IP Security Protocol
IR:	Incident Response
IRMA:	Incident Response Management
ISBR:	Information Security Baseline Requirements (OLF)
ISO:	International Organization for Standardization
ITIL:	Information Technology Infrastructure Library
MTO:	Man, Technology, Organisation
NCS:	Norwegian Continental Shelf
NIST:	National Institute of Standards & Technology (US)
NorCERT:	Norwegian Computer Emergency Response Team
NPD:	Norwegian Petroleum Directorate
OLE:	Object Linking and Embedding
OLF:	Oljeindustriens LandsForening (Norwegian Oil Industry Association)
OPC:	OLE for Process Control

PC:	Personal Computer
PCS:	Process Control System
PDS:	Reliability of computer based safety system (Pålitelighet av Databaserte Sikkerhetssystemer)
PLC:	Programmable Logic Control(ler)
PSD:	Process Shutdown System
Ptil:	Petroleumstilsynet (Petroleum Safety Authority Norway)
SAP:	Systeme, Anwendungen, Produkte in der Datenverarbeitung (German: Systems, Applications & Products in Data Processing; SAP AG)
SAS:	Safety and Automation System
SCADA:	Supervisory Control and Data Acquisition.
SD-model:	System Dynamics model
SIL:	Safety Integrity Level
SIS:	Safety Instrumented System
SOIL:	Secure Oil Information Link
SOL:	Sikker Operasjonsløsning(Secure Operation Solution), HYDRO
SSL:	Secure Sockets Layer
STEP:	Sequential Timed Events Plotting (Flow diagram, flow sheet, step-by-step diagram)
TCP:	Transmission Control Protocol

Appendix B Terms and definitions

Incident: In this report, “incident” or “security incident” refers to a successful attack, i.e. something that actually happens and must be dealt with. Thus, a virus infection is an incident, but a virus that is detected and removed/isolated by the antivirus program is not.

Remote control: Part of the operation is managed and operated from other places. This can cover a wide spectrum of possibilities, from control of parts of the process in a normal situation to total control of the installation in an emergency situation. Central control room operators are present at the installation.

Remote operations: The entire process is managed and operated from other places. This is the situation for the unmanned installations where all the control room functions and other operation functions are executed from a remote location. Today, this is the case for sub-sea installations.

Safety: Protection against unintended, accidental acts or circumstances that may impact the system

Safety and security culture: The safety and security culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine commitment to, and the style and proficiency of, an organisation’s health, safety and security management [52].

Security: Protection against intended, malicious or hostile acts or circumstances that may impact the system

Security culture: The aim is to establish a security culture and an awareness level where security is a natural part of the daily activities of an organisation [53]. Culture is a more complex issue than awareness, as seen from the definition in Merriam-Webster Online Dictionary:

- Awareness is defined as “having or showing realization, perception, or knowledge”.
- Culture is defined as “the integrated pattern of human knowledge, belief, and behaviour that depends upon the capacity for learning and transmitting knowledge.”

In this report, when we refer to security culture we mainly think about the organisation as a whole having both knowledge, belief and behaviour, while we view security awareness more as a element or result of safety culture. Security awareness is about knowledge and attitude – an ongoing process of learning. Each person’s security awareness level influences the organisation’s security culture – the shared basic assumptions of the group – together with other aspects like management focus, tools available and the way security is built into daily working routines.

Virtual organisation: A virtual organisation is a group of people from different organisations located at different geographical locations working together in shared interdependent processes to achieve shared objectives within a defined timeframe. The authority and roles of the participants are clearly defined, ref [54].

Appendix C Interview Guide

Background

Reporting of unwanted ICT incidents

SINTEF in cooperation with HiA (Agder university college), the oil industry association (OLF), supported by the research council, has been working with the research project IRMA – Incident Response Management. The project timeframe is 2005 – 2007. Hydro and STATOIL has participated in the project together with OLF. A planned result from the project is the "IRMA – guide" – a short presentation of Incident Reporting.

The proposed structure of incident response is divided in the following phases:

1. **Prepare**
2. **Detect and recover**
3. **Learn**

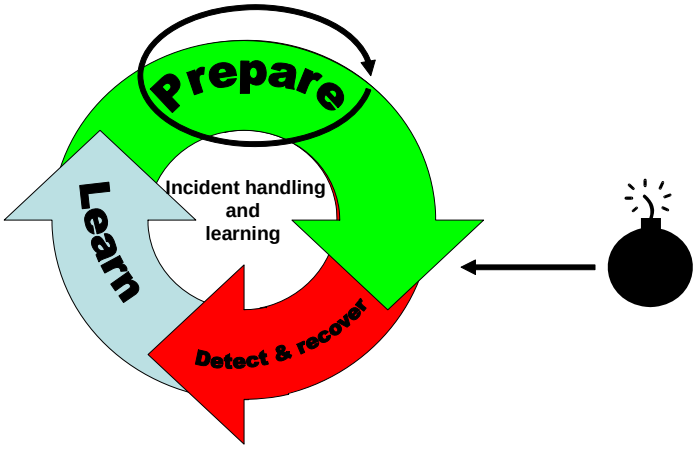


Figure 1: IRMA: Incident reporting

Questions

1. **Describe your responsibility.**
   a) Describe the systems and work procedures in your area of responsibility..
   b) Describe the interfaces to SHE management and ICT securty management.

2. **What is your definition of an unwanted ICT incident?**

3. **What is the frequency of unwanted ICT incidents? What kind of incidents are documented?**
   a) Do you have any good histories describing unwanted ICT incidents?
   b) How was the incident managed? What was the quality of the incident management?
   c) If you don't have any unwanted ICT incidents – what is the reason?

4. **What is the most critical systems related to unwanted ICT incidents?**

(SIS, PCS, UPS, CCTV, Video, ICT management systems, ..)

5. **How are unwanted ICT incidents managed? What procedures are being used?**
   A) Prepare
   B) Detect and recover
   C) Learn

A)Prepare:

- Is there one document describing incident handling?
- Do you train on handling incidents?
- What is the main barriers related to incident handling?

B) Detect og recover

- Who has the responsibility?
- What is the main challenges?
- Are the logs from the firewalls reviewed?

C) Learn

- Are ICT incidents reported?
  - What systems are being used?
- What part of the organisation are involved in learning from incidents?
- How do you learn?
  - Are procedures changed in the whole organisation, or are you putting out fires
  - Do you share experiences?
- Why do you want to learn from incidents?
- Are all ICT incidents analysed and are root causes identified?

6. **Should we focus on knowledge, procedures, technical issues or organisational issues?**
   - How is knowledge related to the unwanted ICT incidents?

7. **How is the quality of the incident management you have described?**
   - What could be improved
   - What are the main challenges to improve incident management?

8. **What are your suggestions to improve Incident Management – related to MTO?**

9. **If you should propose a guide related to incident management – what should this guide contain?**
   - Stories?
   - Best practice?
   - Scenarios to be explored to avoid unwanted incidents?
   - Establishment of communities of practice
   - Forms to be used in incident management?

Appendix D Relevant standards and good practice

An overview of the standards and good practice documents most relevant to the IRMA project is given in this appendix. They concern information security management in general and related to the oil and gas industry.

D.1 ISO

International Organization for Standardization[13]is the largest developer of standards in the world. It is a network of 155 national standards institutes and represents therefore a broad specter of all countries in the world. Some of the most referred standards related to information security are developed by ISO, and these are presented below.

D.1.1 ISO/IEC TR 18044: Information security incident management

ISO/IEC TR 18044:2004 [3] is a technical report of type 3, meaning that it contains a different kind of content than what one would normally find in a standard. For this report, the content is more like a representation of state of the art within information security incident management.

Being a representation of state of the art, the technical report is well suited both as an introduction to incident management and as a reference book for those having incident management as an important part of their job. The report is not that long – around 50 pages including appendixes – and focuses on organisation of the work on incident response and the processes that are directly part of incident management. The main content can be summed up with the following bullet points:

- *Why information security incident management.* The benefits of having an information security incident management scheme and the key issues that need to be addressed to convince management. Examples of information security incidents and their causes.
- *The incident management processes*
    - Plan and prepare – Establishing the necessary organisational structures, as well as policies and schemes for incident management.
    - Use – Detect, report and response to an information security incident.
    - Review – Identify lessons learned.
    - Improve – Make improvements to the incident management scheme as well as to the information security.
- *Example schemas and guidelines*

A technical report is not a standard, and consequently you cannot get a certification against ISO/IEC TR 18044. The report builds on and refers to ISO/IEC 17799:2000 (now 27002) and ISO/IEC 13335-1:2004 (to be 27005), both presented below.

D.1.2 ISO/IEC 27001 and ISO/IEC 27002: Information security management systems

Both the standards ISO/IEC 27001:2005 [22] and ISO/IEC 27002:2005 [23] deal with management of information security, though their contents are a bit different. ISO/IEC 27001:2005 provides requirements for information security management systems; i.e. how to establish, implement, operate, monitor, review, maintain and improve such a system. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Organisations can get a certification against ISO/IEC 27001:2005, but not towards ISO/IEC 27002:2005 since the latter has more the form of a code of practice and a description of security controls to help in

[13] www.iso.org

the implementation of the former standard. The close relation between the two standards is emphasized by their history. They both have their origin at the UK Department of Trade and Industry, and in the middle of the 90's the first version of the standard BS 7799 was available. BS 7799 had two parts, where the first part has later developed into ISO/IEC 27002, and the second part into ISO/IEC 27001.

The standards are concerned with the overall management of information security, of which incident management is one important part. One will therefore find information on security controls and code of practice related to incident management in these standards.

D.1.3 ISO/IEC 27004: Information security management measurements[14]

This emerging standard [55] is currently on a working draft level (autumn 2007), and may not be referred to as an International Standard. However, it is intended to help an organization establish the effectiveness of its ISMS implementation, embracing benchmarking and performance targeting within the PDCA cycle.

D.1.4 ISO/IEC 27005: Information security risk management

This recent standard [12] is currently on a working draft level (autumn 2007), and may not be referred to as an International Standard. However, it will define the ISMS risk management process, including identification of assets, threats and vulnerabilities. It is likely that there will be relationships to BS 7799-3:2006 and ISO/IEC 13335.

D.2 NIST

National Institute of Standards and Technology[15] is a non-regulatory federal agency in the US. They develop guidelines and standards related to information security, but they mainly address conditions of interest for American parties. However, much research and many results developed in the US are internationally accepted, and some of the most acknowledged experts worldwide in the discipline contribute to NIST's publications.

D.2.1 NIST 800-61: Computer Security Incident Handling Guide

This publication [6] was released some months prior to ISO's TR18044. It is a comprehensive guide for incident response teams, splitting up the process of incident response into the following four phases:

- Preparation
- Detection and analysis
- Containment, eradication and recovery
- Post-incident activity

In addition to describing these phases in general, it also speaks of five different types of incidents – denial of service, malicious code, unauthorized access, inappropriate usage, and a composition of multiple incidents – and explains how each of the phases applies in these cases. Suggestions for metrics regarding incident response are also included.

D.2.2 NIST 800-80: Guide for Developing Performance Metrics for Information Security

This publication [56] exists only as a draft. It focuses on developing and implementing metrics for an information security program. Incident response is slightly mentioned, and one specific metric

[14] The name of the standard is not yet specified.
[15] www.nist.gov

for incident response is suggested. However, this publication is more suited when looking at the total picture of information security, not incident response in specific.

D.2.3 NIST 800-82: Guide to SCADA and Industrial Control Systems Security (draft)

This publication [13] provides guidance for establishing secure industrial control systems. It gives an overview of typical components in such a control systems, surveys vulnerabilities and threats, and suggests countermeasures to mitigate threats. The measures span from network topology, perimeter controls, firewall rules to organisational issues like personnel security and media protection. It touches incident response slightly, but mostly when referring to NIST 800-61.

D.3 Others

Industry specific organisations contribute with best practice and guidelines with respect to information security.

D.3.1 OLF-104: Information Security Baseline Requirements (ISBR)

The Norwegian Oil Industry Association (OLF)[16] is a member organisation for operators and suppliers working on the Norwegian continental shelf. The ISBR [57] is a guideline that documents best practice regarding information security for process control, safety, and support networks. It is based on ISO/IEC 27001:2005 and adapted to the oil and gas industry. ISBR applies to all offshore industry on the Norwegian continental shelf. The measures presented in ISBR shall be implemented unless they can be justified and documented as not applicable.

D.3.2 CPNI: Policy and best practice regarding process control and SCADA Security

Centre for the Protection of National Infrastructure (CPNI)[17] has provided a set of best practice guides regarding process control and SCADA security [4]. One of these (no. 3) is about establishing response capabilities. It is therefore most helpful in the startup of an incident response team; suggesting plans and procedures that should be in place regarding three phases: protect, detect and respond. Early warning system and reporting are among the discussed issues, and incident response is seen as a part of business continuity plans.

D.3.3 ITIL: IT Infrastructure Library

ITIL [7] consists of several books that together describe best practices in IT service management. The focus is on people, processes, products and the use of partners, and how these should be managed to deliver high quality IT service. ITIL is developed by OGC (Office of Government Commerce), and the latest version, v3, was released in June 2007.

Regarding handling of incidents, ITIL looks at this as two areas – incident management and problem management – which are both parts of service support. An incident is “any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in the quality of service”, while a problem is “the unknown underlying cause of one or more Incidents”. The goal of incident management is though to restore normal service operation as quickly as possible, while the goal of problem management is to identify the underlying cause of incidents to be able to prevent them from happening again. Management of security incidents are also considered more specifically within the module security management.

[16] www.olf.no
[17] www.cpni.gov.uk

The ISO/IEC 20000 International Service Management standard [58] reflects the IT service management best practices provided by ITIL, though it also supports other IT service management frameworks and approaches. It is possible for organisations to get a certification against this standard.

D.3.4 Sarbanes-Oxley

Sarbanes-Oxley (SOX) [59] is developed by US Securities and Exchange Commission (SEC) and applies to all organizations registered on the American Stock Exchange. The section 409, “Real Time Issuer Disclosures,” may pose the thorniest compliance challenge. It calls for real-time reporting of material events that could impact a company's financial performance. Although the SEC has not defined “real time” (and no final deadline for Section 409 compliance has been set), many companies are interpreting it to mean 48 hours. Industry analysts have noted that significant system integration, and implementation of real-time notification and event-driven alerts, will be necessary to comply with section 409.

The requirement stated in section 409 brings along the need for systematic documentation of incidents.

“One underemphasized provision of SOX is the requirement that companies disclose to investors both material events and contingent liabilities that might impact the bottom line. In this regard, IT security becomes more relevant. If you had a choice between investing in a financial institution (or a nuclear power plant) that had sound IT security practices, or one that had none, clearly you would find the IT security decisions to be important. Similarly, a significant attack on an infrastructure could yield losses to confidentiality, reliability or integrity of systems or data that would have to be disclosed to investors (just ask ChoicePoint about that).” (http://www.offshore-income.com/archive/2005_05_01_archive.html)

SINTEF

Appendix E Example Incident Reporting Form

Information security incidents should be registered in an HSSE system such as Synergi together with other incidents/accidents/events. However, there is a need to register more information than typically will be reported in Synergi, so as to better be able to aggregate incident information and thereby learn e.g. what types of incidents happen most often, have biggest consequences, etc.

The Group for Advanced IT at BCIT (British Columbia Institute of Technology) has developed an industrial security incident database reporting form [60]. The form is aimed towards sharing incident information with BCIT so that it can be included in a database and used to get new knowledge of incidents that affect control systems. This form can be used as a starting point for registering incidents, but should be adjusted to the needs of the organisation. Particular points to consider include:

- **Simplification:** All technical details that should be registered in the BCIT form may not be relevant or necessary.
- **Organisational aspects and human factors:** The BCIT form focuses on technical systems and barriers. Organisational and human factors should also be taken into account, especially when it comes to barriers in place and actions that shall be taken. One should also consider whether responsibilities for identified actions should be registered in this form.
- **Indicators:** The indicators chosen for monitoring incident response management (Section 4.6) should be included in the form.

Below we present an example of how the BCIT form [60] can be adjusted to a given organisation's needs, where we specifically have added some items covering the MTO perspective. The form should be filled out by experts involved in incident handling and reflect the outcome of the learning activities. Conclusions from the STEP and barrier analysis should also be summarised in this form.

Incident Reporting Form			
1. Who is reporting			
Company:			
Field:			
Installation:			
Date:			
Name:			
Title:			
e-Mail:			
Telephone:			
2. Incident Information			
Title of Incident			
Date of Incident	Year:	Month:	Day:
3. Location of Incident			
@Company:			
@Field:			
@Installation:			
Technical area	ICT-adm: ☐	SCADA/SAS:☐	SIS:☐

SINTEF

4. Incident type – Accident, Attack or Audit		
Accidental Incident:	Network Failure:☐	Equipment Failure:☐
	Other:☐ Description:	
Attack:	Internal: ☐	External: ☐
	Virus/trojan/Worm:☐	Denial of service: ☐
	Non-Auth. Access: ☐	Fraud/Theft: ☐
	Sabotage: ☐	System penetr:☐
	Description:	
Audit Incident:	☐	
Other:	☐ Description:	

5. Incident details		
Perpetrator - Insider:	☐ Current employee, ☐Former employee	
	☐ Current Contractor, ☐Former contractor	
Perpetrator - External:	☐ Hacker, Skript kiddies, Terrorist, Activist	
	☐ Competitor	
Perpetrator - Other:	☐ None or Description:	
Point of Entry LAN:	☐ HMI (Human Interface)	☐ Laptop
	☐ Via network	☐ Other
Point of Entry Remote:	☐ Internet	☐ VPN connection
	☐ Dial up modem	☐ Wireless
	☐ Trusted 3'd party	
	Other/Description:	

6. How was security problem detected (Prior to incident, During Incident or After incident)		
Prior to incident:	☐ IDS/Honeypot	☐ Risk level
	☐ By Internal ICT dep	☐ By Internal SCADA dep
	☐ By Outside - Contractor	☐ By other
Prior – description of: Technical barrier	:	
Organisational barrier	:	
Human barrier	:	
During incident:	☐ By Internal ICT dep	☐ By Internal SCADA dep
	☐ Outside - Contractor	☐ By other
During – description of: Technical barrier	:	
Organisational barrier	:	
Human barrier	:	
After incident:	☐ By Internal ICT dep	☐ By Internal SCADA dep
	☐ By Outside - Contractor	☐ By other
After – description of: Technical barrier	:	
Organisational barrier	:	
Human barrier	:	

SINTEF

7. Security barriers in Place prior to the Incident	
Technical barriers– Description	Firewall: Access Control: Encryption: Detection:
Organisational barriers– Description	Plans: Organisation: Responsibility:
Human Factor barriers– Description	Training: Awareness: Knowledge:

8. Missing or faulty barriers	
Technical barriers– Description	(Firewall, Access Control, Encryption, Detection)
Organisational barriers– Description	(Plans, Organisation, Responsibility)
Human Factor barriers– Description	(Training, Awareness, Knowledge)

9. Remedial action taken	
Technical actions– Description	(Firewall, Access Control, Encryption, Detection)
Organisational actions– Description	(Plans, Organisation, Responsibility)
Human Factor actions– Description	(Training, Awareness, Knowledge)

10. Result of incident – related to HSSE (Health, Safety, Security, Environment)		
Health	☐ Staff injury or death;	
	☐ Public injury or death;	
	☐ Other:	
Safety:	☐ Equipment loss of control	
	☐ Equipment damaged or lost	
	☐ Loss of production	☐ Loss of time
Security	☐ Loss of confidentiality	☐ Loss of Integrity
	☐ Other, describe:	
Environment	☐ Gas/Oil spill	
	☐ Loss of respect/ Other:	

11. Approximate Production Impact
☐ Loss of production 1-4 Hours
☐ Loss of production 4-8 Hours
☐ Loss of production 8-24 Hours
☐ Loss of production :

SINTEF

12. Approximate Financial Impact
☐ 0 – 10,000 $
☐ 10,000 $ - 100,000$
☐ 100,000 $ - 1,000,000$
☐ More than 1,000,000$

13. Equipment Involved	
Controller	☐ Describe: (SAS, SIS, ICT)
Network	☐ Describe:
ICT	☐ Describe: (servers, desktop, laptop)

14. Manufacturers of equipment			
☐ ABB	☐ Siemens	: ☐ Other:	☐
☐ AIM (Kongsb)	☐ AllenBradley	: ☐	☐
☐ Honywell	☐ Bailey	: ☐	☐

15. Network Type
Describe:

16. Protocols Involved		
Industrial Application	☐ Describe:	
Internet Protocol	☐ Describe:	

Incident description in free form, not covered earlier

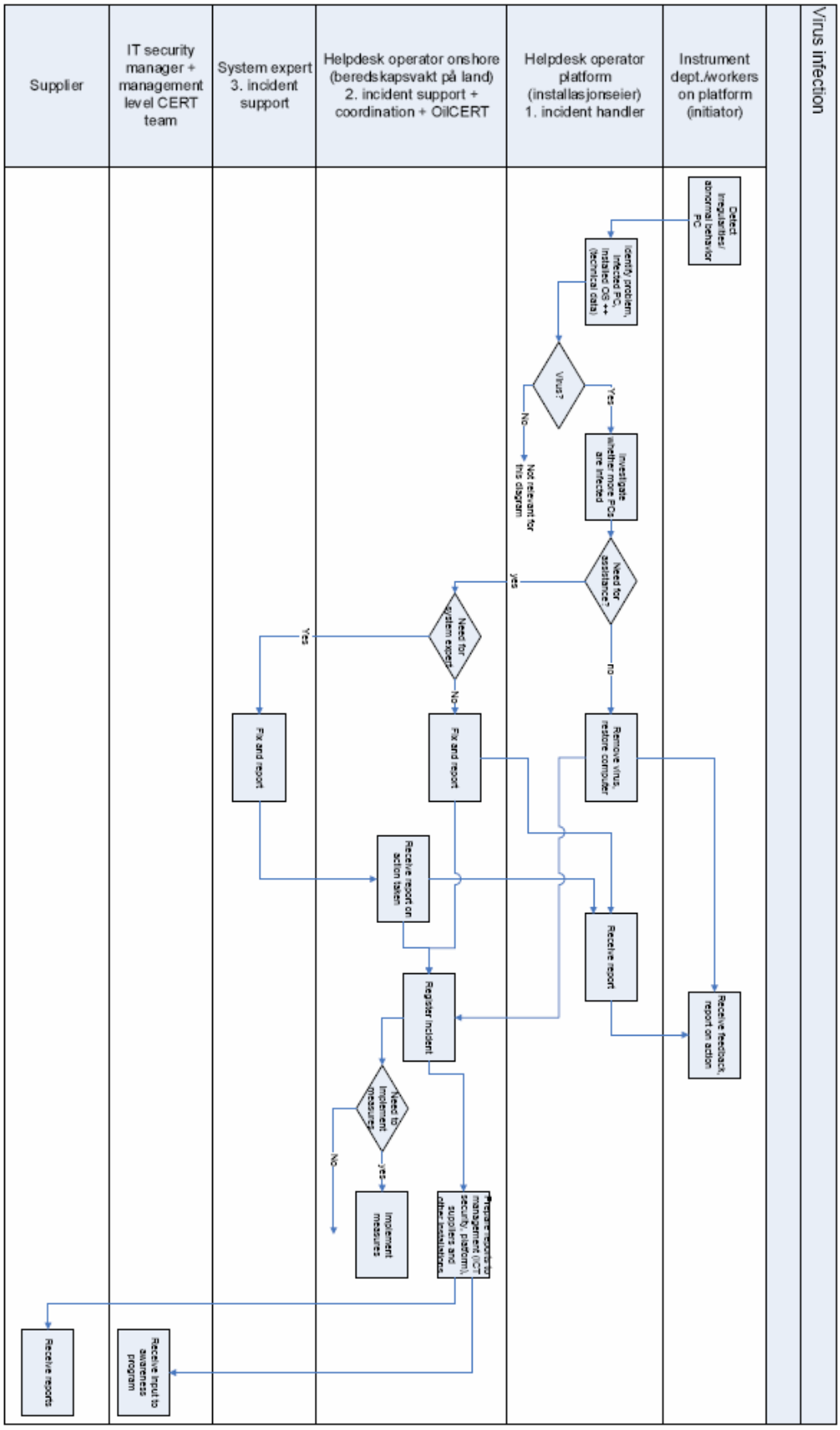
17. Step diagram with a general description of the incident

18. Description of impact on the organization

19. Suggested barriers to ensure that the incident is not happening again

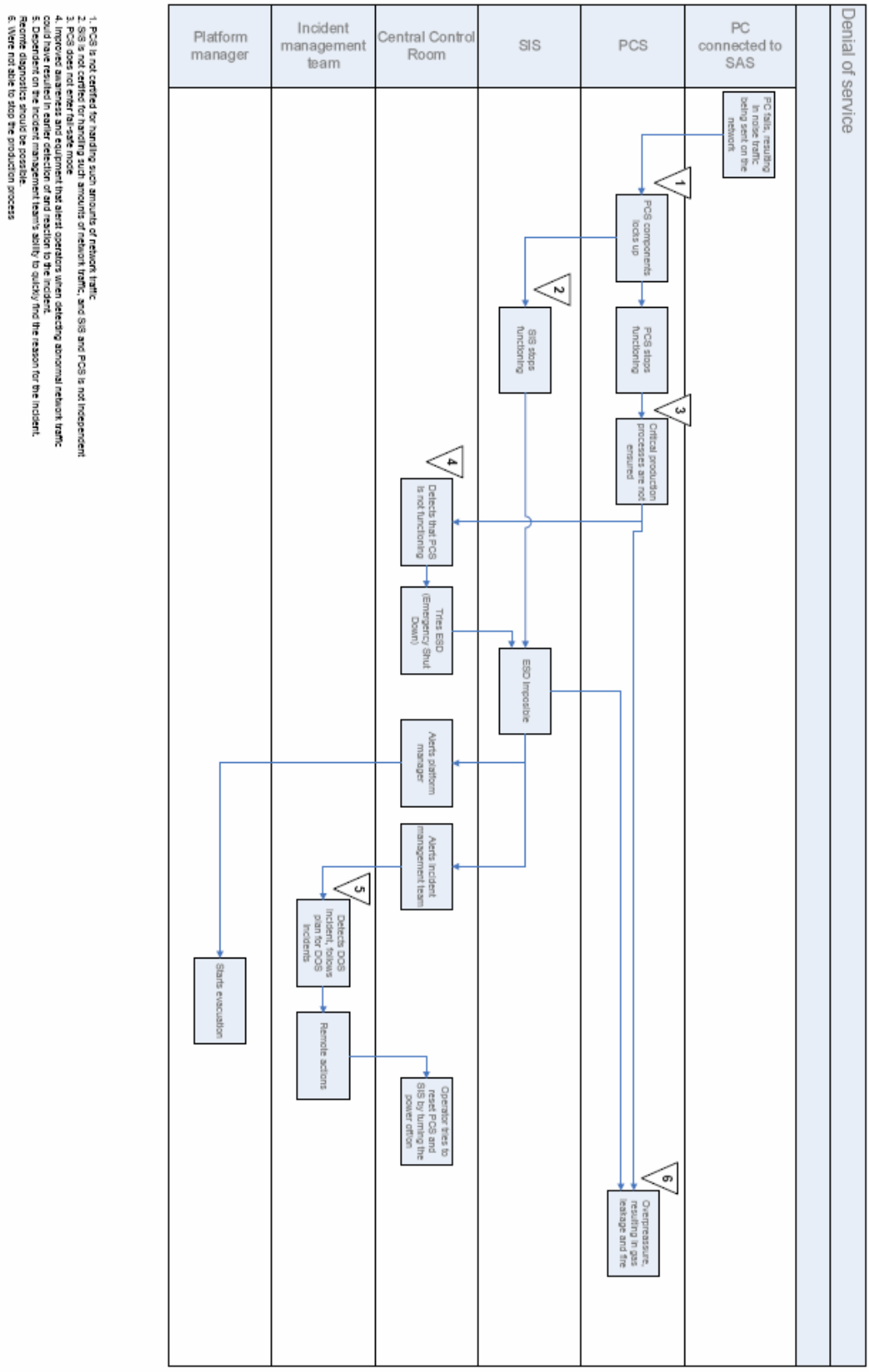
20. References to the incident (Web, articles, publications)

Appendix F STEP Diagram for Incident Response Planning



This diagram is available electronically at http://www.sintef.no/irma

Appendix G STEP Diagram for Documenting an Incident



This diagram is available electronically at http://www.sintef.no/irma

Appendix H The use of CheckIT

The aim of CheckIT is to reduce the probability and consequences of ICT/SCADA incidents by improving safety and security culture in the oil and gas industry. Our focus is security and safety problems that arise in a network of cooperating companies performing integrated operations. A full description of CheckIT can be found in [61].

CheckIT has been based on organisational culture [62]. The framework for cultural assessment draws on Westrum's taxonomy [63]. A possible development of safety and security culture from "bad" to "good" (i.e. from the pathological culture to the generative culture) is described. The levels of safety culture from Westrum are:

- *The pathological/denial culture* – organisations that fit this characteristic are self organized on a basic level and strive to maintain status quo. They will deny warning signals, punish those who bring them up and try to keep reporting at a minimum. Their focus is on doing business and maintaining the impression of everything being as normal.
- *The calculative/rule based culture* – These organisations are strongly rule oriented, and driven by management systems. They put great effort into forming and imposing rules, which are intended to cover both unwanted situations and external requirements. They have a limited repertoire of measures when an event occurs, and focus is mainly on simple deviation handling.
- *The generative/learning culture* – organisations that are generative put great effort into active participation on all levels, and align organisational goals with safety oriented goals. They perceive safety and security as an opportunity and an inherent part of the business, rather than an imposition of costs. The company's own and other companies' experiences are actively used to continuously improve the safety performance. Attainment of this level is suggested as the goal in CheckIT.

A key foundation of CheckIT is to change fundamental values or root causes by establishing meeting arenas where double loop learning can be performed as described by Argyris and Schön [64]. Through group discussions, root causes should be identified and the participants should be able to suggest changes and improvements To establish discussion of underlying values it may be important to involve external participants in the process, since external observers could more easily identify underlying values. To further aid in this discussion, scenario analyses of safety critical operations could be performed ref [54]. To analyze the different scenarios, it is suggested to use different accident investigation tools to aid in creating common mental models. The STEP method [49] could be useful.

The basic package of CheckIT comprises 31 questions [65]. Additional questions are provided to configure the survey according to the needs of the organisation. Each question has a description of alternative answers related to the cultural level. The aim is to develop a rating of the organisation on a numerical scale from 1 to 5, where alternatives one, three and five are described. The alternatives correspond to the cultural taxonomy described by [63]:

- Denial culture (Level 1)
- Rule based culture (Level 3)
- Learning/generative culture, seen as "Best practice" (Level 5)

The utilization of a five-point scale provides a basis for a normalized score throughout the organisation and makes it possible to compare results against other organisations.

Many of the questions are based on work within the field of safety culture and high reliability organisations (HRO) [66]. Central topics include management involvement, establishing clear

responsibilities, establishing a common risk perception, common manners of communication, and trying to build a common understanding.

The implementation and use of CheckIT could be seen as implementing a fundamental change. To ensure that such a change can take place, we suggest following the best practices related to leading change as described by Kotter [67] e.g.:

- Establish a sense of urgency among the participants in the organisation and in the cooperating organisations.
- Creating a Coalition, involving management and key stakeholders
- Developing a motivating vision that is relevant to the actual business and Communicating the change vision to empower broad-based actions
- Generating short-term wins, document the benefits, consolidating the gains and producing more change and anchoring new approach in the culture

The suggested approach includes the following steps (See Figure 7-1):

1. *Identify key indicators.* Identify goals and key indicators to be improved by the use of CheckIT. A key indicator could be the number of security incidents that penetrates the security barriers. It is important to get management commitment to scope and effort for the use of CheckIT. It is important to establish a learning arena among important stakeholders to support organisational learning. Prior to use the questions should be discussed and adjusted to the vocabulary and terms used in the specific industry.
2. *Perform assessment of safety and security culture* via the questionnaire to identify challenges. The questionnaire should be filled out individually and then discussed in a group setting. This implies that we view culture as a property of collectives – e.g. groups or organisations.
3. *Reflection in groups:* Discuss and reflect on the answers in a group setting, to identify areas to be improved. During this discussion it is important to try to identify the root causes or fundamental changes to be implemented to improve the key indicators. Management should be a part of the group. Key stakeholders outside the organisation influencing safety and security should be included.
4. *Identify and agree on actions* based on good co-opting processes. (The term *co-opting process* is used to describe a decision process involving both management and work force where the issues are discussed freely prior to a decision.) Implement the suggested actions in a good co-opting process.

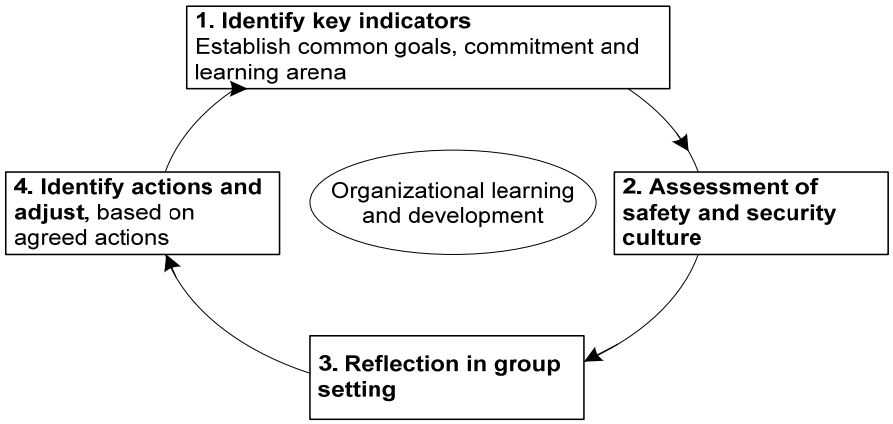


Figure 7-1: Suggested approach to foster organisational learning

This assessment should be done in two steps. First, the individual participants are to complete the questionnaire on their own. Then the result should be discussed in the workgroup. If key safety and security operations are outsourced to a service firm, actors from the service firm should participate.

The participants should identify areas to be improved. Reasons to improve the culture are a result that shows that the cultural level is too far from "best practice" or differences in the cultural levels among the actors in the network are significant and may lead to misunderstandings or even an incident or accident. The structure and layout of the questionnaire is illustrated in Figure 7-2 .

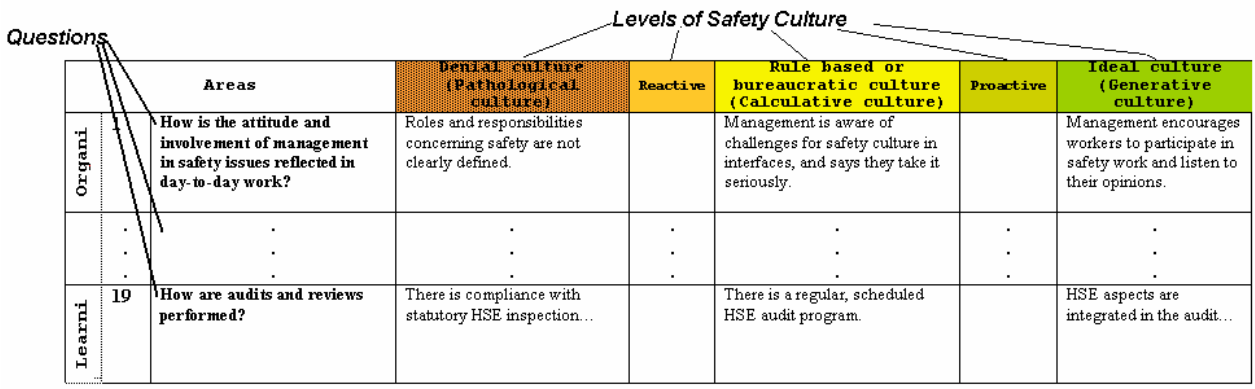


Figure 7-2: Layout of the CheckIT questionnaire

The questions to be elaborated are documented on the CheckIT web page [65, 68].

The main activities and resources to be used in a CheckIT analysis are:

- **Preparation and organisation (**½ day) – identify relevant key indicators and identify people to attend the workshop, go trough and adjust the questionnaire to the relevant industry, establish a sponsor from management, motivate and prioritize the work with safety and security, culture.
- **Workshop (**½ day) Assessment and reflection of security and safety culture in a group. Use CheckIT. Identify actions – as agreed in teamwork.
- **Follow-up (**½ day). Document improvements in security and safety culture and Information Safety in general. Document the development of key indicators, discuss the result with the relevant stakeholders.

Improvement of security and safety culture is not an activity that can be done only once; it is a continuous process. We propose that a CheckIT survey should be performed periodically, each year. The development of key indicators should be assessed each period, and the effect of using CheckIT should be assessed. The use of the method does not require many resources but requires management commitment.

Appendix I Proactive and reactive barriers

In the following we present examples in tabular form of proactive and reactive barriers that may be employed in an offshore setting.

Proactive Organisational barriers

Projects	Are information security prioritised early in all projects?
Responsibility	Is there precise responsibility related to operations of the ICT/SCADA network
Rules and Procedures	Has there been established a short and common plan documenting incident response?
	Has a best practice routine such as Hydro SOL been implemented, involving a Central Room Operator to control remote access in addition to technical solutions?
	Has a risk assessments been performed for process control, safety, and support ICT systems and networks. (ISBR 2)
	Is there a disaster recovery plan for critical process control, safety, and support ICT systems. (ISBR 7)
	Are there change management and work permit procedures for all connections to and changes in the process control, safety, and support ICT systems and networks. (ISBR 10)
	Are there procedures for reporting of security events and incidents. (ISBR 16) and is an open reporting culture been established among operators and suppliers?
DFU scenario training	Has a DFU scenario analysis been performed between operator and suppliers?
	Has the suppliers and operators discussed common risk perceptions?

Proactive Technical barriers

Firewalls	Have firewalls been implemented based on a best practice scheme?
	Are the firewall logs analysed systematically?
IDS	Has an IDS system been implemented?
HoneyPot	Has a Honey-Pot solution been established, to act as a proactive indicator related to incident handling
Selected Technical elements from ISBR	Has the interconnection between ICT and SCADA systems been tested and certified, and have the SCADA network been tested and certified for ICT traffic?
	Does the infrastructure provide segregated networks, and are all communication paths controlled. (ISBR 4)
	Is there an updated network topology diagram including all system components and interfaces to other systems (ISBR 11)
	Are the ICT systems kept updated when connected to process control, safety, and support networks. (ISBR 12)
	Do the process control, safety, and support ICT systems have adequate, updated, and active protection against malicious software. (ISBR 13)

Proactive Human Factors barriers

Training and awareness	Have the users of process control, safety, and support ICT systems been educated in the information security requirements and acceptable use of the ICT systems. (ISBR 5)
	Have the participants from suppliers and other operators been educated in the information security requirements and acceptable use of the ICT systems.
Safety Culture (CheckIT)	Has a CheckIT analysis been performed? (We are suggesting to perform a CheckIT analysis annually, to ensure that no complacency is setting in.)

Reactive Organisational barriers

Responsibility	Clear responsibility and Incident Response Team is available
Rules and Procedures	Updated Incident Management routines are available
	Use the IRMA incident response form to document the incident and record the missing barriers

Reactive Technical barriers

Firewalls	The firewalls are implemented as a best practice solution
Technical elements from ISBR	The systems have the latest patches

Reactive Human Factor barriers

Training and awareness	Have the users of process control, safety, and support ICT systems been educated in the information security requirements and acceptable use of the ICT systems. (ISBR 5)
Safety Culture (CheckIT)	Has a CheckIT analysis been performed

Organisations should analyze the detailed risk assessment, identify the cost of mitigation for each risk, compare the cost with the risk of occurrence, and select those mitigation controls where cost is less than the potential risk. Because it is usually impractical or impossible to eliminate all risks, organisations should focus on mitigating risk with the greatest potential impact.

As the team identifies mitigation strategies, risks may be identified that can be mitigated by "quick fix" solutions—low-cost, high-value practices that can significantly reduce risk. Examples of these solutions are restricting Internet access and eliminating e-mail access on operator control stations. Organisations should identify, evaluate, and implement suitable quick fix solutions as soon as possible to reduce security risks and achieve rapid benefits. The Department of Energy (DoE) has a "21 Steps" document [69] that could be used as a starting point to outline specific actions to increase the security of SCADA systems.

SINTEF

Appendix J Publications from the IRMA project

The IRMA project has generated a number of scientific publications and presentations, which are summarised in the following.

International

The IRMA project was outlined in the following paper (published before commencement of the project):

- *From Incident Response to Incident Response Management* [70, 71]

  ABSTRACT
  In this paper we propose the development of a methodology for efficient handling of computer security related incidents. Such a methodology should include technical, cultural, and organisational issues.

Papers published during the project:

- *Towards more secure virtual organizations by implementing a common scheme for incident response management* [72]

  ABSTRACT
  Remote operation and control of offshore oil and gas production is increasing in the North Sea. The technology used to support operations and exception handling is changing from proprietary closed systems to standardized IT systems built on PCs and MS Windows. The PCs are integrated in networks that can be connected to the Internet. This leads to a major change in which threats the industry faces. PCs using MS Windows are vulnerable, new exploits are continuously found and the number of hacker attacks is increasing. The reliance on MS Windows and Internet is thus increasing the vulnerability of the oil and gas production. In addition, a network of companies that functions as a virtual organization is increasingly performing the operations and management of the oil and gas fields. These virtual organizations and the increased number of vulnerabilities create the need for common safety and security culture, communication and incident management during regular operations and when handling information security incidents. In this paper, these challenges are presented and discussed, and a suggestion for a standardized scheme for Incident Response Management in the North Sea is proposed. We suggest exploring information security incidents across the virtual organizations, and to standardize on reporting and on training to be able to establish common goals and objectives. All in order to establish more resilient organizations and systems related to information security.

- *Monitoring of Incident Response Management Performance* [40]
  See section 4.6.1

- CheckIT articles [61, 73-75]
  See Appendix H.

In Norway

- ”Access @ Plant - Automatisering av prosesser på et IKT-sikkert grunnlag”, arrangert av Norsk Forening for Automatisering (NFA),
  26.- 27. januar 2005, Bergen.
  Johnsen, S.O.: *Sikkerhetskultur i organisasjoner basert på SjekkIT*

- ”IKT SoS-seminar” arrangert av Norges forskningsråd for alle som har fått prosjektmidler fra forskningsprogrammet IKT Sikkerhet og sårbarhet.
  1.-2. mars 2005, Gardermoen.
  Longva, O.H.: *Incident Response Management*

- ”Risiko og sikkerhet i IKT-systemer”, Tekna-seminar
  9. – 10. mars 2005, Oslo
  Longva, O.H.: *Incident Response Management*

- ”Automatisering og integrerte operasjoner”, arrangert av NFA,
  14.-15. juni 2005, Høgskolen i Østfold, Halden.
  Johnsen, S.O.: *Leveransesikkerhet i integrerte operasjoner (safety and security)*

- ”Høstkonferansen ISF 2005”,
  13. – 15. september 2005, Sandefjord
  Johnsen, S.O.: *Utvikling av sikkerhet og sikkerhetskultur*

- ”Sertifisering og standarder innen informasjonssikkerhet”, Abelia-seminar
  20. september 2005, Oslo
  Line, M.B.: *ISO/IEC TR 18044:2004 Information security incident management*

- “Integrasjon DCS/IKT-systemer”, IFEA-seminar
  25. januar.2006,
  Line, M.B.: *Sikkerhet ved sammenkobling av DCS- og IKT-systemer*
  Johnsen, S.O.: *Utvikling av sikkerhet og sikkerhetskultur i nettverksorganisasjoner*

- ”Access @ Plant - Informasjonssikkerhetsstandarder og etablert praksis for automatiseringssystemer”, arrangert av Norsk Forening for Automatisering (NFA), 1- 2. februar 2006, Stavanger.
  Bodsberg, L., Johnsen, S.O.: *Hvordan kan integrerte operasjoner gi bedre sikkerhet?*

- Society of Petroleum Engineers (SPE)-seminar,
  26. april 2006, Bergen
  Line, M.B.: *Information security – a must for successful integrated operations*