NTNU – Trondheim
Norwegian University of
Science and Technology

Indicators for ICT security incident management

Bimal Raj Pandey

Master of Telematics - Communication Networks and Networked Services (2
Submission date: Januar 2013
Supervisor: Svein Johan Knapskog, ITEM
Co-supervisor: Maria B. Line, ITEM

Norwegian University of Science and Technology
Department of Telematics

Indicators for ICT security incident management

TTM4531
Master's Thesis
(January 19, 2013)

Bimal Raj Pandey
Telematics

Supervisor : Maria B. Line
Professor : Svein Knapskog

Department of Telematics
Norwegian University of Science and Technology
Autumn 2012

NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY, MATHEMATICS AND ELECTRICAL ENGINEERING

PROJECT ASSIGNMENT

Student's name:	Bimal Raj Pandey
Course:	TTM4531, Master thesis
Thesis title:	Indicators for ICT security incident management

Thesis description:

Managing security incidents, such as DoS attacks and intrusions, is a challenging task for many organizations. The use of indicators can improve the abilities for follow-up on information security incident management. Indicators such as "average time spent on responding pr. incident" or "total consequences of incidents during a period" can say something about the quality of the incident management process. Indicators can also potentially be used as early warnings that incidents are about to initiate. Within safety there exist a large body of work on indicators. Though measurements and the use of indicators have gained some attention also for information security incident management, the experiences of using indicators for this purpose are relatively sparse. This task includes assessing to what extent the indicators commonly used for safety can be reused or adapted for information security incident management.

Department:	Department of Telematics
Supervisor:	Maria B. Line
Responsible professor:	Svein Knapskog

Preface

The thesis entitled, "Indicators for ICT Security Incident Management", is final year project performed as a partial requirement for the fulfilment of Master of science in Telematics at Norwegian University of Science and Technology, Department of Telematics, Trondheim, Norway.

I express my deepest gratitude to Prof. Svein Knapskog whose valuable suggestion and continuous guidance was major factor to reach to point where I am now. His care and tremendous cooperation always kept me on the right side. His encouraging suggestions always build my inner strength to acquire positive attitude. It is my pleasure to thank my supervisor Maria B. Line. Her attention and guidance has been one of motivative factors to do this project. Her advices always used to add value to my project. I would also like to thank Laurent Paquereau and Mona Nordaune from our department for their great help and support. I am also indebted to Ole Morten Grodås from Norsk Helsenett for his valuable suggestions and information. Many thanks to Arne Oslebo and Rune Sydskjør from Uninett for their valuable information.

A many many thanks goes to my friend Pramod Ghimire who has been always with me when I needed some suggestions. I would also like to thank my other friends and my families for their help and support.

Bimal Raj Pandey
Trondheim, Norway
January 2013

Abstract

Managing the different types and the nature of information security incidents has become a challenging task. However, the use of security incident indicators can improve the capabilities of the incident management process. Indicators are not only needed to assess and monitor the quality of incident management capabilities by quantifying overall processes, but also to provide an early warning and notification of incident occurrences. Though some research work has been initiated for development of measurements and indicators in information security incident management, use of those have been relatively sparse. Also, varied profiles of organizations, changing nature of threats and frequent update and advancement in technology have made it difficult to establish a set of common measurements and indicators. However, there exists significant amount of research, development and implementation of indicators in the safety field. It would be of significant interest to investigate whether safety performance indicators could be adapted to the field of security incident management.

In this thesis, a literature study has been performed in the field of safety performance indicators. This study provided us with some results, indicating that effective safety performance indicators could be adapted to the security incident management field. Effective indicators have been adapted to different phases of security incident management through a defined methodology. Those indicators are analysed in detail with their usage, scope, pros and cons in different phases of the incident management process. This thesis also includes a scenario describing the use and implementation of such indicators. It was found that safety indicators could be adapted to the plan, prepare and protect phase, the respond phase and the review phase of an incident management process, and they have been effective to measure the efficiency as well as the capabilities of corresponding phases. For the detection phase, however, it was found that the safety indicators could only be adapted with great difficulties.

Contents

List of Figures

List of Tables

Acronyms

CIA Confidentiality, Integrity and Availability. 1, 18, 50, 73, 82

CIS Centre for Internet Security. 4, 20

CSFs Critical Success Factors. 17

CSIRT Computer Security Incident Response Team. 23, 49, 53–56, 77

DoS Denial of Service. v

ETA Event Tree Analysis. 12

FTA Fault Tree Analysis. 12

HRA Human Reliability Analysis. 12

HSE Health and Safety Executive. 14, 15, 21

ICT Information and Communication Technology. 4, 5

IDPSs Intrusion Detection and Prevention Systems. 31, 33, 44, 46, 49, 50, 73, 78

ISIRT Information Security Incident Response Team. 56

ISMS Information Security Management System. 69

ISO International Organization for Standardization. 3, 4, 11, 23, 29, 55

ISO/IEC International Organization for Standardization/International Electrotechnical Commission. 9

ISPs Internet Service Providers. 33

IT Information Technology. 23, 40, 49, 53, 54, 77

MARS Major Accident Reporting System. 12

NIST National Institute of Standards and Technology. 3, 4, 10, 11, 20, 23, 29

OECD Organization for Economic Co-operation and Development. 11, 12, 14, 15, 21, 24

PoC Point of Contact. 56

RIF Risk Indicating Factor. 12

SANS SysAdmin, Audit, Network, Security. 23, 50

SCADA Supervisory Control and Data Acquisition. 19

SIEM Security Information and Event Management. 46, 49, 50, 78

SMIS Security Management of Information Systems. 3

SPI Safety Performance Indicators. 15

UK United Kingdom. 14

US-CERT United States Computer Emergency Response Team. 2

USA United States Of America. 14

Chapter 1

Introduction

1.1 Background and Problem

Information is created by people. There is also chance that they will loose it. People loose information because other people want it. The people who are stealing the others' information are technically called attackers, hackers or intruders. They steal information for various reasons. Some might want to make money, some might want to disrupt the organizations and their values and some might want to leak the secret information. To prevent all these information theft done for any reason, essentially to protect critical information, information security comes into play. It has a very long history. Since introduction of digital world, the need of information security has been increasing more and more. Though the unambiguous definition information security has been topic of debate, still accepted explanation of information security is, 'Information security is way of ensuring Confidentiality, Integrity and Availability (CIA) of an information'. In an organization, information systems are critical assets supporting the organizational mission [2]. The vulnerabilities in those systems might be exploited by threat agents or attackers resulting the occurrence of information security incidents. It can compromise the CIA of information as well as disrupt business process of an organization. The figure 1.1 shows how security incidents are occurred. It shows that the weaknesses, so called vulnerabilities, in the security control systems are exploited by threat agents and lunching the attack vectors they disrupt the security functionality, critical assets which might result in huge business impacts. ISO/IEC 27035 [4] has documented following categories of security incidents:

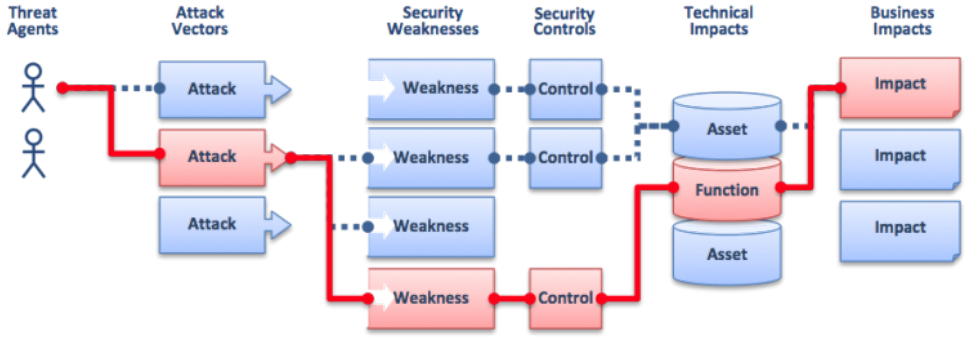

Figure 1.1: Security Incident Occurrence [3]

1. Denial of service

   An incident that prevents the partial or complete access of networks, systems, or applications to legitimate users by exhausting resources.

2. Malicious code

   A virus, worm, Trojan horse, or other code-based malicious entity that are inserted into other program to modify its original content.

3. Inappropriate Usage

   An incident caused when user violates organization's information security policy.

4. Unauthorized access

   A incident caused when an unauthorised person gains access to or misuses a system, service or network.

5. Information gathering

   Activities linked with finding potential targets like vulnerabilities in the system or network that could be exploited.

The figure 1.2 shows number of security incidents reported by federal agencies to the United States Computer Emergency Response Team (US-CERT) during fiscal years from 2006 to 2011. It shows that the total number of incidents was 5503 in 2006. It has increased to 42887 in 2011. The increase is more than 650% during five years. This proves that how insecure our information systems have been. However, US-CERT has interpreted this result as improvement in

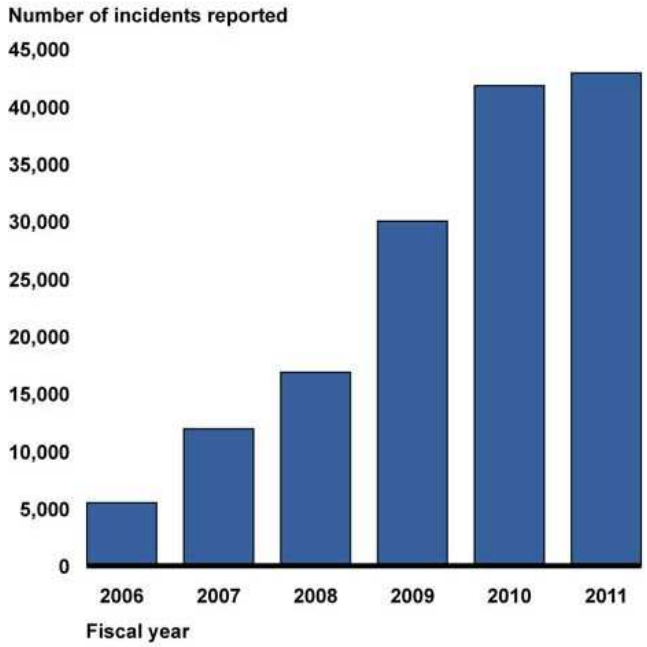

Figure 1.2: Incidents reported to US-CERT by federal agencies during fiscal year 2006 to 2011 [5]

detecting and reporting of incidents in addition to the serious information security risks illustrated by it. [5].

Security Management of Information Systems (SMIS) has been focusing towards patching and fixing breaches rather than implementing dynamic strategies for preventing them [6]. However, the priority must be given to prevent the security incident first. In case of their occurrence, necessary steps must be taken to respond and recover from those incidents. Standards like National Institute of Standards and Technology (NIST) [7], International Organization for Standardization (ISO) [4] have documented the formal steps for handling those incidents. It includes steps and procedures from protecting against security incidents to detecting and responding to them.

The technologies are advancing, nature of threats are changing, organizational requirements are growing due to increasing and changing demand of customers and users, at the same time information security practice is different for different organizations. Above all of those, organizations have different goals and objectives. They have plan, policies and guidelines to achieve those goals. Every time numerous and diverse security incidents are occurring. The managing those in-

cidents is somehow challenging. It is somehow difficult to eliminate threat but it might be easier to find out degree of vulnerability and risk presented in the system which are being exploited. It is also mandatory to monitor the performance level of your incident management process or implemented information security management system. Considering all those factors, the fact regarding the measurement of security and its processes can not be ignored. If something is to be improved, it needs to be measured in quantitative term which will indicate its trend. When the results are quantitative, then it will be easier to compare, decide, review and communicate.

The direction of measurement in the information security has just started few years back. After the few research papers [8, 9, 10, 11, 12] on information security metrics, the standards NIST and ISO documented the measurement of information security process in their publications *Performance Measurement Guide for Information Security* [13] and *Information technology - Security techniques - Information security management - Measurement* [14] respectively. Then it was followed by number of research papers [15, 16, 17], research organizations [1,2,3] presenting their research papers [18, 19, 20, 21] on information security measurements, metrics and indicators. Though there are lots of taxonomies, classification and development of information security metrics and indicators, standard, formalised and implementable indicators are yet to be discovered and this is challenging too. A researcher from NIST, Wayne Jansen, presented in his paper that metrics and indicators developed by Centre for Internet Security (CIS) [19] have been somehow useful in implementation too.

Organization's business goals and information security goals are inter related to each other. The ineffectiveness of implemented information security control system always impacts the overall business goals. But, to understand the effectiveness of implemented security control systems, it needs to be measured. This task is fulfilled through development and implementation of the indicators. After then, efficient allocation and utilisation of security resources, evaluation of assets and economy might be achieved [6].

1.2 Purpose and Scope

The thesis, entitled as 'Indicators for Information and Communication Technology (ICT) security incident management, is task for fulfilment of partial require-

[1]http://www.sans.org/
[2]http://www.securitymetrics.org/content/Wiki.jsp
[3]http://cis.org/

ment of Master of science in Telematics in Norwegian University of Science and Technology. This thesis is performed under the guidance of supervisor for department of telematics.

The main purpose of this thesis is to perform the theoretical study of the indicators for the ICT security incident management. Numerous security incidents are occurring day by day. Managing those incidents is a challenging task. But the introduction of the indicators in field of security have somehow been effective for management of those incident. Indicator not only measures the performance of the incident management process but also provides the early notification that the incident is occurring. This information could be vital for early prevention of the security incidents. This could also be effective way to manage the changes occurring in an organization regarding the security process. All in all indicators can be used for monitoring the performance of the incident management process which include preventing incident to detecting and responding to it and also measures the capability of incident management team. But the problem is that, within security area there are limited standardised and formalised indicators.

In the safety area, researches on the safety indicators have very long history. Since establishment of various hazardous industries like chemical industries, oil and gas industries, number of accidents were increasing and necessity improvement of safety performance level was felt. This has led to development of various indicators for monitoring of the safety performance level in those industries. Thus, the reuse and adaptation of those indicators in the security incident management could be of immense interest. This thesis deals with the reuse and adaptation of safety indicators to security incident management. The task of this thesis could be summarised as below:

- To study and research the available indicators in the safety area
- To assess what extent safety indicators can be adapted as security incident management indicators
- To perform high level analysis of those indicators

However, the scope of this thesis is limited to the development of the indicators. The implementation of the adapted indicators from safety to the security incident management is out of scope of this thesis. It is also important to remember that the issues and the indicators from the safety area are analysed in terms of information security i.e confidentiality, integrity and availability.

1.3 Research Approach

The research methodology adapted in this thesis is a pure theoretical study. There are no practical experiments done in this thesis. Though during the study, meetings with UNINETT and Helsenett, which are leading network provider in Norway in field of education and health respectively, were conducted to gather useful information regarding the security incident management process and indicators. It helped to provide some information regarding the challenges as well as difficulties regarding the implementation of incident management process and indicators. Similarly, a lot of literature review is done to gather information of useful indicators that already exited in the safety field as focus of thesis is also adapting the safety indicators to security incident management.

1.4 Structure

The thesis is mainly focusing on the topic development and reuse of the indicators those already existing on the safety field to the field of security incident management. The thesis provides theoretical study and development of the security incident management indicator. It is written in such a way that it flows from the methodology used to adapt safety indicators as security incident management indicators to general assessment of those indicators in a smooth pattern. The total number of pages in this report is 114 including formal pages (like title pages, abstract), references and appendices. The whole thesis is divided into six chapters excluding references and appendices. The following section presents the brief introduction of the thesis structure.

Chapter 1: Introduction

This chapter presents the overview of the problem exited in the information security field focusing on the background and history of the information security indicators and metrics. This also presents the purpose and scope of this thesis including the approach taken for this research generally called as research methodology. So overall this chapter provides overview of the whole thesis.

Chapter 2: Background and Knowledge Adaptation

This chapter basically provides the literature review on related field. The different previous works done in the field of indicators (security as well as safety) are overviewed in this chapter. This chapter provides basic foundation for adapting safety indicators in the field of security incident management.

Chapter 3: General Method for Incident Management Indicators Develop-

ment Programme

This chapter deals with the general process that can be used to develop the security performance indicators. Somehow based on this process the methodology used in this thesis to reuse the safety indicators as security incident management indicators are discussed. The methodology discussed here is followed on the following chapter.

Chapter 4: Security Indicators Development and Assessment

This is the main chapter of the thesis. This chapter provides the detail description of how security incident management indicators are developed from the safety part. The detail description of the incident management phases are also described. Along with this, indicators are developed and described in each phases of security incident management with their short specification in tabular form.

Chapter 5: Discussions and Recommendations

This chapter presents the discussions of the indicators developed in the chapter 4. It includes description regarding advantages and disadvantages of those indicators. It also presents the characterization of indicator as leading and lagging indicator. Finally, a short scenario is presented to show how those indicators can be used and implemented.

Chapter 6: Limitations, Conclusion and Further Research

This chapter briefly concludes the thesis with limitations of the research work. It also provides brief description of future works that be carried out further in this field.

Chapter 2

Background and Knowledge Adaptation

2.1 The purpose of indicators

Organizations always have some goals. When we set a system, we also set goals. Sometime it becomes necessary to find out level of progress we have achieved towards meeting our goals. Those levels can only be discovered by the help of indicators. Basically indicators measure our progress towards goals. It is way of quantifying 'things' for better understanding, comparing, improving and sustaining. The 'things' could be in different sectors like financial, health, communication, engineering, networking, security and safety. Mostly indicators are useful to evaluate the system change. They track the progress and objectives of the system by providing notification of change. Though indicators measure system performance, it is also essential not to skip the performance goals while evaluating indicators. Otherwise indicators become meaningless. *International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27004:2009 Information technology - Security techniques - Information security management - Measurement* [14] defines, "An indicator is a measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs." It also adds to the statement that indicators becomes useful when they are used with respect to defined needs and goals. The Institute of Operational Risk describes in its paper [22] that indicators should be selected based on their characteristics and further mentions, the desired characteristics of indicators as *relevance, measurable, predictive, easy to monitor, auditable and comparability*. So, the

organizations should not just only pick the indicators to measure the system performance but should select the good indicators that provides true reflection of their system performance.

Indicators evaluate the system performances. Apart from that, indicators also notify that something is going to happen. In the field of information security, it is also known as incident precursor. Though there has been lot of research on indicators in the safety field, information security field still lacks basic and standard indicators. The reason behind this might be absolute nature of security field. Threats keep on changing day by day, as technology is advancing. The changing nature of threats makes it hard to predict. To identify whether the security incidents have occurred or not or might be occurring, the notification regarding incidents must be identified. *NIST SP 800- 61 Revision 2, Computer Security Incident Handling Guide (Draft)* [7] has defined those signs as precursors and indicators. Precursors provide signs of incidents that might occur in future where as indicators provide signs regarding what may have occurred or may be occurring. These can be viewed as the direct warning indicators rather than the performance monitoring indicators of the system. Cloppert [23] classifies the indicators based on the attack progression and behaviour of the attacker. He classifies them as atomic indicator, computed indicator and behavioural indicators. He further states that atomic indicators are pieces of data to indicate the activities of attacker whereas computed indicators are well computed data like hashes of malicious files and behaviour indicators are combination of all indicators which creates the profile of the attacker. He also presented the indicator life cycle as shown in figure 2.1 which explains that indicator regarding occurrence security incidents could be discovered through analysis, search and tune.

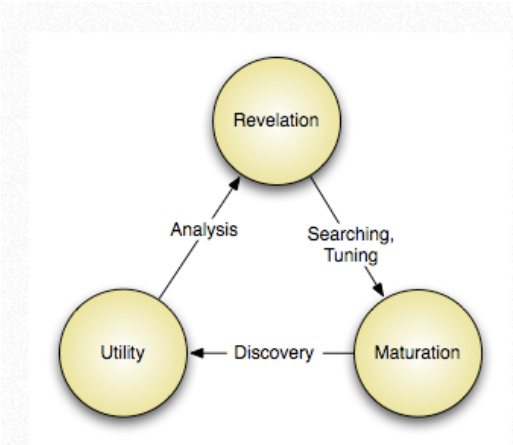

Figure 2.1: The indicator Lifecycle State Diagram

The analysis of the technical information regarding incidents like samples of

malware, different vulnerabilities exploited by incidents, hostnames and IP addresses of adversaries are always helpful to find suitable indicators of incident occurrence. NIST's Computer Security Incident Handling Guide (Draft) [7] also supports the above statement and further clarifies that sharing of internal indicators and external indicators gain form partner organizations also will be useful in identifying true incidents.

2.1.1 Metric vs. Indicator

Measurement provides the standard value that are specific to time. When two or more than two measurements are taken and compared, then it becomes metric. Basically, metric is objective as well as subjective analysis of the different values that are resulted because of the measurement. When those values are compared against the predefined, standard or baseline value, it will show deviation and trend of measured values against the baseline which indicates the performance level, so called as an indicator. ISO [14] has also used the term 'measures' to refer to the indicator. José [12] mentions in his paper that indicators might be seen as refined metrics. Furthermore, he indicates that in addition to be few and stable, indicators always need retrospective view which are provided by the long running metrics. This expounds that the effectiveness as well as development of indicators somehow depends upon the past values. Organization for Economic Co-operation and Development (OECD) [24] states that "an indicator is designed to collect information about whether an issue of concern is achieving the desired result. A metric is then the approach by which indicator data is collected and reported". It also signifies that metric is way of collecting data through measurement and indicator reflects how those data are behaving and representing performance level. It further states,"the metric associated with an indicator is focused on the question of how the indicator is being measured, so it is defined as a system of measurement used to quantify performance (safety) for outcome and/or activities indicators". OECD [25] has used the term 'metric' basically as a system of measurement that provides data for indicators.

2.1.2 Safety Indicators

Indicators are something that provides the early warning that something is going to happen. Indicators can be used in different sectors and areas. In areas like Petroleum Production, oil and gas exploration, nuclear power plant, necessities of the safety indicators have been felt since start of those industries. Now it has been pre-requisite of those industries mentioned above to implement the effec-

tive safety performance management system to identify, eliminate and reduce the risk and accident. Many accidents have occurred in the past taking human lives. In Major Accident Reporting System (MARS)[1], 111 accidents were registered by the end of the year 1991 in oil and gas industries [26]. It was followed by other major accidents in the past. So, the necessity of safety indicators were felt those could serve as the tool to provide the early indication and warnings to reduce the accidents. OECD [24] defines "Safety Performance Indicators provide important tools for any party with responsibilities related to accident (chemical) prevention, preparedness and response and allow organizations to check whether actions they have taken to address risks (e.g., implementation of policies, programs, procedures and practices) continue to achieve their desired outcomes." Safety indicator not only provides an early notification of catastrophic failure but also leads to improvement in health, safety and environment by increasing awareness among the staffs and facilitates to take effective decision for safety-related resource allocation [24].

The research on the safety indicators have been done on the two perspectives; one is by predicting the possibility of the accidents (predictive) and another is by investigating occurred accidents i.e. finding causes after the occurrence of an event. OECD has defined this as activities indicators and outcome indicators respectively. According to it, Outcome indicators measure impact of safety actions whereas activities indicators measure safety performance against a tolerance level explaining why a result has been achieved or not [24]. Safety is one of the major attributes to assess the dependability of the system along with availability, reliability and integrity. Qualitative and quantitative analysis of safety can be performed to find the dependency between the level of system hazards or risk and system component failure. K. Øien [27] also identifies this as quantitative risk assessment which is of predictive nature. Techniques like Fault Tree Analysis (FTA),Event Tree Analysis (ETA) and Human Reliability Analysis (HRA) provide the predictive assessment to find the potential accidents.

Though the safety indicators resemble risk indicator and are used as interchange of each other, K. Øien [27] has made some distinction between those terms. He states that they are developed with different approaches as risk indicators are developed from risk based approach where as safety indicators are developed from incident based or safety performance based or resilience based approach. He introduces term Risk Indicating Factor (RIF), a theoretical vari-

[1]Major Accident Reporting System (MARS) has been established by the Commission of the European Communities for structured information collection on major accidents in industrial installation occurring within territory of its member states.

able whose operational variable is risk indicator, obtained by linking RIF to risk metric through risk model. Sometime there might be effect on the safety, so the safety indicators are evaluated based on the assumed effects on safety or by correlation [27]. The development of research on the safety indicators started in early 80s with different terms like index, rate, and measurements. Though the initial research saw some problems like lack of empirical organizational analyses, unavailability of direct measures, lack of exploration to the sub-areas, data problems or lack of data, problems in linking the safety operational indicators to risk model for its quantification, problem in evaluation of real effect on the safety though correlation between indicators and safety were assumed, many of the safety indicators and their perspectives were developed such as indicators giving early warnings or indirect indicators, level based indicators, operator specific indicators, probabilistic safety indicators, PSA based risk indicators, accident sequence precursors, resilience based indicators. There has been also a lot of research, debate and discussion on the lagging and leading safety indicators. Following section provides brief introduction to lagging and leading indicators and their utilization in the safety performance measurements.

There have been many terms used for defining indicators type by many researchers like direct and indirect indicators, reactive and proactive or active indicators, outcome-based indicators and activity based indicators, predictive and retrospective. Somehow it might be relevant to say that they are mainly talking about the leading and lagging indicators through different perspectives. The main aim of safety indicators is to monitor and notify the changes in the level of safety in the system and provide with some necessary information to take decisions for the concerned authorities regarding the changes. Sometime indicators are used after the occurrence safety incident like no. of accidents due to failure of safety instruments. It provides the information regarding the causes of incidents rather than giving the warning or notification that something is going to happen. These indicators are called the lagging indicators. Leading indicators are those that provide the early notification of the warning within the system. They monitor and evaluate errors and risks so that necessary safety procedure can be adopted and implemented to prevent the major accidents and loss of lives and properties. Øien [27] defines lagging indicator as the reactive monitoring to show the failure of the desired safety outcome and leading indicator as active monitoring used as input to achieve the desired safety outcome. Leading safety indicators are intended to predict the safety outcomes and those outcomes are provided by the lagging indicators. It can be said that the lagging indicators are the base for implementation of the leading indicators. But still differences between the lagging and leading indicators have been interest of re-

Indicators	Areas
Number of separate human performance (HP) meetings	Management commitment
Percentage of HP issues getting root cause analysis	Awareness
Ratio of unplanned to planned work orders	Preparedness
Average time to close a Smart Form	Flexibility
Number and duration of temporary modifications	Just culture
Ratio of corrective actions involving discipline/counseling/retrain or change procedure/systematic changes	Learning culture
Number of quality management observations	Opacity

Table 2.1: Leading indicators by EPRI

search. Sometimes indicators that have been selected can be interpreted as a leading and lagging indicators both and the misinterpreting lead as lag or lag as lead might result serious incidents. Hopkins [28] criticizes the differences that are provided by the some papers and safety research organizations like HSE . Hopkins [28] as well as other researchers believes that focus should be on the development and utilization of meaningful safety indicators rather than the differentiation between lead and lag. The table 2 below shows some of the leading indicators by EPRI[2] [27].

In the report by Helene Cecilie Blakstad [29], she presented number a of safety indicators used in petroleum industry of United Kingdom (UK), United States Of America (USA) and Norway. Though she has not differentiated whether used indicators are lead or lag indicators, number of issues like purposes, approaches, aspects, nature (predictive or retrospective), effects, generalization and uses of the indicators within the national context have been discussed.

The research organizations like Health and Safety Executive (HSE), OECD, SINTEF have been actively involved in the safety performance indicators development. They have published number of research papers and standards on

[2] Electric Power Research Institute http://my.epri.com/portal/server.pt?

safety performance indicators development. The research papers by OECD, *Guidance on Developing Safety Performance Indicators related to Chemical Accident Prevention, Preparedness and Response* [25, 30], have been effective in developing as well as implementing the safety performance indicators. It provided safety performance indicators development guidance to different targeted audience like industry, public authorities and communities. It has documented step by step approach to develop an effective Safety Performance Indicators (SPI) program for targeted audiences with some scenarios providing guidance for implementation. It also provides benchmark to assess existing SPI programme and discover worthful improvements.

Similarly, HSE paper, *Developing process safety indicators: A step-by-step guide for chemical and major hazard industries* [31], provides development and implementation of safety performance indicators for managing process safety risk. The OECD guidance on safety performance indicator development is also based on the HSE guidance. According to HSE, the companies implementing those safety performance indicator programmes have reported that they have:

1. increased their risk management and protection assurance.
2. saved their cost by avoiding collection and reporting of irrelevant performance information.
3. demonstrated suitability in their risk control systems.
4. enhanced their quality management by utilising the information collected for other purposes.
5. managed to minimise costly incidents.

This shows that the process safety indicators developed by them have influenced greatly in implementation too. In the same way, SINTEF technology and society under safety research, number of research papers and guidance on safety performance indicators have been documented for different hazardous industries like oil and gas, chemical. Øien has documented the research paper on the safety performance indicators, where he has developed the number of early warning safety indicators based on the resilience engineering[3] with their implementation guide. The implementation guide [32] provides guidelines on

[3]Resilience Engineering refers to capability of recognizing, adapting to, and coping with unexpected. Resilience based indicators might be useful in situation of incomplete knowledge about what may go wrong as in hazardous industries like oil and gas, chemical, we might not be aware of accidents that might happen

how those indicators can be implemented. It provides basis for proactively monitoring and evaluating safety critical activities. Thus, we have also adopted the issues, and developed safety indicators from these papers, *Guidance on Developing Safety Performance Indicators related to Chemical Accident Prevention, Preparedness and Response* [25, 30], *Developing process safety indicators: A step-by-step guide for chemical and major hazard industries* [31], *Development of Early Warning Indicators based on Resilience Engineering* [33] and *Guideline for implementing the REWI method* [32], to be used in information security incident management.

2.1.3 Security Indicators

Leading and lagging indicators are also called proactive and reactive indicators respectively in the safety field. In security incident management, leading, lagging and coincident indicators have been used. Leading indicators represent the security state of the system before the security incident. It provides the notification of what will be the security state of system in near future. Basically it predicts the outcomes. Lagging indicators represent the security state of the system after the security event. It normally analyses the historical performances. Coincident indicators indicate the concurrent security condition of the system [17]. Though the lagging indicators are used frequently as they are easy to identify and describe, the significance of leading indicators have been notified by many researchers. Leading indicators provide time and reason to adjust the information system and their components from being compromised. In security incident management, if there is early notification of increase in threat because of identified vulnerability in the system, risk of the information leaking can be minimized. But, misinterpreting the leading and lagging indicators may result in serious security consequences. Wayne [17] describes some of the indicators that can be interpreted as either leading or lagging. For example, while scanning the system by antivirus, if there is increase in the number of virus detected, as lagging indicator, it can be interpreted as the effectiveness of the implemented antivirus but as leading indicator, it shows the increase in threat level as there is increase in number of detected viruses.

Leading indicators detect implemented ineffective controls as early as possible before an incident occurs. This is only possible through implementation of a set of performance goals, so that security performance can be measured, monitored and analyzed, and corrective actions can be taken.

In Fig 2.2, Performance indicators act as tool that monitors the system. The result indicated by the performance indicators can be compared against the im-

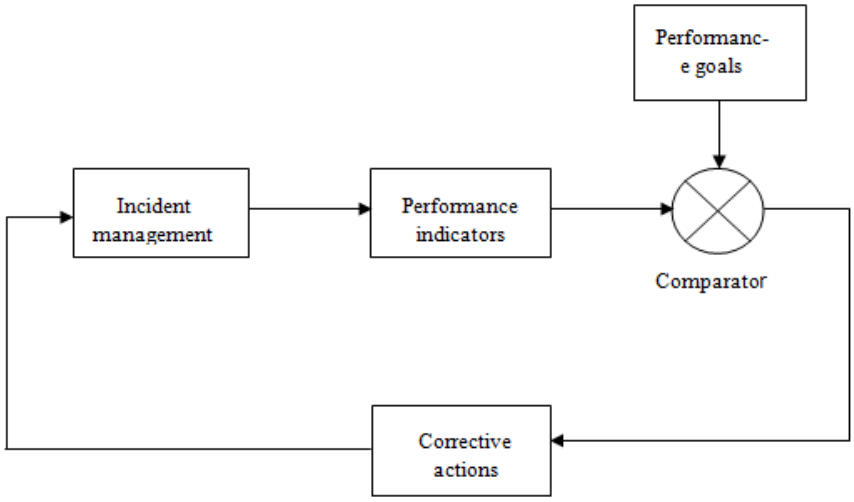

Figure 2.2: Indicators used as monitoring tool [1]

plemented or set performance goals of the system or organization. After then necessary corrective actions can be taken if there is any deviation [1]. The indicators used in this controlled loop can be viewed as a leading indicator. The performance indicator used here analyses and notifies that system's implemented control mechanism is ineffective and needs to be corrected. The behaviour of indicator is outcome based and predictive.

Jose et al. [6] identified 12 sets of Critical Success Factors (CSFs) for effective information security management. He divided all 12 sets of CSFs among three component. He argued that these 12 sets of CSFs are most demanded by information security technology, processes and people. These CFSs, as shown in table 2.2 are also essential to improve the organization's critical asset protection [6]. He identified total 76 sets of indicators for all 12 sets of CSFs. He also argued that these indicators are easy to calculate and provide valuable informations to the organization. Though the identified indicators seem easy to understand and use, the number of indicators seems too many and it might not be feasible to use and manage all of those by an organization.

2.2 The relevance of safety indicators to security

Systems have certain qualities called as attributes of the system. Those attributes of the system need to be measured qualitatively or quantitatively to find the overall performance of the system. Those attributes are also called as dependability attributes as availability, reliability, safety, integrity and main-

Component	CSFs
Technical	IS Security Architecture
	Business Connections
Formal	IS Security Strategy
	Dynamic Evaluation of Infosec Effectiveness
	Risk Assessment
	Infosec Integration
	Law Enforcement and Compliance
	Project Accomplishment
	Security Budget
Informal	Infosec Awareness
	Management Commitment
	Staff Competence

Table 2.2: Identified Infosec CSFs [6]

tainability. Fig 2.3 shows that dependable system consists of attributes of the security without considering confidentiality but it can be said that security is also the one of the attribute of the dependable system. All of those attributes have also dependencies on each other. When we think about the safety and security, they have also dependencies on each other. For example, when the system has been infected by the number of infected viruses, system becomes unreliable and unsafe as well. Safe systems are those generally being available and reliable. When there is risk in the system, it could be made sure that system's safety has been compromised. Safety can be defined as absence of risk in the system that potentially can harm. Risks are those which lead to the adverse impact upon operation of system due to compromise of CIA which are the attributes of security. So, it is fair enough to say that security is essential for safety. Oxford dictionary[4] defines safety as "the condition of being protected from or unlikely to cause danger, risk, or injury" and security as "the state of being free from danger or threat". It shows that the primary definitions of the both terms are similar and weakness in security creates increased risk resulting decrease in safety. So, safety and security are directly proportional, but both are inversely proportional to risk [34].

The life cycle model of both security and safety starts from initial identification and assessment of risk. It provides likelihood of an occurrence of an incident and its consequences. It is hard to estimate the likelihood of occurrence of an

[4]http://oxforddictionaries.com/

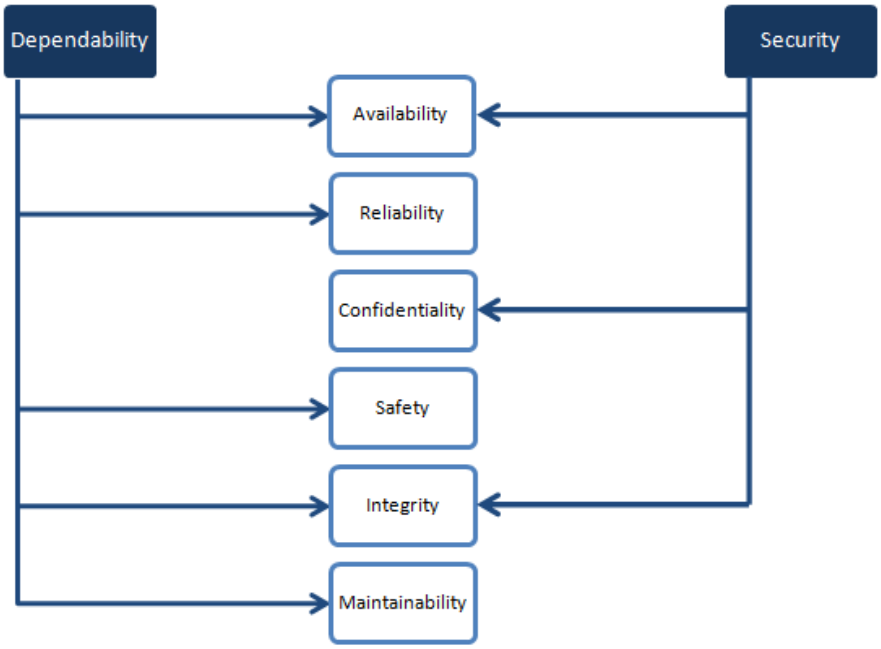

Figure 2.3: Relationship between Dependability and security

incident especially in security system as it depends on the skill and determination of an attacker [34]. This suggests that security incidents occur due to planned actions where as safety incidents are accidental. There exits threat in both safety and security but its nature is somehow different. The threats are not always observable and approximate in the security whereas in the safety those can be observed and are proximal. Here, we mean by 'security' is 'information security'. Though the methodology of both obtaining safety and security are same, the contents are different. Content refers to systems, processes and way of performing and following the methodology. In information security, we are protecting information and organizational assets, and in safety, we are protecting environment, human lives, health and whole physical system which gives clear idea that though the methodology are same, the way of executing the methodology is different. But, some systems require security as well as safety, for example, Supervisory Control and Data Acquisition (SCADA) system in chemical industry might require safety as its reliability and operational hazards needs to be maintained as well as security as attacker can hack it to get data through network.

2.3 Security Incident Management and Indicators

This thesis is extension of the project titled 'Metrics for Information Security - Incident Response', done in the previous semester [35]. The project presented the state of the art of information security measurement, metrics and indicators. It also included the discussion and analysis of some of important incident management metrics and indicators that were already developed by some of research organizations like CIS, NIST in their papers 'The CIS Security Metrics' [18] and 'Performance Measurement Guide for Information Security' [13] respectively.

Chapter 3

Method for Incident Management Indicators Development

This chapter presents the processes involved in developing as well as implementing the incident management indicators. The main objective of developing incident management indicator is to monitor performance of an organization regarding its plans, policies, procedures, incident management capability, system and security practices to protect and respond against malicious incidents. The performance monitoring insures either an organization is meeting its security goals or not. Based on the results, required corrective actions could be identified and implemented to assure its security objectives. The following section describes the six steps to develop and implement the incident management indicators. Though the scope of this thesis is limited to indicators development, this section also presents steps in implementation methodology combined with indicators development methods with their short description. After that, the methodology to adapt safety indicators to the security indicators are presented and described based on the general methodology. This is also the methodology of this thesis. The general step by step methods presented here for incident management indicators development are inspired from papers by OECD [24] and HSE [31] on safety indicator development.

3.1 Security Performance Indicator Development Steps

The following steps are for development as well as implementation of the security incident management indicators.

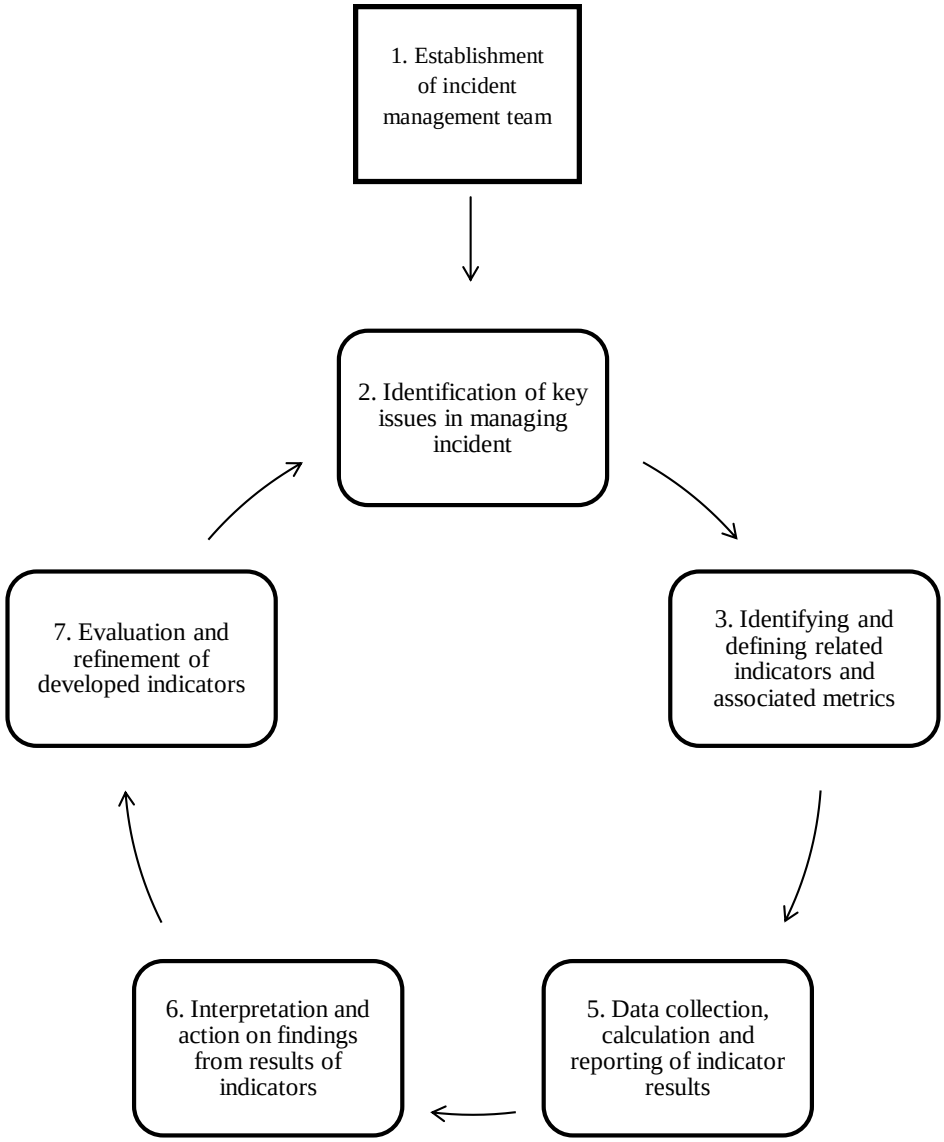

Figure 3.1: Indicators Development Process

1. **Establishment of incident management team**

   Now a days in an organization, the establishment of the security incident response team has been in practice to facilitate protection and responding against different kinds of security incidents. It is also required to establish the incident management team that specifically works in the performance indicators development and implementation. So, the first step involves establishment of the security incident management team whose one of the task is indicator development and implementation.

   The team will be effective if the people from different department and areas are involved like management department, Information Technology (IT) department (Computer Security Incident Response Team (CSIRT), IT staff). While developing the security indicators programmes, it is important to have team with knowledge regarding the organizational plans, policies, goals and objectives, information security goals and objectives, security incident and its management, critical information system and resources. It is only possible through the involvement of people in a team from different department. As a first work of a team, they should really understand what they are going to do and how. This needs planning, preparation and study within the areas and also, setting time table and allocation of budget [25]. Establishing the separate incident management team might be infeasible for small organizations where different roles are handled by the single person. The resources and budget might not be enough to establish the team in small scale organizations.

2. **Identification of key issues in managing incident**

   The next step that has to be performed by the team is to identify the issues in the area of security incident management. Issues[1] are the plans, procedures and security practices that are necessary to prevent, protect and respond against security incidents. As defined by standards and research papers like NIST [7], SysAdmin, Audit, Network, Security (SANS) [36], ISO [4], the incident management involves different phases and different security practices in each phases.

   This paper has defined the incident management phases in chapter 4. It also includes the issues in each phases and their descriptions that are

[1] In the safety area, the word 'issue' is defined as subjects to be addressed or actions that manages the risks, hazards, failure, operation. For example risk identification, system knowledge could be issues for managing risks. In the security area, the word 'security practices' have been used for same purpose as issues have been used in the safety field. So, in the rest part of thesis, the word 'issue' has been used explicitly that beholds same meaning as security practices.

necessary to handle an incident. This step is not only about identifying the issues but it is also about identifying issues which are of great importance. It also focuses on prioritising them based on their impacts on the managing incidents. The issues which might affect the incident management process greatly should be taken into consideration first. It will also significant to have discussion regarding what to monitor rather than how to monitor [30].

3. **Identifying and defining related indicators and associated metrics**

   Identifying and defining indicators depend upon the identified important issues in the previous step. For each issues of concern, lagging indicators as well as leading indicators are identified and defined. The two indicators could be identified and defined by combining. The description of both indicators are presented in chapter 2. Leading indicators predict outcomes which are measured by lagging indicators. So, the leading indicators might become useful in providing reason to the results of the lagging indicators. The combination of the two indicators increases the credibility of the monitoring incident response management as well as increases understanding of how it functions [1]. It also makes easier to insight into organizational plans, policies and security practices.

   The selection of the best indicator always depends on selection of the best metrics firstly as metric is system of measurement that provides data for the security performance indicators. OECD [25] has also defined that metric defines how the indicator is being measured and is the way in which data is collected and reported for an indicator. Choosing best metric always depends upon the indicator subject that is being measured. After then suitable data types and its collection methods, metric categories, must be selected. Analysing historical data is also important for indicator selection.

4. **Data collection and calculation of indicator results**

   After defining the lagging as well as leading indicators, the next step will be data collection and the calculation based on the data. The method and approach for the data collection should be chosen appropriately according to the defined indicators. Based on the collected data, result should be calculated and documented. The calculation and documentation should be repeated regularly in predefined interval to track down the changes. Historical data might also be used for benchmarking.

5. **Interpretation and action on findings from results of indicators**

The documented indicator results might be interpreted that will notify the deviation in results. It confirms that necessary action should be taken to correct that result. So, necessary actions must be taken in time. It should be maintained that, for each issues, the result for both lagging as well as leading indicators must be suitable and satisfactory otherwise necessary amendment should be made.

6. **Evaluation and refinement of developed indicators**

   The developed indicators must be evaluated and refined. There might be some indicators and measurements that are not contributing to the organization. Those should be refined. The evaluation is based on periodic review and update of the results shown by indicators, and their effects upon the organizational security goals.

3.2 Adapting Safety indicators as Security indicators

As discussed in chapter 2, much of research has been performed on safety performance indicators. Consequently there have been development of large number of safety performance indicators. We have adopted following process to adapt the safety indicators to the field of security incident management. The process is also somehow based on the incident management indicator development steps as described above in section 3.1.

1. **Review of issues of security incident management**

   This step involves the identification of different security issues that are vital to each phase of security incident management. These issues are identified through review of standards, research papers and general knowledge. It does not include the development of new issues but existing issues are presented. The description of activities and processes under each issues are also presented.

2. **Review of issues in the safety field**

   After reviewing and presenting the security issues in each phase, the safety issues are identified through literature review of standards and papers related to safety performance indicators. All the identified safety issues are checked with its significance in each phases of the security incident management.

3. **Selection of relevant issues from safety to security**

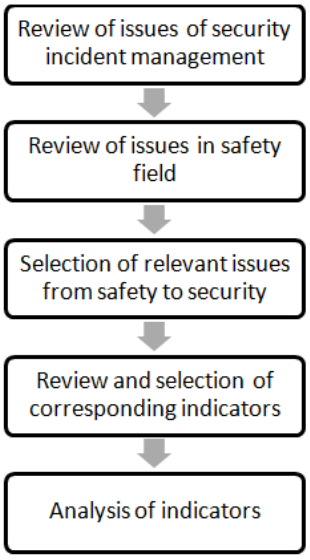

Figure 3.2: Process for adapting safety indicators as security

The relevancy checking and comparison of all of identified safety issues with the identified and described security issues is performed in each phase of incident management. The relevancy checking is based on the common understanding and knowledge on whether safety issues can be adapted and have significance in information security incident management. After then it involves selection of relevant set of safety issues that can be adapted to the security incident management.

4. **Review and selection of corresponding indicators**

   This step involves the review of corresponding indicators of selected issues of previous step. It includes the high level analysis of the indicators for their selection and reuse in the information security field. This analysis is based on understanding and significance of indicators in each phases of security incident management. The questions related to security practices of each phases (presented as a table in each phases) have also provided baseline for indicator analysis.

   After then manageable set of indicators are selected to reuse in the security incident management. The attached table in appendix A shows list of selected issues and indicators in each phase of security incident management.

5. **Analysis of indicators**

The selected indicators are now analysed in a detail in information security field. The detail analysis of the indicators are also based on some attributes. The attributes are taken from different standards [13, 14], research papers [21, 37, 11], knowledge and experience. The selected indicators are judged on basis of values of attributes. The following are the attributes with their description:

a) Definable

This attribute denotes whether an indicator is clearly explainable. This is used to identify the nature and qualities of an indicator. 'High', 'Medium' and 'Low' values have been used here respectively for 'clearly definable', 'somehow definable' and 'hardly definable' respectively.

b) Availability

This attribute denotes whether the measurement data are easily available and accessible. 'High', 'Medium' and 'Low' are used here to define availability of data of different indicators. 'High', 'Medium' and 'Low' are for data are 'highly available', 'somehow available' and 'rarely available' respectively.

c) Relevance

This attribute denotes whether selected indicators are suitable and appropriate for the field of study. It also provides an information if indicator measures the aspect of the selected system and if it is significant to the system. 'High', 'Medium' and 'Low' are used here to show the relevancy of indicators in security incident management. 'High' is for relevant, 'Medium' is for somehow relevant and 'Low' is for not so relevant

d) Objective and reliable

It assesses reliability of data and decision making. Since it needs implementation of indicators, it is not considered here.

e) Cost effectiveness

It shows if the measurement data can be easily collected without bearing too much of cost. 'High', 'Medium' and 'Low' are used for high cost, medium cost and low cost required for data collection respectively.

f) Interpretability

This provides if the indicators are clear and can be easily understood and use. 'Easy' and 'Difficult' are used here for representing 'highly interpretable' and 'hardly interpretable' respectively.

g) Comparable

   This assesses if the indicators can be compared with past values as well as with the performance goals. This also requires real data and implementation of indicators for assessment.

h) Effectiveness

   It assesses if the indicators measure the exact point of corresponding security issues. 'High', 'Medium' and 'Low' are used to show 'highly effective', 'somehow effective' and 'rarely effective' respectively

The attributes values described above are assigned to the indicators based on general knowledge on specific topic.

Chapter 4

Security Indicators Development and Assessment

Security incident management is about preparing, protecting, detecting, responding and sustaining against security incidents. Sometime the ineffective and insufficient implemented security controls provides an ample of opportunities to the attackers to initiate attack vectors and to get into the system. The weak security control causes the increase in volumes of incidents. This leads to the disruption of secure information, property, data and system itself. Thus, there must be systematic approach to prevent the occurrence of security incidents. Both qualitative and quantitative mechanisms should be in place to detect and respond even though incidents occur. Based on the guidelines from the NIST [7] and ISO [4], the four functions are selected for overall incident management (response) as shown in the figure 4.1.

In the following section, description of the four phases of incident management and the related indicators in each phases are presented. The indicators presented that are adapted from the safety field according to the described general process in chapter 3 section 3.2. Each of the indicators correspond to suitable phases where they are described and analysed in a detail. The table specifying the short details of indicators, their attributes and values, and sources of data are also presented.

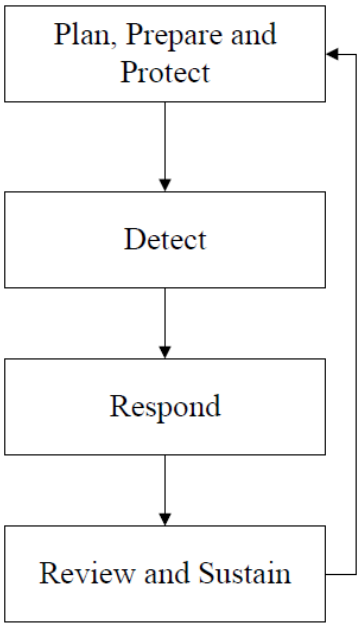

Figure 4.1: Incident Management functions and Process

4.1 Plan, Prepare and Protect

The main aim of incident management is to prevent the occurrence of security incidents. To prevent the incident, the plan and preparations are necessary. This phase focuses on stopping the potential exploitation of the critical security resources. It is possible only through performing the assessments like risk assessments, vulnerability assessments that helps in identifying the level of risk, vulnerabilities, threats of the system. Similarly, strengthening the overall system security through secure host and network configuration, antimalware software installation, personnel support and training are done in this phase. The best security practices can then be helpful for ensuring the security of designed and implemented system. The following are the essential security practices to ensure the protection against the incidents.

1. Risk assessments and awareness

   Risk assessment is means of identifying the security weaknesses and problems in organization's security infrastructure. It is also proactive way of protecting the system against incidents. It provides quantitative or qualitative value to risks. These values are necessary to understand, prioritize, mitigate security risk in a proper way. The awareness about threats and vulnerabilities also helps in predicting the nature of incidents. Periodic risk

assessments are helpful in understanding and determining system specific threats and vulnerabilities [7] and development of the security specification and requirements for a system.

2. Personal awareness and trainings

   The understanding of organization's security plans, policies and procedures, critical assets, system and data is necessary for every personnel working in an organization. It can only be possible through personal awareness and trainings. Every personnel should be aware and trained of the network components and its use, configuration information, software information, operating system. The knowledge sharing of previous incident experience among the personnels also adds to gain awareness so as to control frequency of incident occurrence [7].

3. System security

   This involves the securing of the host as well as the network. Network security is maintained through proper network configuration and management, use of secure communication channel as well as connection points. Host also should be configured in a standard way like proper file permission configuration, password management configuration, firewall configuration and proper handling of privileges.

4. Vulnerability assessments

   These are necessary to find out the vulnerability in the system which might be exploited by the attacker to get into the system. Vulnerability in the system could be identified using the vulnerability scanning tool. The process involved in the vulnerability assessment is somehow similar with the risk assessment. This process not only identifies vulnerabilities but also quantifies and prioritizes them.

5. Control system update

   New threats are evolving day by day. System and its constituents need to be updated in a regular interval to prevent and minimize the impact of those risks and threats. Control system update involves updating of tools like Intrusion Detection and Prevention Systems (IDPSs) and antivirus software, installation of patches for vulnerable software, necessary amendment in firewall and network devices to prevent new malicious code from entering the system.

6. System evaluation

SECURITY PRACTICES	QUESTIONS
Risk Assessments and awareness	• Are Risk Assessments performed on systems regularly? • Are corrective actions taken when problems are identified by Risk Assessment activities?
Personal awareness and trainings	• Are personals aware of critical systems, data, and information? • Is necessary guidance provided to personal for protecting their systems, information and data? • Are security education, training, and awareness provided to the users?
vulnerability assessments	• Is proactive vulnerability scanning performed on networks and system's infrastructure? • Are corrective actions taken when problems are identified by proactive vulnerability scanning?
System security and protection	• Are network and host perimeters configured securely? • Is there use of standard antivirus and malware protection software?
Control system update	• Is there regular update of IDPS, other control systems and software?
System evaluation	• Are regular evaluations performed based on different assessments? • Is there implementation of infrastructure improvements based on previous results?

Table 4.1: Some questions for indicators development

The system is evaluated based on the result of different assessments like vulnerability assessments, risk assessments. As result of system evaluation, the better decision making regarding changes to system to cope up with the new threats could be possible. System evaluation also serves as a basis for assessing the security controls implemented in the system.

Different questions regarding above security practices might provide some benefit to develop indicators in this phase. The table 4.1 presents corresponding questions related to security practices listed above [38].

For the indicator development in this phase three papers [33, 25, 30] related to safety performance indicators are selected. The review of papers and the reason behind how they are relevant for adapting in this phase of the incident management are discussed in chapter 2.

With continuous literature review and relevancy checking of issues regarding safety performance indicators from papers [33, 25, 30], the following sets of the issues are considered to be adapted in this phase of the security incident management. It is felt that the following sets of issues might contribute greatly for plan, prepare and prevention of security incidents and development of the

related indicators in the same field. The table 4.2 shows the selected issues with their description.

Selected Issues	Description
Risk understanding and identification	It is way of gaining knowledge about risk through courses, information and analysis which might provide information regarding the critical security systems and possibility of their exploitation.
Learn from experiences	Sharing and learning own and other's experience regarding the incidents might help in preventing the repetition of occurrence of incidents as most of the security incidents are repeating time to time.
Emergency preparedness planning	The emergency planning based on identification of possible incident scenarios with internal resources and manpower is necessary. Sometime it might be necessary to take help from external authorities and resources when internal resources are inadequate.
Personal training and education	The training and education regarding the possible threats, dealing with possible incidents, proper use of system resources, securing of network and application affects greatly on incident prevention.
Internal and external communication	Communication serves as basis for providing awareness and respond to the given situation. Internal communication in all levels of organization regarding potential incidents, risk, threats and vulnerability in the system is necessary. External communications among organizations, concerned authorities like Internet Service Providers (ISPs), external incident response team are also meaningful.
Adequate resource allocation	Adequate numbers of security personnel, incident response teams as well as sufficient amount of security system resources and back up team in case of unavailability are needed.
Security Process disturbances control	It is always necessary to look thoroughly and pay attention to any security process disturbances like signals from detection systems, changes in log files of host or server, entering of unknown packets through network, changes in traffic flow. Those signals should be acknowledged in time.
Timely procedure and updating of information and system	Nature of threats are changing day by day, it is also needed to update and change the system infrastructure like IDPSs, antimalware software, application software. Information and its procedure also should be updated to all levels of organization.

Table 4.2: Selected issues for development of indicators in plan, prepare and protect phase

After the selection of relevant issues, the high level analysis of the corresponding indicators from the papers [33, 25] is done. The following sets of indicators

are selected to be adopted in this phase of information security incident management.

- Risk understanding and identification

1. **Number of incidents related to unforeseen risks**

   Incidents are likely to occur when there is presence of risk in the system. Risks in the system are identified and mitigated through the risk assessment. It leads to reduction in likelihood of the occurrence of security incidents. In critical system, there might be some risks which are not identified and mitigated through the assessment. When risks are not identified and mitigated, likelihood of occurrence of incidents and its impact increases. This indicator indicates the capacity of organization and security team to identify new risks. It is easier to get number about the occurred incidents related to seen risks but it might be difficult for unforeseen risks. This indicator also indicates the level of risk control system implemented in an organization. It might lead to the organization to have strong risk control mechanism. When the number of security incidents due to unforeseen risk increases, rather than ignoring those risks, team should motivate themselves to identify and mitigate those previously unforeseen risks. Though this indicator is highly relevant to this field and also highly effective, but the data for this indicator might be hard to gather as identifying unforeseen risk is difficult.

Indicator name:	Number of incidents related to unforeseen risks					
Definition:	This indicator indicates the capacity of organization and security team to identify new risks and also indicates the level of risk control system implemented in an organization					
Data source:	Incident Reports, Risk Assessments Reports, Incident Analysis Reports					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Medium	High	Medium	Easy	High

Table 4.3: Indicator Specification: Number of incidents related to unforeseen risks

2. **Fraction of operational procedure that have been risk assessed**

   It is always necessary to have each operational procedure of an organization to be assessed for risk. The security attackers are always looking for some loopholes in the system operation. When each system operations are risk assessed, there is less chance of finding loopholes for the attackers. This means less likelihood of occurrence of security events like denial of service attacks, malicious code. This indicator indicates the status of the system operational procedure i.e. whether the system operations are secure or not. This indicator is highly effective and clearly definable. It measures the exact point of general issue i.e risk understanding and identification. Data availability is also high as it is easy to put in number of procedure that are not risk assessed and collection cost might be low.‘

Indicator name:	Fraction of operational procedure that have been risk assessed					
Definition:	This indicator indicates the status of the system operational procedure whether they are secured or not.					
Data source:	Risk Assessments Reports					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.4: Indicator Specification: Fraction of operational procedure that have been risk assessed

3. **Portion of staffing and operating personnel taking risk courses last 12 months**

   The risk understanding is based on knowledge and experience on the same field. The staffing and the operating personal must maintain their knowledge and understanding on the risk to prevent the occurrence of incidents. The knowledge regarding new threats and vulnerabilities could be obtained through participating in risk courses. This indicator can be seen as early warning indicator for system monitoring. It indicates the efficiency of personnels based on the risk knowledge which could be first thing for incident prevention. This indicators is highly definable, easy to interprate, highly relevant and effective. Data availability is also high and might require low cost to collect it.

Indicator name:	Portion of staffing and operating personnel taking risk courses last 12 months					
Definition:	It indicates the efficiency of personnel based on the risk knowledge					
Data source:	Risk Training Reports					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.5: Indicator Specification: Portion of staffing and operating personnel taking risk courses last 12 months

4. **No. of violations to authorized entrance of systems**

   The system users, staffs, operating personnel and other people involved in an organization must authorise themselves before entering to the system. There might be chance that some users might have violated the rules, may be due to unawareness and lack of risk understanding. This indicator is measure of user's (staffs, operating personnel) knowledge and understanding on risk and system security, lack of which leads to the severe incidents. More the violations are made, less the people are aware of risk and system security. This is also one of the early warning and important indicator for system monitoring. It might be hard to know who has violated the authorized entrance of system but reviewing system logs might provide some clue. This indicator is highly relevant, effective and clearly explainable but, data availability might not be high.

Indicator name:	No. of violations to authorized entrance of systems					
Definition:	This indicator is measure of user's (staffs, operating personnel) knowledge and understanding on risk and system security lack of which leads to the severe incidents.					
Data source:	System Logs					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Medium	High	Low	Easy	High

Table 4.6: Indicator Specification: No. of violations to authorized entrance of systems

- Emergency preparedness planning

1. **Number of elements in the plan which work correctly when tested**

   The organization must be prepared for what to do in the emergency case. For example, some incidents like denial of service attack can compromise a system within a short time. There must be prepared plan for a such case. The emergency plan is related to the whole incident management like protection, prevention, detection, reporting, containment, elimination and recovery from malicious incidents. This indicator measures the effectiveness of emergency incident response plan. When the prepared plan is tested and process is working, it shows its effectiveness and increase in value represents increase in its efficiency. This indicator is highly effective as it measures exact issue of concern but it might not be so easy to collect data. This indicator is clearly definable and also very easy to interprate.

Indicator name:	Number of elements in the plan which work correctly when tested					
Definition:	This indicator measures the effectiveness of emergency incident response plan.					
Data source:	Test Reports					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Medium	High	Low	Easy	High

Table 4.7: Indicator Specification: Number of elements in the plan which work correctly when tested

2. **Increase in number of incidents with effective emergency plan in place**

   This indicator also measures the efficiency of the adopted emergency plan. Incidents might occur despite of emergency planning and preparedness. This might be because of the absolute nature of the information security and changing nature of the attack vectors. Despite of that, increase in incidents even after implementing emergency plan shows the ineffectiveness of that plan. It suggests that improvement should be made to existing plan in place. This indicator is highly relevant, clearly explainable and highly effective. Though data can be easily available, it might cost more to collect those data.

Indicator name:	Increase in number of incidents with effective emergency plan in place					
Definition:	This indicator measures the efficiency of the adopted emergency plan					
Data source:	Emergency Plan Reports, IDPSs Logs, Network Device Logs					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	High	High	Medium	Easy	High

Table 4.8: Indicator Specification: Increase in number of incidents with effective emergency plan in place

- Personnel training and education

1. **No of emergency preparedness exercise last three months**

   The one way of enhancing knowledge and education regarding security incidents, security system resources, threats and vulnerabilities is through training and exercises. More training and exercises are always beneficial to understand the processes. This indicator is measure of the capability of concerned people (staff, security response team, IT officers) working in an organization to manage the incidents. The increase in value of this indicator shows the increase in competencies of the personnel to manage incidents. The data for this indicator might be easy to get as there might be availability of report of emergency exercises conducted. This indicator is clearly definable and highly effective as it directly affects the corresponding issue of concern which is personal training and education in this case.

Indicator name:	No. of emergency preparedness exercise last three months					
Definition:	This indicator is measure of the capability of concerned personnel working in an organization regarding incident management					
Data source:	Emergency Plan Reports					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	High	Medium	Low	Easy	High

Table 4.9: Indicator Specification: No of emergency preparedness exercise last three months

2. **No. of different incident scenarios included in exercises last month**

   Information security incidents exist in different forms like denial of service, unauthorized access, malicious code, inappropriate usage, information gathering to identify potential targets [4]. Exercise regarding management of different types of incidents and scenarios always help in enhancing the personal competencies and experience. It helps in building up knowledge and confidence for concerned personal to deal with security incidents (in case of sudden security attacks). This indicator is measure of the effectiveness and competencies of people working in an organization regarding their knowledge and experience in managing different kinds of information security incidents. This also shows the capacity of an organization to deal with different kinds of incidents. This indicator is highly effective indicator as it measures exact point of issue which is personal education and

training. It is also highly relevant to the field of incident management and interpretable as well. The data sources could be training reports, emergency planning reports which are easily available, and also are less costly to collect it.

Indicator name:	**No. of different incident scenarios included in exercises last month**					
Definition:	This indicator is measure of the effectiveness and competencies of people working in an organization regarding their knowledge and experience in managing different kinds of information security incidents					
Data source:	Training Reports, Emergency Planning Reports					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.10: Indicator Specification: No. of different incident scenarios included in exercises last month

3. **No. of security proposals per employee**

   Security proposals by concerned people in an organization also reflect the competencies of each person. Security proposals here mean the report (proposal) prepared by each concerned people to prevent, detect and respond against information security incidents. This indicator is a measure of skill and competency of concerned person working in an organization. The different ideas regarding incident management will always be beneficial to an organization and can be applied in real case scenarios. The increase in proposals per person shows increase in efficiency of manpower as well as incident handling

capability of an organization. This is highly relevant and effective indicator. It requires less cost to collect data as they are easily available too. It is clearly explainable and interpretable.

Indicator name:	No. of security proposals per employee					
Definition:	This indicator is a measure of skill and competency of concerned person working in an organization.					
Data source:	Training Reports, Emergency Planning Reports, Employee Records					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.11: Indicator Specification: No. of security proposals per employee

- Internal and external communication

1. **No. of risk issues communicated to the entire organization each month**

   This indicator measures the effectiveness of the internal communication of an organization. The identification of risks only would not help to prevent the incidents, it should also be communicated to entire departments and people in an organization so that they can look for their mitigation and be prepared to handle them. Most of the incidents are also occurring due to lack of communication among people and different departments in an organization. Risk can be identified only after identification of threat and vulnerability of the system [39]. Those things need to be communicated to protect against security at-

tacks. More the risks are communicated, better will be the security posture of an organization. This indicator is highly effective as it measures exact point of issue i.e. internal and external communication. The data can be collected by interviews and surveys but it might cost more to collect them. It is highly relevant, definable and interpretable.

Indicator name:	No. of risk issues communicated to the entire organization each month					
Definition:	This indicator measures the effectiveness of the internal communication of an organization.					
Data source:	Interview, Survey					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Low	High	High	Easy	High

Table 4.12: Indicator Specification: No. of risk issues communicated to the entire organization each month

2. **No. of cases in which communication among personals have been inadequate**
   The inadequacy in communication among employee regarding threats, vulnerabilities, critical system resources and data, security incidents, organization's security plans, policies and procedures, might affect the organization in great deal. The open and direct communication should be one of the vision of an organization when it comes to securing against various security attacks. Communication could be in forms of reporting, email, information broadcasting, notices, telephony, meetings and conferences. Though it is hard to figure out that

current increase in security incidents (cases of security incidents) is due to lack of communication, timely (weekly or monthly) surveys and interview could be helpful to find the causes. This indicator also measures the efficiency as well as adequacy of implemented communication mechanism in an organization to spread critical information. This indicator is effective and highly definable but it might be hard to collect data and also costs more.

Indicator name:	**No. of cases in which communication among personals have been inadequate**					
Definition:	This indicator measures the efficiency as well as adequacy of implemented communication mechanism in an organization to spread critical information.					
Data source:	Interview, Survey					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Low	High	High	Easy	High

Table 4.13: Indicator Specification: No. of cases in which communication among personals have been inadequate

- Security process disturbances control

1. **Average no. of persons monitoring the security control system continuously**

   Detection systems like IDPSs are monitoring and looking for the malicious activities in the network or system. If malicious activities are found, it will signal warning message to the concerned station (people). The concerned station should react to the signal as soon as

possible. They should also analyse the traffic pattern to find out the abnormal behaviour. This indicator indicates if there are availability of enough people to respond to the warning by the monitoring system and measures effectiveness of organizations staffing policy. Unavailability of people for monitoring the security process disturbances might lead to serious damage to system data later on. Data for this indicator are easy to collect and requires less cost to collect as they are easily available on staffing plan report.

Indicator name:	**Average no. of persons monitoring the security control system continuously**					
Definition:	This indicator measures the effectiveness of staffing plan allocated for monitoring the security system					
Data source:	Staffing Plan Report					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Easy	Medium

Table 4.14: Indicator Specification: Average no. of persons monitoring the security control system continuously

2. **No. of alarms not acknowledged during last month**

   Alarm here is the signal that is generated by the detection and monitoring system to inform the malicious activities in the system. The acknowledge to an alarm is done by the people monitoring the those systems. Lack of acknowledgement implies that there might be unavailability of the person or people are not aware of the alarm. This in-

dicator indicates the efficiency and adequacy of the authorised people (monitoring the detection system) in an organization. The increase in number of unacknowledged signals from detection system implies inefficiency of the responsible people. It might be hard to collect data for this indicator. Logs of IDPSs, Security Information and Event Management (SIEM) might provide some data for this indicator calculation, though Care should be also taken for identifying the false positive alarms.

Indicator name:	**No. of alarms not acknowledged during last month**					
Definition:	This indicator indicates the efficiency and adequacy of the authorized people (monitoring the detection system) in an organization					
Data source:	IDPSs, SIEMs					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Low	High	Low	Easy	Medium

Table 4.15: Indicator Specification: No. of alarms not acknowledged during last month

- Adequate resource allocation

  1. **No. of cases in which resources/staffing have been inadequate last three months**

     The resource allocation and number staffing in an organization depends upon the size and reputation of the organization. Organizations having good status and reputation among the customers as well as

those having high financial value are on the eyes of security attackers. Enough system resources and staffing should be allocated to prevent the security incidents in those organizations. The inadequacy of system resources like IDPSs, SIEM, network devices, antimalware software and staffing to monitor as well as handle the security incidents leads to increase in security incidents. It leads to disruption of critical resources as well as company value. This indicator measures the adequacy of the resources and staffing in an organization. It might be hard to determine increase in number of cases of incidents due to inadequate resources. The analysis of incident nature, time and date might provide some data to validate it. The incident analysis report, incident reporting form might provide some data for this indicator. But, generally it might be difficult and costly to collect exact data for this indicator.

Indicator name:	**No. of cases in which resources/staffing have been inadequate last three months**					
Definition:	This indicator measures the adequacy of the resources and staffing in an organization					
Data source:	Incident Analysis Report					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Low	High	High	Easy	High

Table 4.16: Indicator Specification: No. of cases in which resources/staffing have been inadequate last three months

2. **No. of cases in which response has been initiated too late last**

three months

The response time to an incident should be as minimum as possible to protect the damage of critical system data and organization value. The late initiation of response to an incident indicates that there might be inadequate number of staffs like incident response team, information security officer and other concerned people. This indicator is an lagging indicator measuring the effectiveness of resource (staffing) allocation plan of an organization. Though it is effective indicator but, data availability is medium. Some sources of data could be incident analysis report, incident reporting form.

Indicator name:	No. of cases in which response has been initiated too late last three months					
Definition:	This indicator indicates that there might be inadequate number of staffs like incident response team, information security officer and other concerned people to respond to an incident					
Data source:	Incident Analysis Report, Incident Reporting Form					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Medium	High	Medium	Easy	High

Table 4.17: Indicator Specification: No. of cases in which response has been initiated too late last three months

- Timely procedure and updating of information and system

  1. (on hold)[1]

[1] 'on hold' represents there are no specific indicators under this category in the safety papers.

- Learn from experience

    1. (on hold)

4.2 Detect

Incident detection phase is the primary as well as the most difficult phase of security incident management. Intrusion detecting systems, antivirus mechanisms, antispyware, network and traffic analysis systems, deep packet inspection, anomaly detection systems, are used to detect an incident now days. In fact, it has been hard to accurately detect an incident because detectors may give the false negative detection of incidents. Though there are many indicators that can notify the incidents that may have occurred or may be occurring, the incident precursors are rare which will notify the occurrence of the indicators in the future. Obtaining information about incidents, vulnerabilities and other information related to the potential incidents requires monitoring of the system and network. The monitoring of the system and network to detect the incident can be done in two ways.

1. Reactive monitoring

    This monitoring includes notification of spreading of incidents like malware, viruses, worms from different internal and external sources and parties. The reporting of the malicious activities within the system's infrastructure to the designated authorities like CSIRT is also a part of reactive monitoring. It is based on monitoring of the system after occurrence of an incident. The knowledge about the incidents can be gathered from external and internal sources, publicly available information regarding new alerts, viruses, worms and vulnerabilities.

2. Proactive monitoring

    It is way of detecting incidents that are likely to occur. It is done to find the malicious activities going on on the system and network by reviewing the logs of network devices, by analysing the the flow of traffic. Every business organization has unique network traffic pattern under normal operation. The understanding of the traffic pattern under normal operation leads

Though issue, timely procedure and updating of information and system, is highly relevant to security. So, it has been adopted from safety papers. The description of this issue can be found in table 4.2

to detect the pattern beyond normal condition. It could be an early indicator of security attack. The content of the different sources IDPSs, SIEM, antimalware and antivirus softwares are important for detecting the potential incidents. Different people are allocated for the proactive monitoring of the security systems like network operator, IT personnel, CSIRT team, IT administrator. It is also important to review and be updated to technology regarding new attacks, worms, vulnerabilities, threats, to correctly analyse and detect the potential incidents.

The other important factors that motivate security attackers to break down an organization are the nature and status of its business activities, and also the position of organization in terms of financial value and reputation. Depending upon the reputation and value of an organization, it might be necessary to lure the potential attackers to identify their attack vectors and methodologies (for early detection). It might be accomplish by using Honeypot [2]. The status of security control system and incident detecting instruments like SIEM, IDPSs, Network devices also directly affects incident detection. It might give false positive detection and sometime no detection as well. The failure and error in those systems might affect the timely and accurate detection of incidents. But, the failure of those devices will lead its analysis to reliability rather than CIA.

The table 4.18 shows the security practices for detection of incidents with their corresponding questions that might help in indicator development for this phase [38].

The systems that are used for detection of incidents in the safety and the security systems are totally different as nature and type of incidents as well as operations are different. The common part is that in both the systems, an incident might occur due to failure of those systems (process disturbances). In case of security, systems like SIEM, IDPSs and network devices are used for incident detection. The failure of those systems could be due to design fault or error or due to attack in those system by security attackers. SANS [18] states, incidents that should not be considered "security incidents" include disruption of service due to equipment failures. So, we are considering the malfunctioning of those systems due to security attack on them. Though security attackers might directly attack the system rather than attacking the detection systems, they might do it to prevent the issuing of warning signal to the management station. Though the issue, security process disturbances and failure from safety papers [33, 31], is

[2]Honeypot is a system which looks and acts like real that is set to trap the security attackers to collect the information regarding their attack vectors and methodologies

Security Practices	Questions
Proactive Monitoring	Are systems and networks monitored proactively at a regular interval?
	Are logs of IDPSs, SIEMs, antivirus, network devices analyzed regularly?
Reactive Monitoring	Is there provision of obtaining report or notification of incidents from external and internal sources?
Information update and awareness	Are all concerned authorities are updated about recent security incidents?

Table 4.18: Security practices in an incident detection and corresponding questions

Selected Issues	Description
Security process disturbances and failure	It states that if there is any failure in the security incidents detecting devices, it might increase the security incident rate. The timely as well as accurate detection of various could be affected. The failure of such devices is due to security attack to malfunction those devices rather than design fault or error. It might somehow be effective to monitor the detection systems and devices not only their logs and flows.

Table 4.19: Selected issues for development of indicators in detect phase

considered to be adapted in the detection phase of incident management. The description of this issue is presented in the table 4.19

After the selection of relevant issues, the high level analysis of the corresponding indicators from the papers [33, 31] is done. The following sets of indicators are selected to be adopted in this phase of the information security incident management.

- Security process disturbances and failure

    1. **Number of security critical instruments and detection systems that fail to operate due to security attacks on them**

       The purpose of attacking detection system is to prevent the relay of signal regarding attack to the monitoring station. It would be benefit to the attacker to stop the relay of signal so that they can penetrate

the system more easily. Some of the attacks like evasion attack and mimicry attack have been identified in host- based as well as network based intrusion detection system [40, 41]. If the detection systems are compromised, the responsible people might not get any warning regarding potential attack and the disruption of the system assets could be severe. This indicator shows the effectiveness of the detection systems. Though it might be difficult to find out reason of failure of those systems, careful monitoring and analysis might help to find out vulnerabilities in those systems which are exploited by the attackers.

Indicator name:	**Number of security critical instruments and detection systems that fail to operate due to security attacks on them**					
Definition:	This indicator measures the effectiveness of detection systems					
Data source:	Detection System Analysis Report, Incident Analysis Report					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	Medium	Low	Medium	Medium	Difficult	Medium

Table 4.20: Indicator Specification: Number of security critical instruments and detection systems that fail to operate due to security attacks on them

2. **Number of incidents due to failure in security critical instruments and detection system**

   Intrusion detection systems might account actions of attackers and also act as a deterrent to future attacks [41]. The number of incidents might increase if detection systems are attacked and malfunctioned.

This indicator can be viewed as measure of efficiency of the intrusion detection system which directly affect the security posture of an organization. Increase in number of security incidents due to detection system failure shows the bad security system of an organisation.

Indicator name:	Number of incidents due to failure in security critical instruments and detection system					
Definition:	This indicator measures the efficiency of the intrusion detection system which might affect the detection capabilities of an organization					
Data source:	Detection System Analysis Report, Incident Analysis Report					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	Medium	Low	Medium	Medium	Difficult	Medium

Table 4.21: Indicator Specification: Number of incidents due to failure in security critical instruments and detection system

4.3 Respond

It is always essential to determine the nature and scope of an incident after it has been detected. In fact determining if an occurrence of event indicated by indicator is an incident, is also hard [7]. It requires technical as well as expert's help. The responding process involves the analysis of the incident to accurately define and find its trend and scope. It also involves the developing plan and strategy to recover from incidents. Varying upon the scale of organizations, responding process are handled either internally or by trusted third party or combination of both internal and external party. First of all, the incidents are reported to the

concerned authorities like CSIRT team, IT security personnel. Then, the analysis is done to find the nature of incidents and then after necessary mitigation and recovery strategies are developed. The responding process also includes the containment of incidents to stop it from damaging other resources and data within a system. It is done by shutting down the system, disabling the network and other functions [7]. The technical as well as management help and cooperation are important for recovery from an incident. The effective coordination and communication of information across all areas is essential for responding to an incident. After successful development of the strategy and its implementation, the malicious vectors causing incidents are eradicated and system is recovered to its normal working state. The following security practices are necessary to respond to an incident.

1. Documentation and reporting

   After detection of an incident, it should be assessed to find out whether it is the security incident or not. The assessment and analysis of the detected incident starts when the incident is documented and reported to the corresponding authorities including incident response team. The timely documentation and reporting of an incident is always encouraged as it affects the overall response process. Every organizations might have their own policies and procedure or guidelines for the documentation and reporting of an incident. They might have standard documenting and reporting form. Standards and research papers [4, 7, 36] also suggest to have predefined guidelines for documenting and reporting of an incident. The standard reporting forms mentioning time and date of detection, nature, possibly type, observer of an incident might help to make timely reporting of an incident. The reporting of the incident could be done through various means like emails, telephone, fax or direct communication. The documented incident should be reported to the concerned authorities like head of department, IT security officer, and possibly to the incident response team.

2. Analysis and validation

   After the reporting of an incident, analysis of incident should be done to validate that it is an incident. The incident analysis is performed by the information security officers and CSIRT. First of all, initial analysis is done to validate an incident. Once the incident is validated, detailed analysis should be done to find the nature, impact and scope of the incident. It might include the forensic investigation, other technical analysis of the attack vectors. It is necessary to do the detailed analysis of the incident as it will

show the what are the assets, system, information and data affected and still affecting by the incident, to what extent it will damage the system, what are the things that needs to be contained to avoid the further disruption. It will not only give information about the incident scope, it will also provide strong basis for developing the plan and strategy to mitigate and recover from that incident. Depending upon the nature and scope of an incident, it is also mandatory to release the alerts, bulletins across the organization to make all the people and staff aware of the situation.

3. Response

   The response process is generally includes containment, eradication and recovery from an incident. The coordination among various parties like management (executive or human resource), technical officers, administrator, legal authorities, public relations, law enforcements, software and hardware product developers, external and internal CSIRT and other security teams inside and outside of an organization, is necessary to eradicate and recover from incident. The first step to response is to contain the incident. It involves the different activities like disconnecting the network, shutting down the system, implementing firewall, changing the security configuration so that the further damage to the system and assets could be stopped. It is done only after finding the scope and impact of an incident. ISO [4] also describes that primary goal of incident management is to minimize the incident impact and identifying attacker is secondary. The eradicating and recovering plans and strategies are then developed based upon previous step's analysis result. It is major duty of CSIRT to develop the recovery plans in collaboration with other parties and people mentioned above. It might be effective to collect information about the attacker and his motive behind the attack as much as possible. It might be achieved by network surveillance [14]. After finding the malicious attack vectors or codes, it should be eradicated. The repairing of the system should be done to recover to normal condition. It might be useful to validate the respond process just to check the condition of security system.

The paper [30] is selected for indicator development in this phase. The literature review of the paper and reason behind its selection to develop security incident management indicator in this phase is presented in chapter 2.

The safety issues presented in the paper [30] regarding the safety incident response might be relevant to security practices in respond phase of security incident management. With continuous literature review and relevancy checking

of issues regarding safety performance indicators from papers [30] in response part, the following sets of the issues are considered to be adapted in this phase of the security incident management. It is felt that the following sets of issues might contribute greatly for respond phase of security incidents and development of the related indicators as well. The table 4.22 shows the selected issues with their description.

Selected Issues	Description
Incident reporting	The incidents and near incidents must be reported to the concerned authorities like information security officer, CSIRT according to organization's policies and rules for that have been set for incident reporting
Investigations	It includes the analysis and investigations of an incident after it has been reported. It requires skills and knowledge, policies and procedures, collaboration with other parties, technical processes. The purpose of an investigation is to find the root cause of an incident and develop plans and strategies for its mitigation

Table 4.22: Selected issues for development of indicators in respond phase

After the selection of relevant issues, the high level analysis of the corresponding indicators from the papers [25] is done. The following sets of indicators are selected to be adopted in this phase of information security incident management.

- Incident reporting

    1. **Extent relevant incidents are reported**

       The reporting of the incidents always play significant role in incident management. Various people and staffs working in an organization could be the source of incident detection. The incidents could not be contained, eradicated and recovered unless it is reported to the concerned authorities. The papers [4, 7, 36] define CSIRT, Information Security Incident Response Team (ISIRT), Security Officer, Point of Contact (PoC) as concerned authorities. Once the incidents are reported to them, they could look for remediation. More the incidents are reported, more timely and quick recovery from incidents could be expected. It means less damage to the system and assets. This indicator indicates how effective is incident reporting system in an organization. This is also an indicator of the personal awareness and

competency regarding the reporting system because people working in an organization might not be aware or trained or informed about the formal incident reporting system of an organization. This indicator also could be used to reflect the overall security posture of an organization. It might be hard to collect the data for this indicator as it might be hard to find out unreported incident. It is highly effective to issue of concern which is incident reporting. Similarly, it is relevant as well as requires less cost to collect the data (if data are available).

Indicator name:	**Extent relevant incidents are reported**					
Definition:	This indicator indicates how effective is incident reporting system in an organization					
Data source:	Incident Documentation Report, Incident Reporting Form					
Attributes	Definable	Availability	Relevance	Cost effectiveness	interpretability	Effectiveness
Value	High	Low	High	Low	Easy	High

Table 4.23: Indicator Specification: Extent relevant incidents are reported

2. **Number of days since last recordable incidents**

   The increase in value of this indicator shows the good security posture of an organization since incidents have not been recorded since long time. It can also be interpreted differently as there might be a case that incidents might not have been detected and reported which is the shows ineffectiveness of detection and reporting system. It indicates decrease in the people's awareness regarding the incident reporting

which might be level of risk in itself. So care should be taken during its interpretation as well as decision making. It might be easy to find data for this indicator if incidents are reported and documented in standard format mentioning their date, nature and other necessary properties. This indicator somehow addresses the issue of concern and is also highly definable and less costly to collect data.

Indicator name:	Number of days since last recordable incidents					
Definition:	This indicator indicates effectiveness of the reporting system as well as effectiveness of the security control system (based on how it is interpreted)					
Data source:	Incident Logs, Incident Reporting Form					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Difficult	Medium

Table 4.24: Indicator Specification: Number of days since last recordable incidents

- Investigations

1. **Extent that incidents are investigated in accordance with established procedure**

   Investigation here means process of eradicating and recovering against incidents. It involves different steps. The investigations procedures might be different for different organizations. The investigation procedures should be according to provided standard. For example, it

would not make sense to start looking for attackers without containing the incident, the impact will be adverse. The established procedures are formal, effective and suitable to the organizations. The investigations might be effective if standard procedure are followed. All the documents can be also easy to track and review later. The investigations procedure also will fast as well as understood by every concerned authorities. It reflects the good policies as well as investigation procedure. The increase in value of this indicator reflects the good incident response policy and capacity which has direct impact on the overall security system. Though it is hard to find data for this indicator, reviewing the procedures, documentation process, result of the investigation might help to find the data. This indicator is highly definable and also somehow corresponds to the issue of concern (i.e.investigations). It not so costly to gather data for this indicator and easily interpretable as well.

Indicator name:	**Extent that incidents are investigated in accordance with established procedure**					
Definition:	This indicator indicates effectiveness of incident response policy and capacity of an organization which has direct impact on the overall security system					
Data source:	Incident Documentations Report, Incident Management Procedure Documentation					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.25: Indicator Specification: Extent that incidents are investigated in accordance with established procedure

1. **Extent of events where the investigators identify root and contributing causes**

   The main purpose of security incident response is to find the root and main cause of the incident and eradicate as well as recover it as soon as possible. The cause might be the vulnerabilities in the system, malicious code, lack of risk assessment of security systems. This indicator indicates the effectiveness of the incident response team and their investigation plans and strategies. More the causes of the incidents are identified, more will the effectiveness of their strategies. This will also help to make corrective action to prevent the occurrence of same incident next time. The indicator data is easy to collect, not so costly and highly relevant to the incident management.

Indicator name:	**Extent of events where the investigators identify root and contributing causes**					
Definition:	This indicator indicates the effectiveness of the incident response team and their investigation plans and strategies					
Data source:	Incident Analysis Report					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.26: Indicator Specification: Extent of events where the investigators identify root and contributing causes

4.4 Review

This is also considered as important phase of security incident management as all the works done in other phases are reviewed and corrective actions are taken to avoid the recurrence of incidents. This phase focuses on the identification and implementation of the strong security system, improving the incident management capability, review of current security plans and policies that fail to operate as intended, revisit to the security goals and objectives, its processes and effectiveness, identifying and updating the information regarding the security incidents, vulnerabilities, threats, risk assessments [4], ensuring the effectiveness of incident response team, infrastructure and guidelines. These processes are based on the current results, documentation, report of the incident management processes. The involvement of senior executive management team, information security team, Incident management team, system administration team, public authorities, law enforcements are expected in this phase. The main aim is to identify the security system weaknesses and implement better security control system. The following are the security practices done in this phase.

1. System evaluation, implementation and management

   The system is evaluated based on the current security incident management processes. All the reports, documentation, records, forms regarding security processes like risk assessments, incident response, vulnerability assessments, incident detection, incident prevention plans and policies are reviewed and weaknesses are identified. It is followed by the correction and implementation of the better system and strategies to overcome those weaknesses. For example, based on the impact of incidents, it might be necessary to review and alter the risk assessment processes so that new vulnerabilities and threats are identified [4]. It also includes evaluation of the staffs and operating personnels based on skills, knowledge and capacity so that changes made in the system processes can be achieved. It also includes the assessment of security control system plans, policies and guidelines. The necessary changes are made after evaluation and implemented. Similarly, the incident data collected during the prevention, detection and response of incidents are analysed and possible metrics and indicators are calculated. It provides ample of opportunities to find the weaknesses in the system and also to measure the capability of the incident response team [7].

For the indicator development in this phase, papers [30, 42] are selected. The literature review of the paper and reason behind its selection to develop security incident management indicator in this phase of incident management is presented in chapter 2.

The safety issues presented in the papers [30, 42] might be relevant to security practices in respond phase of security incident management. With continuous literature review and relevancy checking of issues regarding safety performance indicators from papers [30, 42] in review part, the following sets of the issues are considered to be adapted in this phase of the security incident management. It is felt that the following sets of issues might contribute greatly for this phase of security incidents and development of the related indicators as well. The table 4.27 shows the selected issues with their description.

Selected Issues	**Description**
Follow up, sharing of information and application of lessons learned	This is applied to prevent the occurrence of same incident next time, and also to improve and validate the security system after recovery of an incident . This includes the sharing of the informations, application of corrective actions.
Management systems	It describes how the management systems (information security as well as executive)are involved in reviewing the security incident management processes in an organization. The involvement of the management has direct effect on the incident management

Table 4.27: Selected issues for development of indicators in review phase

- Follow up, sharing of information and application of lessons learned

    1. **Amount of time needed for implementation of recommendations from investigations**
    An investigation is the incident response process which includes analysis of incident to find the root cause of an incident and eradicate it to recover system to normal operation. Investigation might ensure that there are weaknesses in the systems. The result of investigation might provide feedback and suggestions regarding the corrective action that needs to be taken. Once an incident is eradicated and system is recovered to normal operation, the main thing is to do the timely review of the results of investigations and implement it so that recurrence of incident can be prevented. This indicator measures the effectiveness of the overall organizational team to take timely corrective action. The higher value of this indicator reflects poor security

posture as well as ineffectiveness of the review team. If more time is taken to make corrective actions, more will be the chances of incident occurrence and disruption of system assets could be severe. The data for this indicator might somehow be difficult to get. The time between reported investigation suggestions to implementation should be documented.

Indicator name:	**Amount of time needed for implementation of recommendations from investigations**					
Definition:	This indicator measures the effectiveness of the overall organizational team to take timely corrective action					
Data source:	N/A (manually documenting time between)					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	Medium	High	Medium	Easy	High

Table 4.28: Indicator Specification: Amount of time needed for implementation of recommendations from investigations

- Management systems

1. **Number of relevant process/procedures reviewed**
   Incidents might be of different kinds like denial of service, malicious code, unauthorised access. Incident management processes will be different for different types of incidents. During review phase, incident data, report, documented plans and steps, investigation results should be reviewed by management committee. The overall procedures and strategies should also be reviewed. This indicator indicates

the efficiency of the management (review) team to review each processes and procedures in effective manner. The more the processes and procedures are reviewed, the effective will be the security system understanding, and mandatory corrective implementation could be made. The data for this indicator might be easily available from the documented report of the review team. This is effective indicator that correctly measures the point of issue (management system in this case) and requires less cost to collect data.

Indicator name:	**Number of relevant process/procedures reviewed**					
Definition:	This indicator indicates the efficiency of the management (review) team to review each processes and procedures in effective manner					
Data source:	Management(Review) Report					
Attributes	Definable	Availability	Relevance	Cost effectiveness	Interpretability	Effectiveness
Value	High	High	High	Low	Easy	High

Table 4.29: Indicator Specification: Number of relevant process/procedures reviewed

Chapter 5

Discussions and Recommendations

This chapter presents the discussion of incident management indicators that are developed in the previous chapters. The discussion is mainly about the advantages and disadvantages of those indicators. The indicators are also differentiated as leading and lagging indicators. It also includes one scenario that shows how these indicators could be developed and implemented.

5.1 Overview

The following figure 5.1 presents the overview of the developed incident management indicators. There are three levels. First level shows the phases of the incident management. Second Level shows the issues of respective phases that are necessary to perform during each phase of incident management. These are also adopted from the safety part. Third level shows the corresponding indicators that are adopted from the safety indicators. The figure shows that there are all together twenty three indicators have been suitable to use in security incident management. Among twenty three indicators, first fifteen indicators assess the effectiveness of planning, preparation and protection state of incident management. Similarly, next two indicators measure incident detection capabilities, next four indicators measure incident responding capabilities and remaining two measure overall reviewing and decision making capabilities of concerned authorities within an organization.

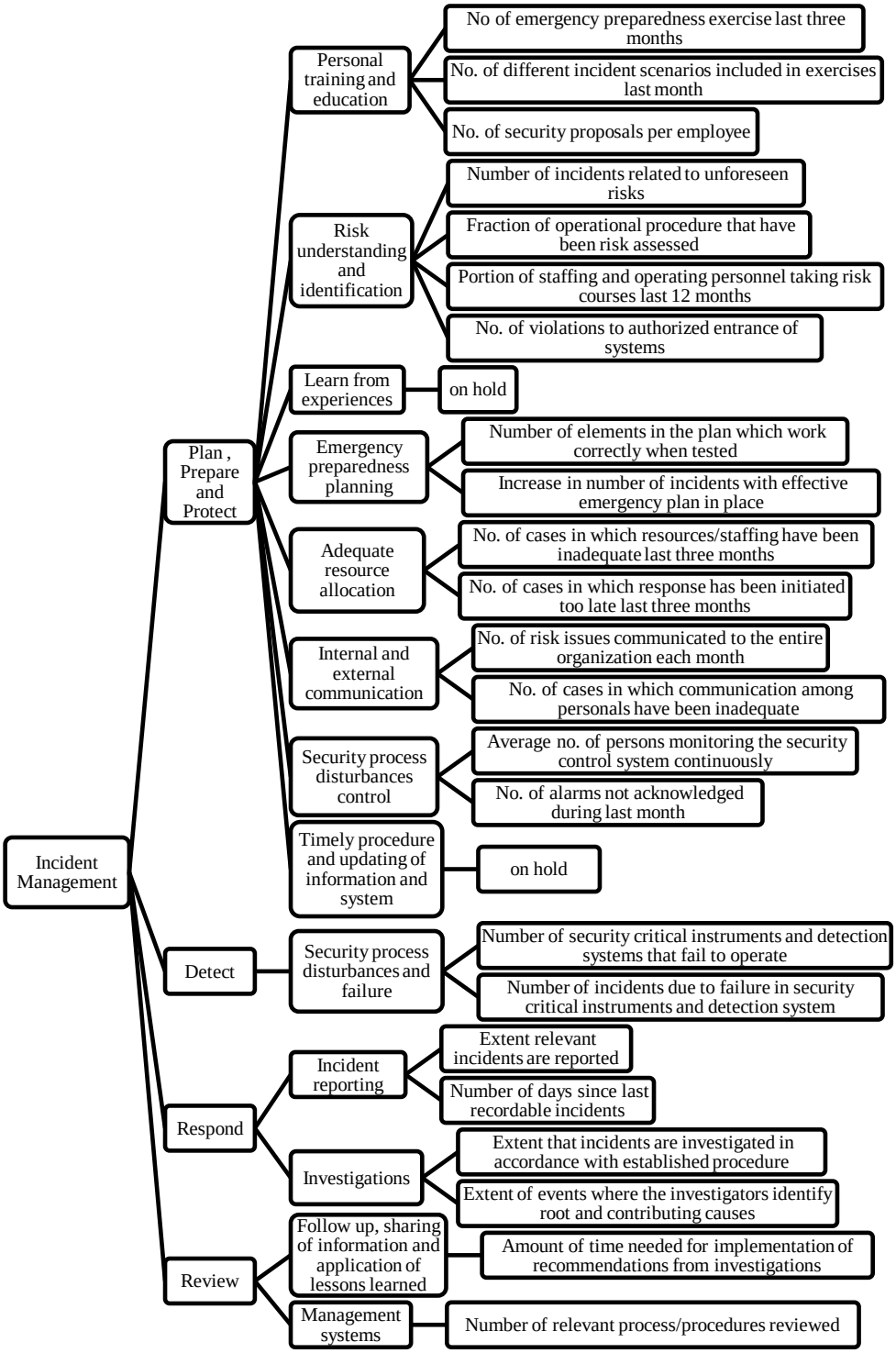

Figure 5.1: Overview of developed indicators

5.2 Indicator Characterization

The effectiveness of the indicators depends upon how they are identifying weaknesses, how they are indicating trend of security resource utilization and how they are measuring the failure and success of the overall system. Many researchers have argued that indicators should be few, stable and relevant to the process as well as business model that are being measured, but it is also true that there will be various security processes and controls in an organization. Those security processes might not be able to measure using only one or few indicators. In those cases, different number of indicators might have to be used which will measure the success as a whole. The selection of number of indicators (either few or many) also depends upon the size of an organization. For small and medium scale organizations, it might be hard to handle too much of data. Similarly, it also depends upon how specifically you want to measure the system performance. For example, if general indicators are used, few indicators might measure the overall system performance, whereas, many specific indicators might have to be used to measure overall system performance. But, specific indicators might be effective than general as they measure the effectiveness of each issues which are responsible for overall system performance. Most of the indicators developed in this thesis are specific indicators.

Managing, analysing and implementing indicators need time as well as resources. In most of the organizations, whether small, medium or large scale, the incident management indicators have not been used and implemented. One of the important reason behind it is lack of resources which is mainly organization's budget. The development and implementation of appropriate incident indicators need special team and special resources which is possible only if an organization has enough budget, and is ready to invest in it. The another important reason for lack of implementation of indicators in an organization might be thought of organization's management team on why to invest money on measuring security rather than doing it. This thought needs to be changed and is possible only if they are aware and familiar to the term return on security investment.

The developed indicators, as shown in figure 5.1, consist of both leading as well as lagging indicators. Wayne [17] suggests indicators should be differentiated as lead and lag otherwise misinterpretation may lead to the serious consequences. The table 5.1 shows the differentiation of developed indicators as lead and lag. Combining leading and lagging indicators also might sometime be useful. It is also necessary to know how the outcome will be achieved and how early warnings are notifying the current track for achieving goals. It is only possible when

lagging indicators are used with leading Indicators . Similarly, using leading indicators without lagging might disable the focus on long-term performance, and sometime it might not provide enough information regarding whether outcomes have been achieved or not.

Phases	Leading Indicators	Lagging Indicators
Plan, Prepare and Protect	• Number of incidents related to unforeseen risks • Fraction of operational procedure that have been risk assessed • No. of violations to authorized entrance of systems • No. of security proposals per employee • No. of risk issues communicated to the entire organization each month • Average no. of persons monitoring the security control system continuously	• Portion of staffing and operating personnel taking risk courses last 12 months • Number of elements in the plan which work correctly when tested • Increase in number of incidents with effective emergency plan in place • No of emergency preparedness exercise last three months • No. of different incident scenarios included in exercises last month • No. of cases in which communication among personals have been inadequate • No. of alarms not acknowledged during last month • No. of cases in which resources/staffing have been inadequate last three months • No. of cases in which response has been initiated too late last three months
Detect	• Number of incidents due to failure in security critical instruments and detection system • Number of security critical instruments and detection systems that fail to operate due to security attacks on them	
Respond		• Extent relevant incidents are reported • Number of days since last recordable incidents • Extent that incidents are investigated in accordance with established procedure • Extent of events where the investigators identify root and contributing causes
Review		• Amount of time needed for implementation of recommendations from investigations • Number of relevant process/procedures reviewed

Table 5.1: Characterizing Indicators as Leading and Lagging

For example, lagging indicator, 'No. of emergency preparedness exercise last three months'(let us say indicator 1) might affect the leading indicator, 'No. of security proposals per employee' (let us say indicator 2). In this case, if the value of indicator 1 has increased, it might be relevant that value of indicator 2 might increase. It does not necessary that it must increase but as a trend it should increase. It shows that the leading and lagging indicators should be considered side by side, to track down the progress of effectiveness.

5.3 Pros and Cons

Indicators can be used for benchmarking within an organization. They produce the trend of performance which could be use for self comparison. However, creating performance targets might lead to downfall if their progresses are not followed. Lack of participation of management team in developing and implementing indicators will decrease the effectiveness of the indicator value. The table 5.2 shows formulae for calculating the indicator value. It shows that there are some indicators which are easy to calculate like indicator 3 (portion of staffing and operating personnel taking risk courses last 12 months), indicator 6 (increase in number of incidents with effective plan in place), indicator 7 (no. of emergency preparedness exercise last three months), indicator 8 (no. of different incident scenarios included in exercises last month), indicator 12 (average no. of persons monitoring the security control system), indicator 18 (extent relevant incidents are reported), indicator 19 (number of days since last recordable incidents), indicator 21 (extent of events where the investigators identify root and contributing causes)and indicator 24 (number of relevant process/procedures reviewed). Other indicators might be some how difficult to calculate. In the rest of the paragraph in this section, indicator numbers from table 5.2 are used to denote the name of indicators.

The indicators 1, 2, 3 and 4 are related to the risk assessment. Risk assessment is the process of understanding, identifying, prioritizing vulnerabilities and threats. Risk assessment process identifies the probability of occurrences of security incidents and their level of impact. It is affected by number of factors like knowledge of personal involved in risk assessment, number of risk assessed areas, level of identifying new threats and vulnerabilities. The indicators 2 and 3 are more relevant as they specify exact point of issue. The indicator 1 is somehow hard to calculate, if succeeded, will be effective than other indicators. Though one of the main reason for the failure of projects related to Information Security Management System (ISMS) has been a poor risk assessments [43],

many organizations, ranging from small to large scale, have not taken it more

	Indicators	Formula
1	Number of incidents related to unforeseen risks	(Total no. of incidents) – (No. of incidents with identified risks)
2	Fraction of operational procedure that have been risk assessed	(No. of risk assessed operational procedure)/(Total no. of procedure)
3	Portion of staffing and operating personnel taking risk courses last 12 months	(No. of staffs taking risk courses last 12 months)/(Total no. of staffs)
4	No. of violations to authorized entrance of systems	Total no. of violations to authorized entrance of system in a month
5	Number of elements in the plan which work correctly when tested	Total no. of elements in plan working during test
6	Increase in number of incidents with effective emergency plan in place	(Total no. of incidents before emergency plan in place) – (No. of incidents after emergency plan in place)
7	No of emergency preparedness exercise last three months	Total no. of emergency prepared exercises performed last three months
8	No. of different incident scenarios included in exercises last month	Total no. of incident scenarios in exercises last month
9	No. of security proposals per employee	Total no. of security proposals by one employee
10	No. of risk issues communicated to the entire organization each month	Total no. of risks communicated in one month
11	No. of cases in which communication among personals have been inadequate	Total no. of cases with inadequate communication
12	Average no. of persons monitoring the security control system continuously	(Total no. of persons monitoring security control system in a day)/(No. of shifts in a day)
13	No. of alarms not acknowledged during last month	(Total no. of alarms during last month) – (No. of acknowledged alarms)
14	No. of cases in which resources/staffing have been inadequate last three months	Total no. of cases with inadequate resources/staffs last month
15	No. of cases in which response has been initiated too late last three months	Total no. of cases with slow initiation of response
16	Number of security critical instruments and detection systems that fail to operate	Total no. of instruments not working due to security attack on them
17	Number of incidents due to failure in security critical instruments and detection system	Total no. of incidents not detected as instruments were failed due to security breaches on them
18	Extent relevant incidents are reported	(No. of reported incidents)/(Total no. of incidents)
19	Number of days since last recordable incidents	(Last reported incident date) – (Current date)
20	Extent that incidents are investigated in accordance with established procedure	(No. of investigated incident with standard procedure) /(Total no. of investigated incidents)
21	Extent of events where the investigators identify root and contributing causes	(No. of responded incidents)/(Total no. of incidents)
22	Amount of time needed for implementation of recommendations from investigations	(Date of recommendations given from investigation) - (Date of implementation of recommendations)
23	Number of relevant process/procedures reviewed	Total no. of procedures reviewed

Table 5.2: Indicators and calculations

seriously than it should be. They are depending upon other trusted sources to

gain information about new threats and vulnerabilities. It is effective as well as efficient to get information regarding new threats and vulnerabilities from other sources but it would not be enough as system within your organization might have other vulnerabilities than those in trusted sources. This will give opportunity to new threat. Though the indicator 4 has been interpreted as lack of knowledge of users regarding system, risk and procedure, but there is also chance that they have violated the rule knowingly by misusing critical informations. They are technically called insiders. Though many companies are focusing on controlling the external attack, it has also become mandatory to protect the critical assets from insider attack. A report [1] says that insider attack has been more costlier to the organization in comparison to external attack. The indicator 4 might provide numbers regarding authorised people who has violated the rule by leaking critical informations, or maybe by trying some activities like checking for errors and vulnerabilities [44], intentionally causing harm for fame, greed.

After then, appropriate protection mechanism can be implemented for further protection against insiders. Though it is hard to collect the data for this indicator, appropriate implementation of control mechanisms and tracking their changes might be helpful to reduce the value of this indicator. There are different methods that can be adopted for risk assessments. Within an organization, there might have to adopt different risk assessment methods depending upon the scope and scale of systems and processes. This leads to inconsistencies in the value of these indicators.

The indicators 5 and 6 correspond to the emergency planning and preparedness. The emergency planning might be done for responding against incidents having wide scope and impacts the system within short period of time like distributed denial of service attack. This attack can compromise the availability of the information to the intended users by blocking the service. It leads to high business impact to the organization within short period. To measure effectiveness of emergency planning, procedure for the emergency planning can be tested by creating real case scenario and working elements can be observed, as denoted by indicator 5. It might be difficult to create the real case scenario. If created then attack vectors used in the scenario and that of real attackers might not be same. In that case, whole planning procedure would not work or need to be changed if actual attack occurs. But the indicator 6 might be effective one that can measure the efficiency of the emergency planning as data are easily available and more relevant and definable than indicator 5.

[1] http://www.csoonline.com/article/661719/report-insider-attacks-expensive-but-there-s-a-silver-lining

The information security awareness through training and education has great influence on controlling security breaches [45]. It can be argued that lack of training and education regarding security incident management has been one of the causes for security breaches in an organization. Many inside threats are also increasing due to improper information security awareness. Similarly, effective security decision can only be achieved if the security personnels are capable to do it. Their capability depends upon awareness, training and education. The indicators 7, 8 and 9 measure the effectiveness of the training and education regarding the risk, security breaches, security incident management. During training and education, if more number of emergency preparedness exercises and incident scenarios are included, the effectiveness will increase, as represented by indicators 7 and 8. The effectiveness of the personal the personal taking training will be evaluated through indicator 9 i.e output of the indicators 7 and 8 can be measured through indicator 9. Many researchers have proved that despite of the training and education provided to the employee by an organization, the transfer of skills gained through training programmes to the work environment has been negligible [45]. It shows lack of commitment of the employees to sustain the awareness gained through training and education. Somehow the indicator 9 presented here could be the effective one to evaluate the efficiency of employees and their learned skills after training programmes.

The indicators 1, 2, 3 and 4 measure the effectiveness of risk assessment process in an organization. But, the risk assessment becomes effective when the results of the assessments are communicated to the entire organization. The internal communications regarding new threats, vulnerabilities, change of plans and policies among the departments, employees, users are very important to improve the efficiency of the incident management system. The indicators 10 and 11 measures the effectiveness of the communication within an organization. The systematic approach is necessary to develop the organizational communication model that might influence greatly in emergency response [46]. Though some large scale organizations have formal communication model, medium and small scale organizations still lack proper systematic internal communication model. The results of indicators 10 and 11 might provide reason to implement the systematic internal communication. In case of emergency response, indicator 11 might be useful to measure how effective was the communication during that period. The organizational structure also affects internal communication within an organization. So, the comparison of indicators 10 and 11 might be hardly done among organizations.

Some of large scale organizations have established 24/7 monitoring team to

monitor the security process disturbances. They are analysing the traffic pattern to see abnormal behaviour as well as tracking the malicious packets through analysis process like anomaly detection, deep packet inspection. The indicators 12 and 13 might be seen as indicators for measuring the effectiveness of the security monitoring personal as well as the staffing allocation plan of an organization which has direct effect on the security process disturbances control. Based on the value indicator 12 (lagging), the value of indicator 11 (leading) could be adjusted. For example, if value of indicator 12 is low, it might be interpreted as inadequacy of persons monitoring the security system, and the value of indicator should be increased to see if that was the case. These indicators are highly definable and relevant indicators. They are not highly effective as they somehow measure the efficiency of security process disturbances control mechanism which is issue of concern for these indicators. But, they might measure the effectiveness as well as efficiency of resource(staffing) allocation plan of an organization.

The effective and adequate resource allocation has been one of the problem in an organization. The security vulnerabilities are changing frequently and threat agents are looking for exploitation of those vulnerabilities. So, the challenges are; to minimise the vulnerabilities using suitable technologies with minimal cost. Lotfi Hajjem et al. describes this as bi-objective problem [47]. In addition to this, response has to be initiated too fast in case of occurrence of security incidents which requires adequate technologies as well as staffing. To address this problem, adequacy of the resource has to be measured frequently. This allows to make decision regarding allocation of required resource effectively with minimal cost in an organization. The indicators 14 and 15 provides results if there has been inadequacy of resources. These two indicators are effective and highly relevant to measure the effectiveness as well as adequacy of the allocated resources and staffing in an organization.

The indicators 16 and 17 will not be able to measure overall the effectiveness of the incident detection capability of an organization. The indicator developed in this thesis are from safety indicator related research papers and standards. In the safety field, the failure of the safety critical instruments also lead to the safety incidents while in security field, incidents due to the failure of the security critical instruments are not considered as incidents. The analysis of the failure of critical instruments corresponds to the reliability analysis rather than CIA. However, failure considered here is due to security attacks on those security critical instrument like IDPSs which makes it more relevant to the information security. There are more indicators for monitoring of the incident detection capability like "mean

time to incident detection" and also the indicators and precursors that indicates the signs of security incidents. As we are adopting indicators from the safety part which are totally different in nature and type in the detect part of the security incident management process, we have only managed to adopt these two indicators, 16 and 17. The indicators 16 and 17 are somehow definable but they might not be effective and relevant. Though the security attacks have been successful in the IDPSs, it can be assumed that threat agent might not waste time on attacking the those detection systems rather than targeted main system. The indicators 16 and 17 might be useful in the large organization which are dealing with the sensitive data and information and have good security control system. In this case, threat agent might target the detection system first to stop the relay of signals to the concerned station.

The indicators 18 and 19 measure the effectiveness of the incident reporting system of an organization. The indicator 18 is highly appropriate in the field of security incident management because the ability to timely and accurately record and report the occurrence of security incidents will always affect the outcome of incident management process. Though indicator 19 is suitable for incident management, but it might be somehow hard to interprate it. The result of this indicator might not provide singular meaning. It should be carefully interpreted to discover the exact issue indicated by it because decrease in value of this indicator indicates improvement in detection as well as reporting capabilities in one hand and in other hand, it indicates ineffectiveness of security control system.

Many organizations still lack formalised incident investigation i.e containment, eradication and recovery process. Though they are handling the incidents, but they lack formalised established procedure. This makes hard to track and trace the process to see if there are any errors. This also makes difficult to measure the overall performance of the process. However, despite of having formal investigations procedure, sometime they are still not followed. The indicator 20 provides results regarding the established investigation procedure. If the indicator value is low, it might provide some information to the management why established procedure are not followed. There might be difficulties in following procedure or people are not aware or they are neglecting. The value of this indicator might affect the outcome of investigation i.e indicator 21. The indicator 21 is very much appropriate for the field of incident management. It is highly valid and measures the effectiveness of investigation process.

The review phase of the incident management must have direct involvement of the management. The indicator 22 measures the timely decision making capa-

bility of the review team. Most of the top level management of the organizations are looking for measuring the effectiveness of the system, technical team, employees but decision has to be taken by them for further correction and modification in process and system. They have to review the relevant processes and procedures too. The most important part will be timely decision making and implementation of the correction. The indicators 22 and 23 are important as well as effective to measure the efficiency of the management team. These indicators are also easily understood by the top level management. From the result of the indicator, they might be able to quantify their efficiency and strength, and correct themselves in case of failure.

The main disadvantage of most of the indicators in all phases of the incident management is that they might not be directly compared among organizations. Organizations have different sizes, scales and profile. Threat agents might use different attack vectors to get into the system depending on security control system implemented in organizations [18]. Similarly, the nature of attack vectors might be different according to the value of organizations. This makes difficult to set the common indicators for different organizations and comparison of indicators among organizations would not be effective. In the same way, challenges will also be identifying data sources, collecting and updating data over time for indicator calculations. In order to regularly measure the effectiveness of incident management process and constantly improve it, infrastructure (data sources, method, system, process and people) are needed to collect and update data over time. These need to be frequent and accurate as well. It might be costly to implement new systems and infrastructure for data collection. So, emphasis should be given to use existing mechanisms for maintaining data. Similarly, the accuracy of indicator result increases when the data are collected through automated means rather than through manual collection. In those cases, care should be taken while doing manual collection of data. The frequency of data collection as well as the indicators visualization method also affect the overall management process.

5.4 Scenario

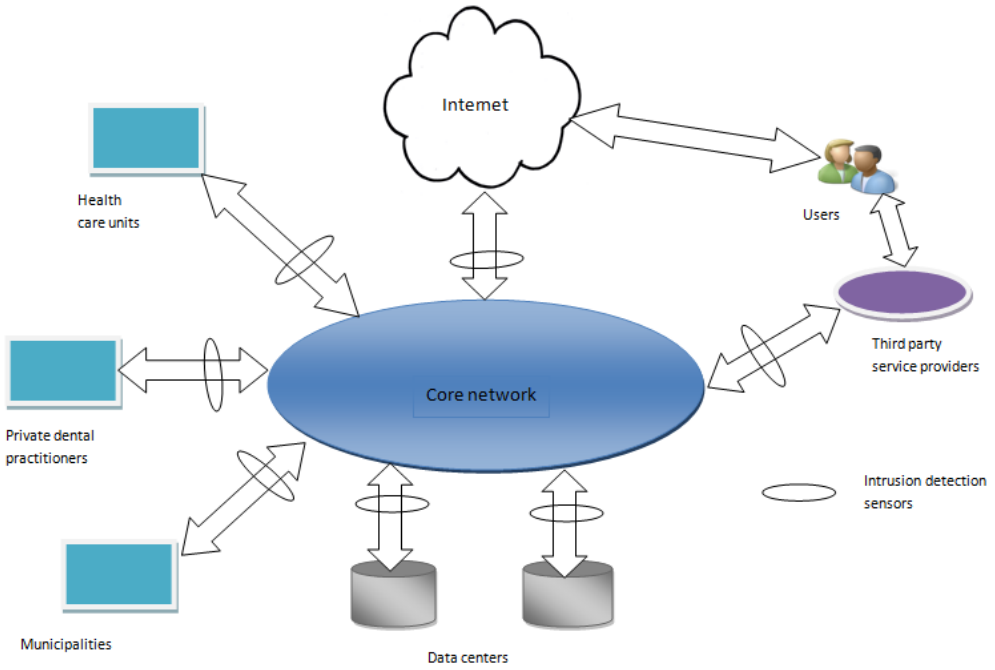

Figure 5.2: Scenario

'World link Network' is one of the leading network operator in the state. It provides network service to the most of the health care units, municipality and private health practitioners in the state. It also provides network service to third party service providers and through them to other users. It also has two data centres as shown in figure 5.2. The most important objective of this company is to interconnect all the parties and users of health system through secure network to exchange the patient information. It shows that all the critical information, data and resources are interconnected through this network. It historically experienced some security breaches that compromised critical informations of some of the health care unit and other users. Because of those security breaches, organization began to lose its reputation. Users complained showing no trust on their services. As a result some of the users disconnected their services. The management described this situation as opportunity to improve their security system as well as incident management capability. So they decided to establish the incident management team whose one of the task was to develop and implement the incident management indicators so that they could monitor and evaluate the effectiveness of their security control system and incident response

program. The other objective was also to find the weaknesses in their incident management procedure and take suitable corrective actions.

The incident management team was established. The team consisted of four members, one from management, two from CSIRT team and one senior IT security officer. The enough resources and budget were allocated for this team. They developed the timetable and all members agreed upon the performing periodic review of the work they have conducted.

The incident management team started their work by reviewing the recent security incidents and their reports. They also reviewed the organizational security plans, policies and procedures for security incident management. They went through the detail procedures and phases, the plan prepare and protect phase, the detect phase, the respond phase and the review phase, of the incident management. The main purpose of this was to find the main issue that has lead to the recent security breaches in the organization. They also increased the number of intrusion detection sensors to the starting edge of their every branch network to users as shown in figure 5.2. They also decided to monitor the network 24/7 where it was half a day previously. For this reason, they asked management for additional number of team members and other resources. Four more member joined the team, two network analysers and two more CSIRT members. They began to monitor the system and gather the data. The important part of monitoring was the traffic analysis to find the trend of their normal traffic behaviour and to do deep analysis in case of abnormal one. The relevant and current processes and procedures were also analysed. With all those reviews, analysis and monitoring, they concluded that the main issues that led to the recent security breaches were risk understanding and identification, security process disturbances control(described in chapter 4 table 4.2). This stated that they had their weaknesses in the early phase of the incident management. There was not effective planning and preparation to prevent the occurrence of potential security incidents.

To address these issues, they decided to develop a indicator and implement it to evaluate the level of risk understanding and identification, and security process disturbances control. The purpose was also to measure their level of weaknesses in the identified issues above and come with suitable corrective action to avoid further breaches. They identified four lagging as well as leading indicators for issue risk assessment and identification where as two lagging indicators for issue security process disturbances control. They are as:

1. Risk understanding and identification

- Number of incidents related to unforeseen risks (leading indicator)
- Fraction of operational procedure that have been risk assessed (leading indicator)
- Portion of staffing and operating personnel taking risk courses last 12 months (lagging indicator)
- No. of violations to authorized entrance of systems (leading indicator)

2. Security process disturbances control

   - Average no. of persons monitoring the security control system continuously (lagging indicator)
   - No. of alarms not acknowledged during last month (lagging indicator)

After identification of the suitable indicators, team decided to collect the data for all the above indicators. They identified the important data sources for the all of above indicators. For the indicators related to issue risk understanding and identification, the possible identified data sources were incident reports, risk assessment reports, incident analysis reports, risk management training reports, system logs. Similarly for issue security process disturbances control, the identified possible data sources were IDPSs, SIEM, staffing plan report. The team decided to collect the data on weekly basis. They notified all concerned authorities to update the data on weekly basis and report to them. With the collected data, they calculated the value of all the indicators on weekly basis. The team identified that trend analysis is necessary to see the changes in data and indicator values and they decided to have graphical representation of the indicator values. For all of the leading indicators they had also estimated the target.

After a each weekly collection of data and calculation of indicator value, the team also had an meeting with management to act upon the result of the indicator value. For example, the value of indicator 'Portion of staffing and operating personnel taking risk courses last 12 months' was very low initially, after meeting, management decided that the risk courses should be taken by all the staffs working and they also increased the number of risk courses to be taken at a time. After one month, the value went on increasing to good number. With all those indicators values and action upon them, initially, the number of incidents did not decrease sufficiently. Though it was decreased to some amount later on but not up to target the team has estimated. So, they began to review the other issues that might have lead to frequent occurrence of the security incidents. After review and analysis they found that, though the risk were identified

and assessed, identified vulnerabilities and threats were not communicated to entire organization sufficiently. So, the weakness was in their internal communication. They identified the indicator, 'No. of cases in which communication among the personals have been inadequate', to assess this issue of concern. They collected the data through interviews and survey. Initially they found that the communication mechanism in an organization to share critical information was very poor. They along with the management decided to change the procedure regarding the communication. They implemented the open and direct communication as one of the values of an organization. Direct communication was encouraged throughout the organization. They also decided to conduct the general meeting of an organization in every week to spread the critical information regarding threats and vulnerabilities. It was monthly previously.

After a certain time, all of those used indicators were reviewed and evaluated based on their effectiveness in achieving the organizational goal which was to monitor the performance of the incident management team and decrease the number of security breaches to the acceptable level. They decide to drop the indicator 'Portion of staffing and operating personnel taking risk courses last 12 months' as risk training was made mandatory to all of the staffs and personals. Similarly they also decided to discontinue with the indicator, 'Average no. of persons monitoring the security control system continuously', as there were enough personnels allocated to monitor the network 24*7. Other than those, they planned to continue with all other indicators. In addition to that, with continuous review and analysis, two other issues were to be addressed and related indicators were also identified for the plan , prepare and protect phase.

The scenario above presents how the security indicators of the previous chapters could be developed and implemented. It is also to show that other indicators developed here might be useful for the organization according to their needs and requirements. It is also obvious that all the indicators might not be able to use at a time. The basic way to develop and implement the indicators would be identifying the best issue of concern. In finding the true issue of concern, one way to start might be finding the loophole in whole system and weaknesses in organizational plans and policies.

It is also suggested that establishing separate team for performance indicator development and implementation might not be feasible and cost effective for any organizations. Instead of that, letting incident management team to work on indicator development and implementation will be beneficial technically and financially (as in the scenario). However, establishing incident management team itself might be difficult for small and medium scale organizations due to budget

issue. There will also be another issue of forming incident management team as different roles are handled by single person in those organizations. In small and medium scale organizations, available data and resources should be utilised and analysed by top management to see if they indicate the system performance as any fragment of data can be seen as indicator of something. The analysis of available data might indicate the performance of the overall security system as a general indicator or measure relevant issues within the system as a specific indicator.

Chapter 6

Conclusion and Further Work

6.1 Conclusion

A theoretical study of safety performance indicators has been performed. The study showed that there are some good and effective safety performance indicators that can be adapted to the field of security incident management. The effective safety indicators were adapted to the incident management field using the defined methodology described earlier in the thesis. An analysis and discussion of the indicators have also been performed. The analysis and discussions included nature, usage, pros and cons of the adapted indicators. This activity also included one scenario to describe how these indicators could be used and implemented within an organization. So, the presented issues and indicators are the result of the literature review, knowledge and expert's opinions from some of the leading network operators like Uninett and Helsenett within the field of information security incident management, and the safety performance indicators found relevant as a basis for development of security incident indicators.

It is found that though there are large number of developed and implemented safety indicators in the safety area, only limited number of them could be used effectively in different phases of security incident management. In the plan, prepare and protect phase of incident management, effective indicators have been adopted from the safety part. Similarly, we have been able to adopt more indicators for the plan, prepare and protect phase of the security incident management than for the other phases. This shows that in the safety area, emphasis has often been placed on preparing and preventing the safety incidents, rather than detecting and responding to them. This may be the case because safety threats are better observable and predictable. On the other hand, in information

security, more emphasis has been placed responding to the incidents rather than protecting against them. Though it is hard to prevent incident occurrence, the use of indicators developed in the plan, prepare and protect phase of incident management might provide support to monitor effectiveness of security practices performed in the same phase. It might well help to reduce frequent occurrence of security incidents in the organization.

However, the detection phase of incident management still lacks effective indicators to measure its performance. In the safety field, occurrence of incidents due to failure of safety critical instruments are also considered, where as in a security field incident occurrence due to failure of security critical instruments are not considered, as we are analysing CIA rather than the reliability. Similarly another reason for difficulties in adopting safety indicators in the detection phase of the incident management is nature and type of incidents as well as critical systems that are used in detecting the incidents. Nature and type of incidents are totally different from each other in the safety and information security field. The critical systems that are used in detecting incidents are also different.

It was not possible to analyse and evaluate each of the indicators as there are large number of developed and implemented safety performance indicators. The methodology used in adapting the safety indicators to the field of security is pure theoretical study and only deals with the development of the indicators. The developed indicators were not implemented to check their usability. To further evaluate quality of developed indicators, its performance needs to be measured in intended operating environment.

6.2 Further Work

One of the future work of this thesis might be implementation of the indicators to see how they measure performance of security incident management process within an organization. It will give us option to observe how reliable collected data are and how they affect the decision making process in the organization.

This thesis only includes security incident indicators adapted from the safety field. So, it lacks good indicators specially developed for the detection phase of the incident management. There are some effective incident management indicators developed by some research organizations like SANS [1]. The indicators developed here may be combined with existing indicators in the field to see the completeness. It might become effective and efficient and overall performance

[1] http://www.sans.org/

of incident management process might be measured.

References

[1] M. B. Line, E. Albrechtsen, S. O. Johnsen, O. H. Longva, and S. Hillen, "Monitoring of incident response management performance," *SINTEF ICT, NTNU*, 2012. [cited at p. 17, 24]

[2] NIST, "An introduction to computer security: The nist handbook," *NIST Special Publication 800-12*, October 1995. [cited at p. 1]

[3] OWASP, *Top 10 Risks*, 2010 (online accessed Nov 22, 2012). `https://www.owasp.org/index.php/Top_10_2010-Main`. [cited at p. 2]

[4] ISO/IEC, "Information technology-security techniques-information security incident management," *ISO/IEC 27035:2009*, 2011. [cited at p. 1, 3, 23, 29, 41, 55, 56, 57, 62]

[5] G. C. Wilshusen, "Cybersecurity threats impacting the nation," *United States Government Accountability Office*, April 2012. [cited at p. 3]

[6] J. Torres, J. Sarriegi, J. Santos, and N. Serrano, "Managing information systems security: critical success factors and indicators to measure effectiveness," *Information Security*, pp. 530–545, 2006. [cited at p. 3, 4, 17, 18]

[7] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide (draft)," *NIST Special Publication 800- 61 Revision 2 (Draft)*, January 2012. [cited at p. 3, 10, 11, 23, 29, 31, 54, 55, 57, 62]

[8] S. Berinato, "A few good information security metrics," *CSO Magazine*, July 2005. [cited at p. 4]

[9] R. Savola, "Towards a security metrics taxonomy for the information and communication technology industry," *Software Engineering Advances, International Conference on*, vol. 0, p. 60, 2007. [cited at p. 4]

[10] R. B. Vaughn, R. Henning, and A. Siraj, “Information assurance measures and metrics - state of practice and proposed taxonomy,” *Hawaii International Conference on System Sciences*, 2003. [cited at p. 4]

[11] V.-v. Patriciu, I. Priescu, and S. Nicolaescu, “Security metrics for enterprise information systems,” *Journal of Applied Quantitative Methods*, vol. 1, no. 7, pp. 151–159, 2006. [cited at p. 4, 27]

[12] J. A. Mañas-Argemí, “Security metrics and measurements for it,” *European Journal for the Informatics Professional*, vol. IV, pp. 28–30, August 2005. [cited at p. 4, 11]

[13] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, “Performance measurement guide for information security,” *NIST Special Publication Revision 1*, July 2008. [cited at p. 4, 20, 27]

[14] ISO/IEC, “Information technology - security techniques - information security management - measurement,” *ISO/IEC 27004:2009*, 2009. [cited at p. 4, 9, 11, 27, 56]

[15] M. Nyanchama, “Information security metrics - an overview,” *Agano Consulting Inc.*, 2009. [cited at p. 4]

[16] A. Jaquith, *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley, 2007. [cited at p. 4]

[17] W. Jansen, “Directions in security metrics research,” *NIST*, April 2009. [cited at p. 4, 16, 69]

[18] Center for Internet Security, “The CIS Security Metrics,” November 2010. [cited at p. 4, 20, 51, 77]

[19] Center for Internet Security, “CIS Security Metrics -Quick Start Guide v1.0.0,” November 2010. [cited at p. 4]

[20] D. Rathbun, “Gathering security metrics and reaping the rewards,” *SANS Institute*, 2009. [cited at p. 4]

[21] Shirley C. Payne, “Guide to Security Metrics,” *SANS Institute Information Security Reading Room*, July 2008. [cited at p. 4, 27]

[22] I. of operational risk, “Key risk indicators,” *Operational Risk Sound Practice Guidance*, November 2010. [cited at p. 9]

[23] M. Cloppert, "Security intelligence: Attacking the kill chain." http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain, October 2009. Online Accesed: 28/09/2012. [cited at p. 10]

[24] OECD, "Guidelines for the security of information systems and networks: Towards a culture of security," *OECD Council*, July 2002. [cited at p. 11, 12, 21]

[25] OECD, "Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response. guidance for public authorities and communities/public," *OECD Council*, 2008. [cited at p. 11, 15, 16, 23, 24, 32, 33, 57]

[26] G. Drogaris, "Major accidents in oil and gas industries," *Commission of the European Communities, Society of Petroleum Engineers*, 1991. [cited at p. 12]

[27] K. Øien, I. Utne, and I. Herrera, "Building safety indicators: Part 1 - theoretical foundation," *Safety Science*, vol. 49, no. 2, pp. 148 – 161, 2011. [cited at p. 12, 13, 14]

[28] A. Hopkins, "Thinking about process safety indicators," in *the Oil and Gas Industry Conference Manchester*, November 2007. [cited at p. 14]

[29] . H. C. Blakstad, "Safety indicators used by authorites in the petrolieum industry of uk, us and norway," *SINTEF Technology and Society, Safety Research*, 2012. [cited at p. 14]

[30] OECD, "Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response. guidance for industry," *OECD Council*, 2008. [cited at p. 15, 16, 24, 32, 56, 57, 63]

[31] HSE, "Developing process safety indicators: A step-by-step guide for chemical and major hazard industries," *Health and Safety Executive Books*, 2006. [cited at p. 15, 16, 21, 51, 52]

[32] K. Øien, S. Massaiu, R. K. Tinmannsvik, and F. Stoerseth, "Guideline for implementing the REWI method," *SINTEF Technology and Society, Safety Research*, march 2012. [cited at p. 15, 16]

[33] K. Øeien, S. Massaiu, R. K. Tinmannsvik, and F. Stoerseth, "Development of early warning indicators based on resilience engineering," *PSAM 10*, June 2010. [cited at p. 16, 32, 33, 51, 52]

[34] E.J. Byres and J.Cusimano, "Safety and Security: Two Sides of the Same Coin," *Chemical Processing*, March 2010. [cited at p. 18, 19]

[35] B. R. Pandey, “Metrics for information security - incident response,” master’s project, NTNU, june 2012. [cited at p. 20]

[36] M. Pokladnik, “An incident handling process for small and medium businesses,” *SANS Institute Information Security Reading Room*, July 2007. [cited at p. 23, 55, 57]

[37] S. Radack, “Security metrics: Measurement to support the continued development of information security technilogy draft,” *NIST*, 2010. [cited at p. 27]

[38] A. Dorofee, G. killcrece, R. Ruefle, and M. Zajicek, “Incident management capability metrics version 0.1,” *Software Engineering Institute*, April 2007. [cited at p. 32, 51]

[39] G. Stoneburner, A. Goguen1, and A. Feringa1, “Risk management guide for information technology systems,” *NIST*, 2002. [cited at p. 43]

[40] D. Wagner and P. Soto, “Mimicry attacks on host-based intrusion detection systems,” in *CCS ’02 Proceedings of the 9th ACM conference on Computer and communications security*, pp. 255 – 264, 2002. [cited at p. 53]

[41] T. Ptacek and T. Newsham, “Insertion, evasion, and denial of service: Eluding network intrusion detection,” *Secure Networks*, january 1998. [cited at p. 53]

[42] CBA and UKWA, “Safety performance leading indicators: Guidance for the chemical warehouse sector,” *Chemical Business Association*, December 2009. [cited at p. 63]

[43] F. Bjorck, “Implementing information security management systems - an empirical study of critical success factors,” [cited at p. 71]

[44] B. Ruppert, “Protecting against insider attacks,” *SANS Institute Information Security Reading Room*, April 2009. [cited at p. 73]

[45] N. Waly, R. Tassabehji, and M. Kamala, “Improving organisational information security management: The impact of training and awareness,” in *High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on*, pp. 1270 –1275, june 2012. [cited at p. 74]

[46] R. Dilmaghani and R. Rao, "A systematic approach to improve communication for emergency response," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, pp. 1 –8, jan. 2009. [cited at p. 74]

[47] L. Hajjem, S. Benabdallah, and F. Ben Abdelaziz, "A dynamic resource allocation decision model for it security," in *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on*, pp. 1 –6, 30 2010-april 1 2010. [cited at p. 75]

Appendices

Appendix A

Figures and Tables

Phases	Issues	Indicators
Plan, Prepare and Protect	Risk understanding and identification	• Number of incidents related to unforeseen risks • Fraction of operational procedure that have been risk assessed • Portion of staffing and operating personnel taking risk courses last 12 months • No. of violations to authorized entrance of systems
	Emergency preparedness planning	• Number of elements in the plan which work correctly when tested • Increase in number of incidents with effective emergency plan in place

Table A.1 – continued from previous page

Phases	Issues	Indicators
	Personnel training and education	• No of emergency preparedness exercise last three months • No. of different incident scenarios included in exercises last month • No. of security proposals per employee
	Internal and external communication	• No. of risk issues communicated to the entire organization each month • No. of cases in which communication among personals have been inadequate
	Security process disturbances control	• Average no. of persons monitoring the security control system continuously • No. of alarms not acknowledged during last month
	Adequate resource allocation	• No. of cases in which resources/staffing have been inadequate last three months • No. of cases in which response has been initiated too late last three months
	Learn from experiences	(On hold)

Table A.1 – continued from previous page

Phases	Issues	Indicators
	Timely procedure and updating of information and system	(On hold)
Detect	Security process disturbances and failure	• Number of security critical instruments and detection systems that fail to operate • Number of incidents due to failure in security critical instruments and detection system
Respond	Incident reporting	• Extent relevant incidents are reported • Number of days since last recordable incidents
	Investigations	• Extent that incidents are investigated in accordance with established procedure • Extent of events where the investigators identify root and contributing causes
Review	Follow up, sharing of information and application of lessons learned	• Amount of time needed for implementation of recommendations from investigations
	Management systems	• Number of relevant process/procedures reviewed

Table A.1 – continued from previous page

Phases	Issues	Indicators

Table A.1: Phases, Issues and Developed Indicators