THE INCIDENT PREVENTION TEAM

A proactive approach to Information Security

Nishan Marc Pereira

Delft University of Technology

January 20th, 2015
Delft

THE INCIDENT PREVENTION TEAM

A proactive approach to Information Security

Committee Chair:
Prof. Dr. Ir. J. van den Berg

Supervisors:
Dr. Ir. W. Pieters
Dr. Ir. D. Hadziosmanovic
Dr. M. E. Warnier
J. Tuin (Dutch Police, LE)
M. Hoeke (ATOS Consulting)

Author:
Nishan Marc Pereira
n.m.pereira@student.tudelft.nl
Student No: 4244672

DELFT UNIVERSITY OF TECHNOLOGY

Faculty of
Technology, Policy and Management (TBM)
Systems Engineering, Policy Analysis and Management

January 20th, 2015
Delft

Dedicated to Mom, Dad, Rahil & Zubin,
Your love, support and prayers, has made this possible.

Executive Summary

Information Security is an important aspect of decision making in organisations today. Organisations use Information Security Risk Management to assess, respond to and monitor risk to its information systems. Information systems are complex technical systems and the management of Information Security depends on technology, processes and people. Incident Response Teams are set up to manage cyber incidents. However, the increasing trends in incidents reported, indicate that these controls are failing to achieve their goals, because, these controls primarily focus on information available after the occurrence of an incident. Despite the efforts in Information Security Risk Management, organisations are unable to implement effective Information Security controls based on dynamic information.

In order for organisations to effectively mitigate risk, there is a need to also focus on incident prevention along with incident response practiced today. Therefore, in this research, we assess the Technical, Institutional and Process aspects of risk management and incident response process, using TIP Design for socio-technical systems. This is a systematic, design-oriented way of analysing the current state of organisation's information system security. We conclude that the process is retrospective and unable to proactively prevent incidents, thereby Information Security controls lag incidents. Furthermore, precursors, i.e. information available before the incident occurs, are not effectively used to prevent incidents. The research goal, "How can an incident prevention process be developed to proactively use information available to complement Information Security Risk Management in organisations?" will be answered in this research.

We structure this research using the Design Science Research Cycle. With the various requirements, generated from the analysis of the risk management and incident response process, we generate design ingredients. Firstly, we use precursors to determine the information available before the incident. Secondly, we use the concepts of trigger, template and twitch from Vigilant Information Systems and extend it with tweak, to interpret the information. Finally, this research proposes to establish "The Incident Prevention Team" to bridge the gap described in Information Security Risk Management.

In this research, we use the Incident Response Lifecycle and extend it by developing the incident prevention process followed by the Incident Prevention Team in the preparation phase of this lifecycle. The Incident Prevention Team assesses the current Information Security status of the organisation using information affecting external organisations. The Incident Prevention Team scans and then prioritises the most relevant information for the risk assessment process. It then performs an Information Security risk assessment of the information system affected and finally recommends control strategies to the management.

The incident prevention process was evaluated using two scenarios and by an interview with an Information Security expert. The validation encourages us to conclude that the proposed Incident Prevention Team and the incident prevention process provide a proactive method to achieve Information Security in organisations. The main limitation of this research is the lack of empirical testing, which is an opportunity for further research. Organisations can easily incorporate the Incident Prevention Team to fulfil both its strategic and operational requirements of Information Security Risk Management. By establishing the Incident Prevention Team, it creates an agile and structured process within the organisation to understand the risk to both the internal and external environment proactively. Therefore, the Incident Prevention Team will transform the organisation's incident response process from being reactive to proactive, thereby making the organisation resilient against potential cyber incidents.

This research contributes to the existing field of Information Security research, with the focus on Incident Prevention by scanning for precursors. We further combine, the elements of "trigger", "template", "twitch" and extends it by "tweak" to structure incident information. This also offers new ways for Information Security professionals to interpret information.

Acknowledgements

Today, I am one step closer to making my career in the field of cyber security, however when I started my Master's, I did not expect to get into this fascinating field of study. This research has been a very long, but inspiring and valuable experience for me. I have had the opportunity to network with many experts in the field, and for that I am extremely grateful.

I would like to thank my Committee Chair: dr.ir. Jan van den Berg for providing valuable advice for my research during this thesis project.

I would like to express my sincere gratitude and appreciation to my first supervisors: dr.ir. Wolter Pieters and dr.ir. Dina Hadziosmanovic for their patience with me. Their constant support, constructive criticism and suggestions provided the right direction for my research. Their *good cop - bad cop* avatars, helped me to not get lost. Their guiadance helped in improving my research contribution and also improved my writing skills in the process. I would also like to thank Martijn Warnier, for his support and feedback. To drs. Jolien Ubacht, your kind words meant a lot.

I would especially like to thank Marcel Hoeke, whose suggestions and feedback helped me to add a practical aspect to this research. His support in helping me correct my writing also improved this report. I would also like to thank Jacques Tuin for his advice and critical input on the subject. I started my research on this subject with Marcel and Jacques, who provided me with the perfect problem to explore. I apologise for not solving the problem, but I hope this thesis is a small step in that direction.

To Raymond and Roy, you have helped me in ways I cannot express. Thank you for placing your trust in me and for your inspiring conversations on the subject. I would also like to thank Ewout, for contributing his valuable time and expertise for the interview.

Finally, I want to thank my family, you have kept me in your prayers. Without your love, support and prayers, this would not have been possible. You have helped me to stay focused, and finish my studies.

Marius, Ruben, Hendrik and CY, many thanks for proof reading this report.

Thank you, Chiwei and Hiske, for your friendship and to Jordy and his family, for having me over to celebrate Christmas. And last but not the least, a very big hug to my Boardies at SoSalsa! and to all my other friends here in Delft, for making this journey worth it.

"Never let music be wasted!"

- Nishan Marc Pereira
Delft, January 3rd, 2015

Contents

List of Figures

List of Tables

Acronyms

CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CPNI	Centre for the Protection of National Infrastructure
CSV	Comma-Separated Value
HHS	Health & Human Services
HIPAA	Health Insurance Portability and Accountability Act
ICS	Industrial Control Systems
IPT	Incident Prevention Team
IRT	Incident Response Team
ISDT	Information System Design Theory
ISO	International Organisation for Standardisation
ISRM	Information Security Risk Management
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
PoS	Point of Sale
SCADA	Supervisory Control And Data Acquisition
SCSIE	SCADA and Control Systems Information Exchange
SSL	Secure Sockets Layer
TIA	Telecommunications Industry Association
TIP	Technical, Institutional and Process
USA	The United States of America
US-CERT	United States Computer Emergency Response Team
VIS	Vigilant Information Systems
XML	Extensible Markup Language

Part I

Introduction

1 | Background

Information is a key driver in organisational decision-making. Information exchange occurs across all levels, from top management to the operational level. At each level, users receive information and make decisions based on individual and organisational interpretation of the information [1]. For example, the management of an organisation providing competitively priced products would take decisions based on economic benefits perceived. To do this, decision makers need accurate and real-time information to justify their decisions.

The advances in communication and networking technology enable organisations to retrieve information from every corner of the organisation. Systems that previously operating in silos are now interconnected in this wide and ever expanding network. Examples like industrial SCADA (Supervisory Control And Data Acquisition) systems remotely operated via the Internet; smart home refrigerators, etc. form part of this wide interconnected network. Organisations use these information systems to reduce costs, maintain a competitive edge in the market and improve productivity and profitability by processing and disseminating vast volumes of information [2, 3]. However, we can see that information itself has value; and has given rise to an information economy [4]. Organisations are transforming into digital organisations using information as capital [5]. Therefore, information is an important asset in organisations today [6]. However, this pervasive use of information technology is not without its share of risk.

The risk in organisation is exploited by attackers targeting them. The impact of these attacks is illustrated in these examples. The Estonian government networks faced a denial of service attack in April 2007. Stuxnet affected Siemens industrial control systems in October 2010. A cyber attack forced the Canadian government agencies to disconnect from the Internet in January 2011. Kaspersky discovered Red October a worldwide attack in October 2012; South Korean financial institutions had their networks infected in March 2013 [7] and recently Heartbleed, a security bug, affected the Internet TLS protocol in April 2014 [8]. The literature highlights two key features of the Information Security environment as reasons for the inability in managing these risk [9]:

1. Diversity of security threats
2. Dynamic changes to Information Security environment

1.1 Diversity of security threats

The threats affecting organisations are diverse. Literature categorises threats based on different contexts, described in detail in Appendix A. Loch et al., (1992) describes threats based on the source (internal and external) and perpetrator (human and non-human) [10]. According to Whitman (2004), threat categories are extensive and include acts of human error, deliberate acts of espionage and sabotage, forces of nature, technological failure, etc. [11] Thomas Rid (2012) simplified the categories of threats into three main activities of sabotage, espionage, and subversion [12]. Hypponen (2011), on the types of online attacks, classifies threats as online criminals, hacktivists and nations states [13]. Based on threat vectors, Chabinsky (2010) differentiates threats based on supply chain and vendor access, remote access, proximity access and insider access [14].

An attacker targets both public and private organisations unscrupulously. More so, our personal accounts are also susceptible to attacks.

With these broad categories described, we see that threats can vary according to the nature of the attacker, the intended target and even the tools and methodologies used. The complexities of interactions with various information systems are only increasing. Therefore, this creates a plethora of opportunities for adversaries to target information systems.

1.2 Dynamic changes to Information Security environment

The Information Security environment is subject to changes due to advances in technology and change in the work environment itself, described in detail in Appendix B.

Technological advances make information systems easier to handle. It also increases the mobility of users and offers increased computing power at a click of a button. However there is also an increased risk with these changes in the Information Security environment. Technologies like mobile Internet, cloud computing, BYOD (bring your own device), etc. help to create new opportunities, but at the same time are prone to Information Security risk [15].

Moreover, the work environment is rapidly evolving. It is no longer restricted to local areas and defined by geographical boundaries. In the book *"The World is Flat"*, Friedman (2006) explains the international outlook of organisations today [16]. These strides in digital development are connecting information systems and offering new avenues for business and growth. However, it is difficult to fully predict the nature of interactions, because theses systems were not connected earlier. Therefore, this creates risk because change in one area of the information system can influence another area.

1.3 Motivation for Research

The increasing trends in cyber incidents highlight that there is a failure in Information Security Risk Management as practiced in organisations today. The risk assessment process helps to develop risk controls for the risk determined [17], based on the combination of risk assessment and context for making decisions [18]. However, in today's dynamic Information Security environment, the context changes and has to be considered in the Information Security Risk Management process.

A quick scan of recent cyber incidents, reveals similarities in types of threats impacting other organisations. Verizon (2014) reports that the point of sale intrusions, denial of service attacks and web application attacks are responsible for 76% of cyber security incidents in the retail industry [19]. Furthermore there is an increasing trend of cyber incidents reported. Pwc in its Information Security Survey, finds the compound annual growth rate (CAGR) of detected security incidents has increased 66% year over year since 2009 [20]. Other reports also indicate the rise and similarity of cyber incidents reported [21, 22, 23].

Practice shows that not all incidents can be clearly characterised with the two features of diversity of security threats and dynamic changes to Information Security environment. Let us consider the example of two large-scale retailers of Target and Home Depot that were recently the target of cyber attacks. These attacks occurred months apart. The data breaches at both organisations had an estimated impact of loss of more than 100 Million Credit card details and another 70 million customer personal information. The financial impact of the data breach at Target and Home Depot runs into millions. In Appendix C, we make a detailed comparison of these two data breaches and summarise the key findings of the cyber incidents below, based on the features of the Information Security environment described earlier [9].

- Diversity of security threats: The threat affected the same Point of Sale (PoS) system at both Target and Home Depot. BlackPOS is allegedly the same malware used in the attack. This means that the diversity of threats is not a factor in this case.
- Dynamic changes to Information Security environment: It is reported that Home depot on learning of Target's data breach, procured encryption software for its credit card data. However, it did no implement the software and failed to update its information system's security controls. This lapse in security was an implementation failure in the Information Security environment.

Therefore, in the above example, we see that the features of the security environment do not always hold true. The BlackPOS threat and the Point of Sale (PoS) systems affected were similar in both cases. With the high profile Target data breach, retailers around the world are aware of a security flaw in the Point of Sale (PoS) system. A key learning from this cyber incident was the requirement of introducing chip-and-PIN technology at the Point of Sale (PoS) systems at retailers as additional controls. However, Home Depot was still affected, even after having procured encryption software for its credit card data. Therefore, the example highlights the question if the scale of the attack could have been decreased if Home Depot processed the information on recent incidents with more urgency.

As additional controls, during a cyber incident, an Incident Response Team is set up to manage the incident [24, 25, 26, 27]. However, the information on threats and vulnerabilities was available before the incident itself. This raises the question, why the Incident Response Team was not able to proactively address Information Security risk based on information already available. We argue that there is a need to also focus on incident prevention along with incident response practiced today. Therefore, in this thesis we will try to address this gap highlighted.

2 | Research Objectives and Methodology

In the previous chapter, we see that there is significant attention given to Information Security, but despite this, cyber incidents continue to occur. Therefore, the objective of this research is to determine the gap in Information Security Risk Management currently practiced in organisations. The ISO/IEC 27005:2011 standard [28] is designed to assist the satisfactory implementation of Information Security based on a risk management approach. However, Information Security controls are imperfect and incidents are bound to happen. Therefore, the ISO/IEC 27035:2011 standard [29], recommends organisations to establish an Incident Response Team (IRT) to manage incidents. However, we argue that the current view on incident response in organisations is not sufficient. The IRT responds to incidents after detecting an incident. It is a retrospective measure. However, an attacker continuously scans for vulnerabilities and targets them, displaying their proactive approach to achieving their goals.

Similarly, organisations today should develop a process to proactively scan for information regarding its Information Security and use it to prevent incidents. This would make the organisation more resilient against Information Security risk. This research will answer *"who"* initiates this process in organisations, *"how"* it is achieved and *"what"* inputs are required to effectively interpret the information.

2.1 Research Goals

To answer the above questions, we formulate the main research question as follows.

"How can an incident prevention process be developed to proactively use information available to complement Information Security Risk Management in organisations?"

This process would provide a step-by-step approach to address Information Security risk to the organisation based on information retrieved proactively. It would also address, who is responsible for performing this process. To gain a deeper understanding of the process and understand its implications to organisations, the following sub questions are derived to achieve the main research question.

(SQ 1) What is the missing link in Information Security Risk Management?

(SQ 2) What characteristics can be used to interpret incident information?

(SQ 3) What are the main operational tasks to be performed?

(SQ 4) What is the added value of the design solution in case of cyber incidents?

We use the process described in the National Institute of Standards and Technology (NIST) publications on Information Security Risk Management. The Computer Security Incident Handling Guide [24] describes the process followed by Incident Response Teams and the Risk Management Guide for Information Technology Systems [17] describes the risk management process. These two guides provide a comprehensive description of the two processes described and is widely adopted [30]. Therefore, we use this literature as a starting point in this research.

2.2 Research Methodology

We structure this research using the Design Science Research Cycle, described by Kuechler & Vaishnavi (2008) [31]. Figure 1, *Design Science Research Cycle for Information Systems*, visualises this research process. This methodology allows for research through design and is the art of learning through the act of building. This method is selected since it can help plan for feedback and changes throughout the phases of this research project. We answer the various research sub-questions in the different phases of this Design Science Research Cycle.

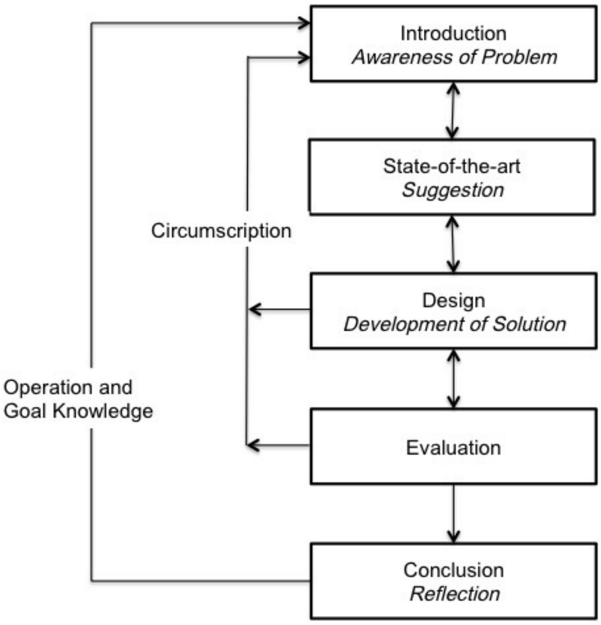


Figure 1: Design Science Research Cycle for Information Systems, derived from [31]

In the following stages we answer the research sub-questions to achieve the main objective of this research.

1. **Introduction**
   This is the problem conceptualisation phase of the thesis. The Design Science Research Cycle describes it as the awareness of problem phase. In Chapter 1 *Background*, we describe the challenges organisations face in Information Security. The literature reviewed and the increasing cyber incidents show the diversity of security threats and changes to dynamic Information Security environment in organisations are not the only reasons for the failure in Information Security Risk Management. The examples, indicate that information about threats and vulnerabilities is available and the focus on incident prevention is inadequate. Therefore, this brings us to the main research question, *"How can an incident prevention process be developed to proactively use information available to complement Information Security Risk Management in organisations?"* to be addressed at the end of this Design Science Research Cycle.

2. **State-of-the-art**
   The Design Science Research Cycle describes this phase as the suggestion phase. We address the research Sub Question (1) in this section of the report. In this phase, we first describe the current Risk Management and Incident Response process adopted in organisations by looking at the scientific literature and industry white papers available. The challenges in these process are further analysed and enumerated using the TIP design perspectives [32], described in Chapter 5 *Aligning Risk Management and Incident Response.* The gap analysis describes the state-of-the-art research in the field, which will help to define the requirements for the design phase of the research.

3. **Design**
   The Design Science Research Cycle describes this phase as the development phase. We answer the research Sub Question's (2) & (3) in this section of the report. To do this, we first describe the key ingredient required for the incident prevention process envisioned. Secondly, the characteristics to effectively interpret incident information to prevent incidents is determined. We then use these ingredients in a structured process. Here, in the design solution, we will answer *"who"* initiates this process in organisations and *"how"* we operationalise the incident prevention process effectively.

4. **Evaluation**
   We answer the research Sub Question (4) in the evaluation phase of the report. Here, we evaluate *who* initiates this process in organisations, *how* it is achieved and *what* inputs are required to effectively interpret the information using example scenarios validated by security experts. The design solution will also be validated with the help of an interview with a security expert. Further scope of improvements and limitations of the proposed design is suggested in this section.

5. **Conclusion**
   Finally, in the conclusion phase of the report, we summarise the main recommendations of this research. This is followed by the limitations of this research as well as the future research based on the limitations. The Design Science Research Cycle also describes this phase as the reflection phase. Based on the main research (sub)questions the operation[1] and goal knowledge can be reflected upon in the conclusion.

2.3 Scientific Relevance

The objective of this research is to add scientific value to the current state of Information Security research. The majority of studies published in Information Security literature focuses on reacting after the incident, therefore there is a gap that can be addressed by this research. The use of Design Science Research Cycle by Kuechler & Vaishnavi (2008) [31] is a structured methodology used to develop the design solution, which adds value to the research. We will make use of TIP design as an approach to analyse and design a solution for socio-technical systems [32]. The TIP design describes three perspectives of Technical, Institutional and decision Process that can be used to evaluate the gap in the current state of Information Security. With the help of these perspectives,

[1] An operational principle can be defined as "any technique or frame of reference about a class of artifacts or its characteristics that facilitates creation, manipulation and modification of artifactual forms" [31].
In this research, the operation will be reflected upon by using the TIP design perspectives [32], described in Chapter 5.

we can generate requirements to develop the incident prevention process by considering both the technical and institutional artifacts.

2.4 Societal Relevance

The development of Information Security research in general is valuable to companies today because of the increasing trend of cyber incidents reported. The initial research describes the situation where information pertaining to a company's security is available and yet it was not utilised to prevent incidents. Therefore, by considering this information in our research, we add another dimension to the perspective of Information Security, therefore being relevant for organisations today.

With the focus of this research, addressing Information Security risk by proactively retrieving and interpreting information available, it will create a more resilient Information Security system in organisations. Furthermore, the use of TIP design helps to describe the socio-technical nature of information systems. This is important because it shapes the decision-making process in organisations.

2.5 Thesis Structure

The Figure 2, *Thesis Structure*, describes the research sub-questions aligned with the main research phases. It further describes the structure of the report.

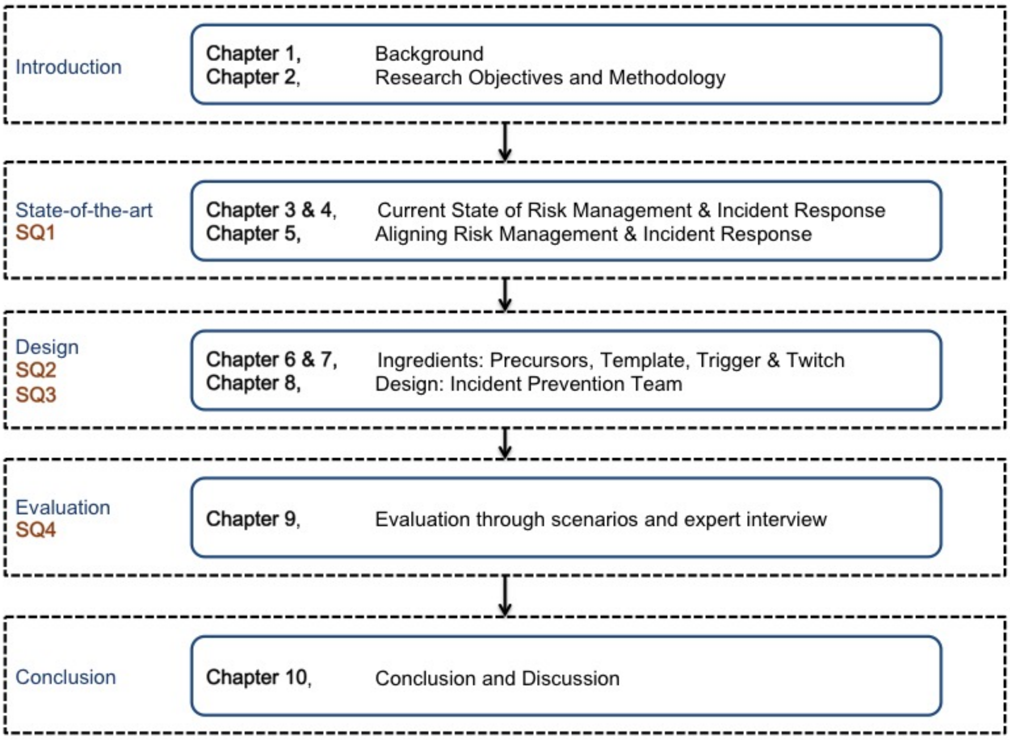

Introduction
Chapter 1, Background
Chapter 2, Research Objectives and Methodology
State-of-the-art
SQ1
Chapter 3 & 4, Current State of Risk Management & Incident Response
Chapter 5, Aligning Risk Management & Incident Response
Design
SQ2
SQ3
Chapter 6 & 7, Ingredients: Precursors, Template, Trigger & Twitch
Chapter 8, Design: Incident Prevention Team
Evaluation
SQ4
Chapter 9, Evaluation through scenarios and expert interview
Conclusion
Chapter 10, Conclusion and Discussion

Figure 2: Thesis structure

Part II

State-of-the-art

3 | Current state of Risk Management

In Chapter 1: *Background*, we found that the Information Security Risk Management process is not fully effective. To understand this process, in this chapter, we will describe the current state of risk management in organisations. In Section 3.1, we will describe the risk management process by dividing it into two main steps of Risk Assessment and Risk Control. This will be followed by describing the risk management tools utilised in companies in Section 3.2 and a summary in Section 3.3.

3.1 Information Security Risk Management

Information systems are an integral part of organisations today. With the pervasive use of information systems, organisations need to strive to achieve confidentiality, integrity and availability of information. These aspects of Information Security are defined in the ISO 27001:2013 standard [33]. Information Security standards are an important starting point towards the development of Information Security Management systems. These standards are guidelines towards the achievement of a minimum level of Information Security.

Blakley, et al. (2001) describes Information Security as "Information Risk Management" or "Information Security Risk Management" (ISRM) [34]. ISRM is not a one-time activity but a reiterating process [35], because the Information Security environment in organisations can change. The ISO/IEC 27005:2011 standard [28] is designed to assist the satisfactory implementation of Information Security based on a risk management approach.

Murray-Webster et al. (2010) [36] describes risk as *"uncertain event(s) that if it occurs, will have an effect on the achievement of objectives"*. Both the internal Information Security environment as well as external threats influences the risk posture in organisations. It is therefore important in organisations today to effectively manage risk associated with these events. To cope with these challenges organisations adopt different ISRM methods [35]. Risk management addresses risk from the strategic level to the tactical level in organisations. Risk management is a comprehensive process that includes establishing the context for risk-based decisions, assessing risk, taking steps to reduce risk to an acceptable level, responding to risk once determined and monitoring risk on an ongoing basis [37]. We will now describe risk management according to the following steps.

1. Risk Assessment
2. Risk Control

3.1.1 Risk Assessment

This section describes the Risk Assessment process, which can be both quantitative or qualitative [38]. The quantitative process uses mathematical and statistical tools to represent risk. For example, quantitative risk assessment is used in large technological systems like nuclear power plants, water repositories, incinerators, etc. [39] This assessment is used in combination with other safety and security requirements to make informed decisions. Qualitative risk assessment on the other hand uses adjectives to represent risk. For example, scenario analysis, questionnaire, and fuzzy metrics are used as qualitative methods [40].

The risk assessment steps help to identify risk in the organisation. Information is recorded in a risk register, facilitating the capture of relevant information about the information system, the risk and associated controls. The information obtained in this process is vital to the understanding of the management of Information Security. The ISRM guide describes risk assessment as a 9-step activity [17].

1. System Characterisation
   The information systems of the organisation are described in detail based on its characteristics. The boundaries of the information system, along with its interconnections are defined in this activity.

2. Threat Identification
   The threat is described as the potential for a particular threat-source to successfully exercise a particular vulnerability. The information retrieved here involves the threat sources, the motivation behind the threat and the threat actions used to attack a target.

3. Vulnerability Identification
   An understanding of the weaknesses in the Information Technology (IT) environment is crucial to the understanding of risk. A list of vulnerabilities help to see what systems are prone to attacks. These are identified from various vulnerability sources like the National Vulnerability database (NVD) or identified by testing the information system.

4. Control Analysis
   In this step the controls implemented are analysed based on the threats and vulnerabilities. The control methods include both technical controls and management controls. Moreover, there are preventive and detective control measures. The information retrieved defines the security baseline of the organisation.

5. Likelihood Determination
   Using the information from the threat identification, the vulnerability identification and control analysis, the likelihood of the threat being exercised is determined. This is a qualitative step, where the information can be categorised as high, medium or low. This categorisation varies according to each organisation.

6. Impact Analysis
   The impact to the business based on sensitivity and criticality of IT assets are used to prioritise information at this stage. The information retrieved at the end of this step quantifies the information for helping decision makers interpret the information easily to take decisions.

7. Risk Determination
   Risk is defined as the likelihood that a certain threat will engage in an attack, the vulnerability of the target (asset) to the threat and the potential impact that the attack might have on the asset [35]. Ionita (2003) describes a variety of risk computations methods to determine risk [35]. A risk scale and a risk-level matrix is developed to describe risk in this step of the process.

8. Control Recommendations
   The control measures to reduce risk are identified. The measures adopted are determined

by the level of risk that the organisation is willing to accept. The goal is the reduction of risk and can be achieved by assumption of the risk, avoiding the risk, limitation of the risk, planning for the risk or risk transference.

9. Results Documentation
   Information learned from the risk assessment process is finally compiled in a risk register. This register helps to inform stakeholders of the potential risk in the organisation and to assist them in taking informed decisions.

3.1.2 Risk Control

This section describes the Risk Control process. The risk control process follows from the risk assessment process and includes the prioritising, evaluation and implementation of appropriate control measures. It is not possible to eliminate risk. This is because there exists inherent risk beyond the control of the organisation. However, risk can be controlled to a reasonable level. This level is based on the risk appetite that varies in each organisation. For example, insider risks in the defence sector dealing with confidential information and insider risk in a supermarket dealing with store inventory information is different.

The ISRM guide describes risk control as a 7-step activity [17].

1. Prioritise Actions
   The risk assessment process identifies a number of actions to be taken. However, not all measures are implemented and have to be prioritised. Risk Levels determine risk the organisation is willing to take and can range from low-risk to high-risk.

2. Evaluate Recommended Control Options
   This step of the process focuses on assessing the feasibility and effectiveness of recommended actions prioritised in the previous step. This step is influenced by the objectives of the organisation. The appropriate controls are selected in this step.

3. Conduct Cost-Benefit Analysis
   Feasibility studies on the recommended controls are a key step that enables the top management to make informed decisions. Moreover, a cost benefit analysis helps to justify the cost versus risk reduction achieved.

4. Select Control
   In this step, the decision on the control is selected for risk determined in the risk assessment. The controls include technical controls like access restrictions or management control like policies, guidelines and standards or a combination of both technical and management controls.

5. Assign Responsibility
   The responsibility of ensuring that controls are implemented according to design is important. Therefore, persons with the required expertise and skills are selected to implement the controls identified.

6. Develop a Safeguard Implementation Plan
   The safeguard implementation plan is described as the process that helps to prioritise im-

plementation actions. It is made tangible with project start and completion dates and with deliverables of control strategies in the plan.

7. Implement Selected Control(s)
   Finally the team responsible as defined in 5th step of this process implements the selected technical and management controls.

3.2 Risk Management tools

There is a variety of risk management tools available to assess and control risk. Organisations need to choose the right tool that fits its business requirements. However, this decision can vary with location, business models, architectures etc. of the organisation. The Open Group (2009) elicited a list of requirements for Risk Management methodologies for target organisations [41]. Using these requirements organisations can select the appropriate tool for risk management.

A list of established risk assessment methodologies used today is described in the literature [35, 42]. The tools can be fulfil both generic risk management requirements or perform specialised functions. These are compatible with a variety of Information Security standards or industry specific security requirements. We summarise these tools below.

1. CCS Risk Manager
   Symantec developed the Control Compliance Suite (CCS) Risk Manager. This tool is able to group and classify various risk according to key business processes. This helps in the understanding of risk and enables decision making in a business risk environment.

2. EAR/PILAR
   The Environment for the Analysis of Risk (EAR) partly funded by Centro Criptológico Nacional (Spanish National Security Agency) implements and expands RA/RM Methodology. This tool provides both a quantitative and qualitative Risk Analysis and Management tool for organisations.

3. GSTool
   The Federal Office for Information Security (BSI) has developed the GStool. It is a comprehensive tool with the main functionality of supporting the requirements of the IT-Grundschutz methodology.

4. Modulo Risk Manager
   The Modulo Risk Manager from Modulo is another comprehensive tool covering risk for different aspects of business, including both IT and physical assessments. It has a knowledge base with more than 11,000 Information Security controls. It covers areas from IT Governance, Risk, and even Compliance.

5. Proteus
   Proteus Enterprise is a comprehensive web server based compliance, Information Security and risk management, and corporate governance tool developed by Information Governance Ltd. This tool supports both quantitative and qualitative Risk Management in organisations.

6. RiskWatch
   RiskWatch is a Risk Management solution that conducts automated risk analysis and vulnerability assessments of information systems. This tool allows both quantitative and qualitative analyses and includes controls from the ISO 17799 and US-NIST 800-26 standards.

7. RM Studio
   RM Studio is a comprehensive risk management solution. It creates a culture of risk management throughout the organisation by combining Risk Management software and Business Continuity management software. Apart from ISO standards, it also supports IT-Grundschutz.

8. STREAM
   STREAM is a comprehensive risk management tool developed from Acuity. It has a range of functionality enabling management to take informed decisions. Furthermore, its database includes a wide range of Information Security controls for various risk already identified.

Other Information Security Risk Management tools include CORAS, CRAMM, Ebios, FAIR-Lite, GxSGSI, HiScoutGRCSuite, ISAMM, Marion, Octave, SAVe, TRICKlight, vsRisk, etc. [35, 42]. These tools offer a variety of specialised Information Security Risk Management solutions. This indicates a plethora of options available to select for managing risk in an organisation. With each selection, there are different benefits and limitations. This adds to the ambiguity and challenge of what is the best one to use [43]. The choices are not always straightforward and companies usually choose risk management solutions that is the most feasible.

3.3 Summary

Risk Management is broadly classified into Risk Assessment and Risk Control. The Risk Assessment and Risk Control process are structured and well defined in organisations. These processes are capable of assessing, evaluating and developing controls for a wide variety of risk in the organisation. Moreover, the tools described are also able to assess risk horizontally, vertically, and cross-functionally in organisations. It is critical to establish reliable Information Security Risk Management systems because, businesses that fail in identifying the risks associated with the technology they use or the environment where they operate are likely to have a negative impact to their business.

However, the current state of risk management appears to be compliance driven only [43]. The current state of risk management is based on standards since it offers a solid foundation that is widely accepted and practiced across organisations [44]. Furthermore, the risk management tools are implemented taking into account economic and regulatory requirements. Some companies also adopt these standards to meet market expectations and improve their marketing image [43]. Risk management, as a security measure is not yet considered as a top priority in organisations. With the increasing trends of cyber incidents reported [22, 23, 20], this mind set has to change. Organisations appear to be just managing incidents and this current state of incident response in organisation is described in the next chapter.

4 | Current state of Incident Response

In the previous chapter, we discussed the current state of Risk Management in organisations. Various risk controls are adopted after the assessment of risk. Furthermore, to mange this, information systems now include many advanced Information Security tools. However, even with the selection and implementation of state-of-the-art controls based on the results of risk assessments, there are risks that persist and cyber incidents occur. The need for incident response is critical in organisations. Therefore, the ISO/IEC 27035:2011 standard [29], recommends organisations to establish an Incident Response Team (IRT) to manage incidents, described in this chapter.

The incident response lifecycle described in the NIST publication the Incident Handling Guide [24], describes in detail the incident response process. We will now describe the incident response lifecycle in Section 4.1 followed by Section 4.2 describing the teams that manage this incident response process in organisations and the summary in Section 4.3.

4.1 Incident Response Lifecycle

The incident response lifecycle was developed as a guideline for detecting and analysing incidents and then determining the appropriate response to each incident to minimise loss. This is depicted in Figure 3, *Incident Response Lifecycle.* This process is used to mitigate the weaknesses that were exploited and restore the IT services affected [24]. The incident response lifecycle is a structured process for handling incidents. The benefit of such an effective Computer Security Incident Response Capability (CSIRC) is the systematic response to incidents by implementing control measures.

However, the prevalent model of handling incidents within many organisations is an ad hoc approach to security. This is because organisations address the need of security only after a breach occurs [45]. Moreover, these measures adopted to handle the latest breach become the model for future occurrences [46]. Therefore, this Incident Response Lifecycle enables organisations to plan for incident management.

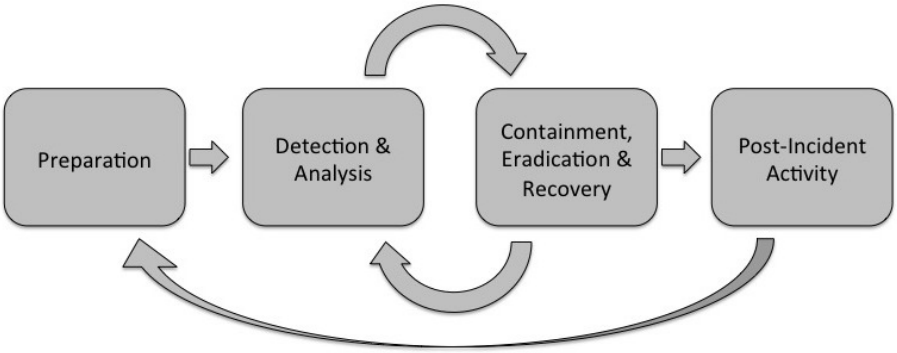


Figure 3: Incident Response Lifecycle [24]

4.1.1 Preparation phase

Cyber security incidents are sometimes beyond the control of organisations, because there is no prior knowledge of where, when and how the next incident will occur. Therefore, the preparation phase prepares the organisation and the relevant members of the IRT before the handling of the incident [47]. This phase helps to prepare the organisation to rapidly respond to incidents. This step is described as the step that precedes the incident response phases in the life cycle. It is a crucial step in incident response. However, in the incident handling process, the subsequent phases are critical because the incident has already occurred. This means that the preparation phase is insufficiently equipped to prevent incidents.

The preparation phase involves not only obtaining the tools and developing techniques to respond to incidents, but also taking preventive actions for the system's security. This process is divided into the preparation to handle incidents and the prevention of incidents itself, described below.

Preparation to handle

This part of the process revolves around enabling the IRT team to handle incidents. This involves developing organisation-wide strategies, implementing incident handler enabling technologies and the preparation of incident response tools. These mechanisms help the organisation to respond to Information Security incidents at the later stages.

The preparation involves the creation of specific strategies to handle incidents. The policy of creation of the IRT team, the mechanisms to be used in the analysis phase, the incident escalation hierarchy, the incident motivation process, the vulnerability and risk assessment process, etc. all form part of these strategies. The tools and resources required for the incident handler are incident handler communications and facilities. For example, contact information for both within and outside the organisation, issue tracking system, incident reporting mechanisms, smartphones, encryption software, etc. The preparation for handling incidents during the later stage will use a variety of incident analysis tools. Therefore ensuring the presence of digital forensic workstations, backup devices, laptops, spare workstations, servers, networking equipment, packet sniffers, protocol analysers, etc. for the analysis of incidents is prepared. This part of the process sets the stage for increased awareness fostering an active security environment.

Prevention of incidents

This step in the process displays proactive security practiced in the organisation. To achieve this, security control measures, are maintained to prevent incidents before they occur. This is reiterated in the objectives of Information Security standards defining the minimum level of security required. With advances in technology, many security tools exist to ensure that a majority of threats are detected and mitigated at the source itself. These include implementing host-based security measures, network-based security measures, end user awareness and training, intrusion detection systems, etc. This is the first line of defence for the organisation. Moreover, the control measures adopted due to risk assessments and best practices from the industry help towards strengthening this step.

If security controls are insufficient, higher number of incidents may occur. However, more controls do not mean better security. The motivated attacker can still use other means to gain access to the organisation's information system and compromise its security. This creates a negative impact for the business. The impact of Information Security failures generally extends to financial loss, reputation loss, etc. which is difficult to recover from.

Therefore its important to have a pre-process that defines the priority of information received, the criticality of information systems potentially affected based on the nature of the threat and vulnerability. This is achieved if a baseline on the level of controls is clearly understood. Ensuring that systems, networks, and applications are sufficiently secure prevents incidents. Therefore, the preparation phase is proactive in adopting many incident prevention mechanisms. With a comprehensive pre-incident process in place, this stage can make a substantial difference to Information Security.

4.1.2 Detection and Analysis phase

This is the second stage of the incident response lifecycle [24]. This stage of the process is divided into two distinct steps. First is the detection of the incident followed by the analysis of the incident.

Detection

This phase of the incident response lifecycle focuses on the determination of the incident from indicators as a source of information. Indicators are described as a sign that an incident may have occurred or may be occurring now [24]. There are many signs to indicate the occurrence of incidents. Incidents are both visible and hidden. The first step is the determination of the incident through the signs of unusual activity. For example, Hacktivist might have defaced the website of the organisation which is visible while a DDoS attack will reduce the flow of information in the network which is not visible. It is important to first detect the incident in order to start the process of analysis and mitigation of risk. The first challenge in this process is the overwhelming volume of information available. This information has to be processed effectively and efficiently.

Many incident detection tools exist. Advances in communication and networking technology have created a wide range of easily accessible tools that can help in the detection of Information Security breaches effectively. For example, network intrusion detection systems like a network tap collects data and flags any suspicious traffic. Anti-spam, anti-malware software are filters between the internal and external network of the organisation. Moreover, advances in technology have given rise to tools that can co-relate data from a wide range of sources. Tools like Security Information and Event Management (SIEM) makes use of cyber intelligence combining information from various sources. There are also a wide range of end-to-end security services and products offered by various cyber security firms. Organisations now create cyber security control centres for managing cyber security incidents. This offers a centralised control to the team handling the incident. However, the detection phase is also described as one of the most decentralised phases, in which IRTs have the least control [47].

Detection of cyber incidents is not easily accomplished because not all indicators are indicative of a security incident. They are also a wide range of other non-security related incident that exists. This includes reasons like the outage of power, disconnected cables, etc. Furthermore, the organisation has to cope with information ranging from overwhelming number of false positives to hidden information [48]. At times, the assessment of a particular event being an incident is sometimes a matter of judgment [24].

However, this phase also shows the critical nature of information. All relevant information regarding the incident itself should be collected. If the organisation has a robust analysis and control mechanism, the information retrieved is used to develop effective controls and create a learning mechanism for future incidents. Therefore, it is important to retrieve information and interpret if its an incident or not. The IRT can then assess the effect of the incident based on business objectives. This is described in next step of the incident response lifecycle.

Analysis

The analysis and inference of the impact of the security risk forms part of this stage in the incident response lifecycle. Based on the incident detected, the impact could be to the Information Security aspects of confidentiality, integrity or availability [33]. Based on the incident, the analysis can throw light on the threat, the vulnerability and the impact. The steps to analyse the incident include the verification of the incident, its analysis and the tracking the source of the incident [48]. For example, the organisation on detecting the incident will move to verify with the help of systems and application logs. The risk to organisation's information systems is assessed and the source of vulnerability is identified. This helps to determine the control failure. Then the appropriate controls are selected according to the risk matrix of the organisation.

This is a problem solving process where the main cause of the incident is identified before action can be taken. Since threats occur from a variety of threat vectors, at times it is impossible to detect the root cause of the problem. Therefore, an initial response is recommended to temporarily mitigate the threat until the vulnerability is identified for further action. With the diversity of threats, a different strategy and control mechanism would be required for each of the threats. For example, a DDoS attack would require the blocking of the IP address affecting the system, while a malware infected system would require the removal of the infected system from the network and its immediate correction. With a dynamic threat and security environment, it is advised to revise the process of Information Security Risk Analysis and update the necessary controls.

A proactive measure for the detection and analysis of potential threats and vulnerabilities would be the implementation of Information Security detection tools with the intention of finding security weaknesses. For example, honeypots detect unauthorised access to systems, pen-testing is an intrusive attack on the system, etc. The various tools used in this phase, are primarily based on being more reactive to changes that are detected to the baseline security posture of the organisation.

4.1.3 Containment, Eradication and Recovery phase

This is the next stage of the incident response lifecycle [24]. In this phase, the organisation will have to contain the problem, solve the problem and take steps to prevent the problem from occurring again. This stage of the process is described as "response" to incidents. The three key methods of response are described as Containment, Eradication and Recovery, enumerated below.

Containment

The process of containment is an immediate control measure initiated after the analysis of the incident. This measure is an early measure to ensure that the incident's impact is restricted and no further damage is allowed. For example, containment measures include immediate shut-down of information system, disconnecting infected systems from the network, access-right removal, etc. These measures are determined by policies in the ISRM plan. The risk level determines the strategy adopted.

A delay in containment strategy is dangerous to the organisation because an attacker could further compromise other systems [24]. With the diversity in threats and changing security environments, the process of containment should be clearly know to the IRT. If ad-hoc teams handle the incident, it could lead to the creation of further risk. Another potential risk of containment is the chances of additional risk on containment itself. This requires a clear understanding of risk. Thereby, reiterating the previous requirement of the necessity of a prior ISRM process in place to determine the appropriate controls for potential risk.

Eradication

This is the process of eliminating the threat in the information system by the identification of all affected hosts and remedial action [24]. Examples of eradication include removal of malware from the infected systems, disabling breached accounts of users, etc. In some cases, eradication may not be necessary. This is because the incident may only require a containment action and is resolved through the recovery process.

Recovery

Recovery is the process wherein the IT system administrator restores the information system to normal operation and confirms its normal functioning [24]. For example, restoring the system to a pre-incident state from backups, installation of software patches, updating user passwords, etc. Recovery involves the implementation of control measures, which could vary from the implementation of new policies to tightening of security controls. However, there is risk in the long recovery time needed after the incident itself. For example, the data breach that occurred at Target required the organisation to offer credit-card fraud protection plan up to a year after the incident [49]. This creates a long and expensive recovery process for the organisation.

While the process of containment is an immediate response to the incident, the eradication and recovery focuses on long-term control measures. Thereby, the process creates a valuable learning experience and has to be documented and reused to prevent future incidents. This information can also be shared between other organisations proactively.

4.1.4 Post-Incident Response phase

The final phase of the incident response lifecycle is critical to a continued learning and improvement curve in the organisation. This process is often neglected in organisations [24]. Every incident that occurs has an impact on the organisation. Small incidents with limited impact that occur via previously recorded threat vectors are easily resolved through appropriate control measures. However, incidents performed through new attack methods are of widespread concern and interest and cause new security processes to be developed and implemented across the organisation [24]. For example, the Heartbleed vulnerability, created the process of changing passwords as a control after its occurrence [8]. This provides valuable insight not only to one's own organisation but also a valuable source of information to other organisations if the information is shared.

Part of the post-incident handling phase is to have a structured recovery plan and an implementation procedure. This is in compliance to the Information Security Standard implemented. The ability to reuse the information learned during the incident response phases to prepare for future incidents can determine the organisation's preparedness towards cyber incidents. With each incident, the organisation can learn something. New threats, discovered vulnerabilities, improved technological solutions and team dynamics, all add to the knowledge base. Therefore, this phase directly leads to the preparation phase of this incident response lifecycle and works towards incident prevention.

4.2 Incident Responders

Even with advances in Information Security in information systems, people are still required to take decisions and manage incidents. Section 4.2.1 describes the requirements of IRTs. A brief summary of the kinds of IRTs is described in Section 4.2.2 followed by the role played by the team during the lifecycle of the incident in Section 4.2.3.

Information Security permeates every aspect of the organisation and is a multi-faceted discipline [47]. People across the organisation like IT administrators, technical and security experts, legal counsel, human resources personnel, top-management, end users, etc. are involved in some way during the response to an incident. Moreover, with the Information Security aspects of integrity, confidentiality or availability of the information affected [33], various stakeholders across the supply chain and customers are also affected. For example, during the Target data breach, people involved included those that investigated the incident both from within and outside the company, the millions of customers affected by the data loss, teams assisting these customers, others responding to the media, top-management taking decisions, legal experts, etc [49]. All these people that work towards the goal of handling incidents are described as incident responders. Prosise & Mandia (2003) describes the team handling the incident as a Computer Security Incident Response Team (CSIRT) [47], or simply Incident Response Team (IRT) in this research.

4.2.1 Requirements of Incident Response Teams

This section of the research will discuss the requirements of an IRT. A wide variety of resources and skills has to be available in the organisation to adequately respond to incidents. Incident response is considered a critical security function in the organisation. This team aims to manage incidents in a timely and cost-effective manner [50]. Both the individual team members and the skills they possess are important elements in an IRT. The IRT can vary from a single person to a team that consists of a team leader, a technical lead and other support staff [24]. The skills and expertise needed by members of the IRT are described below.

Team leaders are generally from a management perspective and are required to be able to defuse crises, liaison with stakeholders and possess excellent communication skills. They should be able to communicate to a wide range of audiences. Prior incident response experience is an added advantage. The team leader should be able to take decisions or have the ability to ensure quick decisions are taken during the handling of the incident.

The technical lead is expected to have experience managing incidents apart from general computer security related knowledge. These include technical system administration, network administration, programming, technical support or intrusion detection skills. Depending on the severity of attacks, system specific or application related skills with in-depth understanding of technologies involved would be an added advantage.

Handling of computer related incidents often require professionals who understand both the technical and incident response aspects of incidents [50]. However, it is not always possible to have the necessary technical skills within an organisation. Organisations have to rely on specialist from outside for the management of its Information Security needs. The organisation can either outsource its entire security operations to external security vendors or a part of the incident response process.

Personnel from non-IT related functions are also required. These are stakeholders who are not directly involved in the management of incidents but whose input is important. Human resources personnel, legal counsel, communication advisors, business managers, end users, help desk workers, and other employees may find themselves responding to incidents [47]. For example, the legal counsel assists in determining the liability of the organisation to a particular incident and helps to determine the best course of action to be taken according to the law.

The creation of an IRT is at the core of the incident response lifecycle. This team enables the organisation to effectively manage Information Security incidents. With increasing complexity of incidents, these teams often require specialist skills to manage incidents. Furthermore, the team has to regularly update their skills to meet the dynamic changes seen in information systems. For the effective management of incidents, there are various IRT models setup, described in the next section.

4.2.2 Kinds of Incident Response Teams

This section describes the different IRT models. The structure, size, geographical distribution, complexity of IT operations and connection with the location of the organisation key information systems play a role in the selection of the IRT model. Killcrece et al. (2003) describes the following five models [51].

1. Security team
   The security team is an ad hoc team. There is no formal selection of members for this team. Being a reactive team, the team constitutes of members best suited and available to handle the incident. This model exists with little to no coordination. For example, in a small organisation during the event of a DDoS attack, the system IT administrators are responsible to handle the incident. The security team's function is to return the systems to normal operation status as soon as possible [51]. With a lack of long-term vision and problem solving focus, this model is not suited as a proactive method to handle incidents.

2. Distributed team
   The distributed model makes use of a formally recognised team within the organisation to handle Information Security incidents. There are defined policies, procedures and processes that this team adheres too. However, the team is not composed of members exclusively for the handling of incidents but comes into effect during the course of incidents. Killcrece et al. (2003) describes multinational corporations, government organisations, educational institutions, etc. as most likely to have a distributed team to handle incidents [51]. The advantage of such a team is the broad base of expertise that it has and the ability of the team to promote good security practices across the organisation. This limitation of this team is that members apart from preforming their routine jobs are also required to perform incident response related work. Therefore, the team's effectiveness depends on the ability of the team to handle incidents simultaneously. Moreover, the lack of coordination between different teams is a challenge during the handling of incidents.

3. Centralised team
   This centralised team is a dedicated team utilised to handle Information Security incidents in the organisation. The team constitutes of full time members whose task is to handle incidents. Killcrece et al. (2003) describes small organisations with a centralised IT department most likely to adopt this model [51]. Other examples include educational institutions, military or government organisation, etc. This model has the advantage of a centralised system and is best suited as a proactive response team. However, the team runs the risk of not able to handle incidents with diverse requirements from individual departments across the organisation. The

limitation is the need for specialised support in instances of directed attacks in specific areas of the organisation. Moreover, the local teams might lack the expertise to handle unknown and sudden threats. With interconnected networks, the organisation could run the risk of not responding effectively to Information Security incidents at a different functional area of the organisation. There can be overlap in functions and tasks that create challenges during a coordinated attack against the organisation.

4. Combined distributed and centralised team
   This model is a combined approach of both the distributed and centralised approaches to incident handling. A centralised team is formed that coordinates between various team members distributed across the organisation. Killcrece et al. (2003) describes the centralised team as one offering high-level analysis and recommending control measures [51]. The distributed teams in this case are responsible for implementation of risk mitigation strategies. Each individual team is divided by business operation, market segment or even geographical location. This is an effective way for large organisations to manage Information Security incidents. It maximises the use of support staff across different areas of the business while using a central team as a strategic advisor. This model combines the limitation of coordination from the distributed team with the lack of organisation wide expertise in the centralised approach and converts it into strength for the organisation. Therefore, this combined model offers a clear mechanism for proactive incident management.

5. Coordinating team
   This IRT is described as offering advice to other decentralised teams. This team performs the functions of vulnerability analysis, support, coordination, etc. This response team is an advisory team providing advice, warnings, and recommended mitigation and recovery solutions. For example, multinational corporations might have different entities having own IRTs. Here the use of a coordinating team is useful in the handing of incidents. A common example of a coordinating team is the CERT Coordination Centre (CERT/CC) which performs the task of proactive analysis of Information Security threats. The main drawback of such a team is that the IRT has no authority over the distributed teams. Its task is merely to recommend actions.

The analysis of the five models shows how organisations respond to Information Security incidents. We see that depending on the nature of business operations, different teams are set up for handling Information Security incidents. However, the nature of threats is diverse and dynamic. Most security teams are formed as ad hoc teams once an incident has been detected [50]. It is important to realise that there is uncertainty in organisations during a cyber incident, because risk is described as a combination of possible consequences and associated uncertainties [52]. Therefore, a structured process is recommended as a best practice to manage incidents [51].

4.2.3 Role performed by Incident Response Teams

After understanding the structure of IRTs in organisations, this section describes the main tasks performed by the IRT. All tasks performed by the IRT are classified into the following three main areas described in the research of Kossakowski et al. (1999) [45].

Preparing

This step of the process involves the preparation actions performed by the IRT. This includes activities from understanding the functional requirements to be performed by each member of the team, the selection and familiarisation of the various tools, procedures and policies for responding to various intrusions and the preparation to respond. The process described in the preparing phase is driven by the need to manage incidents. The team's perspective on Information Security is towards reactive measures to threat and vulnerability information. With the uncertainty in information, this reactive perspective is justified as a means to manage incidents. However, this does not prevent incidents and a more proactive approach is required.

Handling

This function is the act of analysing the incident and the implementation of various security controls to mitigate the risk. It also involves the communication between stakeholders during the incident and collecting information to update the policy, process and procedures. This part of the process is reactive and focuses in returning the organisation to the normal state as soon as possible. The IRT is a dedicated team that manages incidents. However, the team is not responsible for incident prevention [24] and is a gap in the management of Information Security.

Follow up

This process involves the key aspect of learning from the incident. The organisation can temporarily harden security controls in information systems to address risk at that time. However, they have to update its Information Security policies and procedures as well [51]. Moreover, the process can also design and implement an improved incident tracking system [53]. These steps enable the organisation to learn from the incident. However, this team focuses on offering recommendations and implementing technical controls only [50]. With a robust learning process, the organisation's Information Security practices have to improve and become more efficient. However, this process still has a gap in incident prevention.

4.3 Summary

This chapter describes the current state of incident response as a comprehensive process. The incident response lifecycle describes the entire process followed after the detection of the incident in an organisation. The information learned as a result of the incident response lifecycle is used to improve Information Security controls, however, we argue that this is insufficient. The use of primarily indicators as a source of information in the detection phase is a limitation towards effectively preventing incidents. Therefore, the preparation phase of the organisation has a tremendous scope to be more proactive towards Information Security.

We then discussed the various types of incident response teams managing incidents. Incident responders are described as skilled resources within the organisation however, should the need arise external expertise is also used to manage incidents. However, the focus of the Incident Responders in the entire lifecycle is on managing incidents. There should be a forward-looking approach adopted by incident responders during the incident response lifecycle. Therefore, the preparation phase is best suited to address this gap.

In the following chapter, we describe the alignment of Risk Management and Incident Response to arrive at the requirements for the design of a proactive process.

5 | Aligning Risk Management and Incident Response

The previous Chapter 3 & Chapter 4 describes the current state of Risk Management and Incident Response in organisations today. These are two widely used methodologies adopted by organisations to address its Information Security issues. However, we notice limitations in these two processes, because of the increasing occurrence of cyber incidents [22, 23]. Information systems are complex socio-technical systems; and the addition of ensuring Information Security principles of confidentiality, integrity and availability creates a challenging environment in the organisation for those responsible to ensure Information Security.

An approach to analyse and design a solution in socio-technical systems is by using TIP design perspectives of Technical, Institutional and decision Process to assess socio-technical systems [32]. In this chapter the current state of Risk Management and Incident Response are analysed from these three perspectives. It is a systematic, design-oriented way of analysing the current state of organisation's Information Security. Section 5.1 describes the Technical perspective, Section 5.2 describes the Institutional perspective and Section 5.3 the process perspective of the current state of Risk Management and Incident Response. Section 5.4 will describe the stakeholders a crucial step in the design of any process followed by the summary of requirements in Section 5.5.

5.1 Technical Perspective

The technical artifacts are the Risk Assessment tools described in Section 3.2, CCS Risk Manager, Modulo Risk Manager, CRAMM, etc. to name a few. These tools are developed based on the Information Security Risk Management (ISRM) process [17]. The main steps are identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. Organisations need to make trade-offs from the perspective of financial, resource utilisation, compatibility, etc. to implement these tools [43], therefore the benefits of the process is not fully achieved.

The Incident response team also uses a variety of incident response tools to carry out the activities during the incident response lifecycle. In the preparation phase the technical artifacts are incident handler enabling technologies and tools to detect and prevent known threats. In the detection and analysis phase, there is a variety of sophisticated Network Intrusion Detection Systems, anti-spam and anti-malware software, security information and event management tools, etc. [24]. Each tool performs a specific sub-function in the process of incident response after the detection of the incident. Therefore, with the plethora of tools available in the market, the organisation can make use of technology already deployed. This brings us to the requirement of **"use of implemented tools"** which will enable the organisation to easily adopt the design solution suggested in this research.

The incident response team (IRT) retrieves information shared about incidents but, even after this, IRTs fail to react to information [54]. This is because the focus of IRTs is on incident response and its contribution to incident prevention is to provide advice [24]. It provides recommendations on practices for securing networks, systems, and applications; risk assessments; and user awareness and training. However, the access, retrieval and interpretation of information are important aspects of incident response. Indicators and precursors are used as a sign to detect incidents [24, 55].

Precursors are relatively rare, while indicators are easier to detect [24]. The partial or lack of complete information is a major hurdle that the incident response team faces. Sophisticated incident detection and assessment tools are available in the market to interpret the information. Nevertheless, threats and vulnerabilities continue to be undetected in many cases because only indicators are used as the source of information in the detection and analysis phase; thereby creating the requirement of *"the use of precursors as information sources"* to strengthen the process of incident response. Precursor is defined as a sign that an incident may occur in the future [24] and is not yet considered proactively in incident response. This is further elaborated in Chapter 6.

Furthermore, information that does not necessarily affect the organisation directly, still needs to be investigated and monitored for potential risk. Cyber incident information is shared using Cyber Security Reporting System [56]. The final phase of the Incident response lifecycle focuses on reporting of information and is part of the continuous feedback loop in organisations. This acts both as a retrospective measure internally and as a predictive measure to other organisations if the information is shared externally. Therefore, **"using the information from external organisations"** can strengthen the process of incident prevention.

5.2 Institutional Perspective

The following section describes the Institutional analysis of risk management and incident response based on the four-layer framework of Williamson (1998) [57]. The framework is an approach to describe social and institutional arrangements in an integrated fashion [32]. Each level operates at its own pace, protected from above by slower, larger levels but invigorated from below by faster, smaller cycles. This framework allows for liberty in the analysis of separate layers, thus a multi-layer system can be described that shows both bottom-up and top-down causation. According to Koppenjan and Groenewegen (2005), the Williamson's four layer model is relevant because it distinguishes between different layers of institutions [58].

Level 1: Actors and Interactions, describes the actors and their interactions in socio-technological setting [58]. There are various actors directly and indirectly involved in risk management and incident response [51, 59, 60]. The actors interact with complex information systems in cyberspace[2]. IRT's carry out the function of ensuring Information Security by following the various steps as described in the incident response guide; while the management is responsible for ensuring that risk management activities of assessment and control is carried out appropriately [17]. The interactions of these actors are guided by these processes since incidents create an uncertain environment in which decisions have to be taken.

Level 2: Institutional arrangements, describes the formal and informal institutional arrangements of these socio-technologi-cal systems. This includes covenants and contracts, but also informal rules, codes and norms [58]. The National Institute of Standards and Technology (NIST) published the Computer Security Incident Handling Guide [24], describing the process followed by Incident Response Teams while the Risk Management Guide for Information Technology Systems [17], describes the risk management process. Each step of the Risk Management and Incident Response process helps the organisation to achieve compliance to standards described in Level 3.

[2] Cyberspace is defined as *"the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"* [61]

Therefore the compliance helps to promote customers trust by verifying the fulfillment of well-known and accepted international standard [62]. Furthermore, industry specific security checklists like Checklist security of ICS/SCADA systems [63] are used. The technical artifacts described in Section 5.1 are implemented by external security vendors based on service level agreements signed by both stakeholders.

Level 3: Formal Institutional Environment, describes the formal institutional environment; the formal rules, laws and regulations [58]. The ISO/IEC 27000, 27001 and 27002 are Information Security Standards for the protection of the information and information systems [44]. ISO 27005:2011 standard is an Information Security Risk Management standard [28], while ISO 27035:2011 standard is an Information Security Incident Management standard widely adopted in organisations [29]. The standards specify a security baseline that the organisation should achieve and offers guidelines in achieving it. Furthermore, strategies like *National Cyber Security Strategy 2* of the Netherlands [64], Articles 30, 31 and 32 of the Data Protection regulation from the European Union [65], etc. show that cyber security is gaining prominence internationally in both public and private sectors. Therefore, this indicates that at an institutional level these formal rules, laws and regulations contributes to the awareness of Information Security in organisations today.

Level 4: Informal Institutional Environment, describes the informal institutional environment, these are the norms, values, orientation and codes [58]. Information Security is not yet at the forefront of priorities in the organisation. It lacks the full support of top management [44, 66, 20]. The organisational culture has a large part to play here [67]; thereby the norm of organisation wide proactive Information Security awareness has to still develop. This can be compared with the culture of safety in organisations, which has significantly more support from the top management [68]. However, the management focuses on the importance of an incident recovery plan in the event of a security breach [25]. If a high-impact security breach affects the organisation, the seriousness of its control measures are brought to the forefront of organisational priorities. For example the Target and Home Depot data breaches has shown the importance of two-factor authentication at the Point of Sale (PoS) system at retailers. Therefore, the requirement of **"top management support"** is critical to the success of any process.

The four layer institutional model by Williamson (1998) also explains the relationships between the various layers [57]. Even though, Incident Response teams described in Level 1 uses the various Information Security tools described in Level 2, which are implement to be complaint to Information Security standards described in Level 3, it is selected based on trade-offs between constraints and requirements of the organisation. Organisations are limited by labour, financial, expertise, and other resources necessary to implement such comprehensive tools based on these standards [43, 69]. The decision is influenced by the norm that Information Security risk is not likely to affect them and hence not a priority described in Level 4. Therefore, the culture of **"proactive Information Security awareness "** has to be fostered through the process in order to notice changes across all institutional levels.

5.3 Process Perspective

The function of achieving Information Security is effectively accomplished, when the Risk Management team performs the Risk Management process [17]; and the Incident Response team makes use of the process described in the Incident Response lifecycle [24]. Therefore, the Technical (T) and Institutional (I) artifacts[3] described earlier are structures when implemented together with a context, produces the Process (P)[4] that performs the intended function of the artifacts [32].

The output of the risk assessment and incident response process is to reduce risk in the organisation. The risk level determines the extent to which organisations are willing to absorb risk; thereby determining risk control measures [17]. However, we see that the control measures adopted are backward-looking; because of the focus towards incident response. Often, these controls measures fail because of the following two aspects.

Lack of implementation

Information Security controls are not implemented because the perceived benefit of Information Security does not justify the high cost of implementation [71]. The investment in right controls is not for the information sets with the highest vulnerability but for information sets with midrange vulnerabilities [72]. With trade offs being made, organisations run the risk of not having invested in the right security controls.

At times, implementation of controls measures is postponed until it is too late [44]. This indicates that Information Security is not a top priority, because it lacks the full support of top management [44, 20]. However, we see that both private and public organisations, and even individuals are equally susceptible to cyber incidents, therefore, the requirement of **"top management support"** is further advocated.

Failure in implementation

The complexity in information systems means that controls have to be implemented correctly or else failure leads to a less secure system, thereby increasing risk to frequent and damaging security breaches [73]. This is a process failure and has to be addressed by the management.

Even in the presence of controls, information systems are not fully protected because of inherent control weaknesses [74]. Therefore, the incident response process is crucial to ensuring that organisations manage these risk. Organisations respond to incidents by tightening security controls [75]. The tightening of security controls does not indicate greater security, because, once a resource is successfully attacked, there is a high probability of a similar resource being attacked again [24]. Therefore we can conclude that if this information is available to organisations, they can proactively use the information to update its security controls and change its risk posture. However even with various information sharing mechanism in place [54], the control measures are not adapted to the risk. There is lack of appropriate implementation strategies [76], thereby creating the need for **"a forward-looking process"**.

To achieve the overall function of Information Security Risk Management, there are many sub-processes each contributing to achieving the functions of each activity described in the Risk Management and Incident Response process. However, achieving the objectives of each function is not easy, because even with the adoption of the risk management perspective it does not drive the level of security risk to zero [77]. Residual risk still exists, regardless of the action taken [78]. For example. Windows recently detected and fixed a 19-year-old bug in its system [79]. This shows, that even software vendors, in operating system software that undergo wide testing before being

[3] An IT artifact is an entity/object intentionally engineered to benefit certain people with certain purposes and goals in certain contexts [70]

[4] The TIP design model is summarised as A + C = P, described as *"any engineered artifact A is a structure that, together with the context C in which it is implemented, produces a process P that performs the intended function of A"*

released, also have vulnerabilities. The same risk exists in any off-the shelf software. Moreover, these softwares are implemented in other organisations each having diverse information systems. Furthermore, vulnerabilities in the process as well contribute to creating an opportunity for attackers to target the organisation. Therefore, organisations have to be vigilant to any information regarding its Information Security status.

Let us assume a risk control process to determine the characteristics required. Ensuring updated software on information systems is a control measure of risk for targeted attacks using known vulnerabilities. Software vendors constantly provide updates to vulnerabilities detected in earlier versions of the software. Organisations need to regularly update their information systems. Since the risk assessment and risk control process is not carried out frequently, there exist a risk of controls failing, if the organisation fails to update its software. Vulnerabilities are most often exploited only after a security update is available [80]. Therefore, this creates a requirement to carry out the risk assessment and risk control process more frequently. However, the risk assessment process consumes time and resources in the organisation where it is implemented [81]. Therefore, there should be **"an agile risk assessment process"** designed to ensure that the risk assessment is performed at least on the information systems that is vulnerable, or run the risk of having insufficient controls.

The incident response lifecycle offers a structured process for IRT to respond to incidents. This means that Incident Response is initiated only after an incident is detected. The prevention process in the preparation phase of lifecycle fails to prevent incidents even with prior information available. Both the technical and institutional artifacts only prepare the organisation for maintaining a minimum level of security. However, there is no process to proactively prevent incidents. Therefore, with **"the design of a proactive incident prevention process"** we can change the perspective of how organisations view information, thereby improving its Information Security awareness.

5.4 Stakeholders

A stakeholder analysis is a crucial step in the design of any process. Cyber incidents involve various internal and external stakeholders. These actors and their interactions create a challenging environment that has to be addressed. Each organisation has stakeholders who interact in their own unique way with the information systems. By focusing on Risk Management and Incident Response, we see that there are many stakeholders involved. Organisations manage incidents with the help Incident Response Teams. The analysis of the various kinds of incident response teams shows that the requirements for IRTs are diverse [51]. Furthermore, setting up these teams is a challenge with diverse requirements. The kinds of IRTs and the role performed by these IRTs were described in Section 4.2.

This analysis of requirements of incident responders identifies that the skills and expertise of the members of the IRT are crucial to the team's success. Furthermore, there is a high demand for very detailed knowledge about the IT security domain and the actual company environment [82]. The IRTs consist of internal stakeholders who include team leaders, technical experts and process experts. Other internal stakeholders include legal experts, communication advisors, end-users, etc. External stakeholders include both technical and process experts from outside the organisation. Furthermore, the media, customers, supply chain vendors, etc. are external stakeholders. The attacker can also be considered as an external stakeholder [83]. Therefore, we see that the design and set up of IRTs are comprehensive and detailed.

The analysis indicates that even though Information Security Risk Controls fail at times to achieve its goals, Incident Response teams are set up to manage incidents. IRTs are reactive in nature and are implemented once an incident has affected the organisation. However, even with limited resources and capabilities, there is a response mechanism in place. This is valuable in meeting the Information Security needs of the organisation. More advanced IRTs tend to adopt a proactive role, seeking out vulnerabilities before they become incidents [59]. They provide advice and educate employees on Information Security matters [51]. The preparation phase in IRTs includes preventive measures as part of the process but is insufficient. Therefore, **critical stakeholders should be identified from IRTs** in order to engage them to collaborate for the prevention of incidents more actively.

5.5 Summary of Requirements

If organisations are ISO certified then we can assume that minimum compliance mechanisms of risk management are in place. This includes Risk Assessment, Risk Control and the Incident Response Team.

The incident response process was developed to assist organisations to efficiently and effectively respond to incidents after they have been detected. Nevertheless, if information is available before the incident is detected in the organisation, it should be used to prevent incidents. At times, there have been indications of potential threats or vulnerabilities. However, no team exists to react to this information. Therefore, organisations should establish an incident prevention team that reacts to this information and to perform incident prevention process using this information available. Since the present prevention process described in the preparation phase of the incident response lifecycle is insufficient and the IRTs are not equipped to manage this aspect of prevention, the Incident Prevention Team (IPT) offers a unique solution to the problem disscused.

The technical and institutional artifacts are interdependent and contribute to the decision making process of risk management and incident response. We see, the formal institutional environment (Level 3) of the Information Security Standard, specifying the need for implementation of risk management and incident response tools (technical artifacts). These tools have various steps that are defined by institutional arrangements (Level 2) and carried out by the respective teams (Level 1). With a proactive approach, an Information Security awareness culture (Level 4) can be created in the organisation. Therefore, the process of incident prevention should have the following functional and non-functional requirements that were generated from the TIP design analysis.

- Functional Requirements
  - Use of precursors as information sources
  - Using information from external organisations
  - Team should be consist of members from incident response teams
  - Use of implemented tools
  - Agile risk assessment process
- Non-Functional Requirements
  - Proactive Information Security awareness
  - Need for top-management support

Therefore, the requirements for the establishment of the Incident Prevention Team will build on the established Incident Response Lifecycle and extend the preparation phase. This will ensure that organisations do not have to reinvent the wheel but at the same time, address the lack of focus given to incident prevention. In the following chapter, we will discuss, the various ingredients based on these requirements for the process of incident prevention.

Part III

Design

6 Ingredient 1: Precursors

The research in Part II, describes the primary focus of organisations towards incident response mechanisms. In Chapter 5, we describe the various requirements that research still need to address. With increasing cyber incidents, a method for organisations to use information to prevent the incident itself is considered apt to address the gap.

In order to transform raw information into value to the business, organisations have to ensure its availability and reliability. Powerful advances in communication and networking technology, development of software, sensors and other tools can ensure real time availability of a variety of information. This information is used as a strategic advantage to the organisation. However, decision makers cannot take strategic decisions with partial information [84]. This is especially true with incident information where an attacker tries to hide all traces of information related to the attack. As seen in Chapter 5, organisations have to rely on information detected after an Information Security incident has occurred. Therefore, to improve the current state of security, this research focuses on information not detected in the organisation but still available in the form of precursors, hence helping to bridge the research gap. The challenge is to differentiate between precursors and indicators, and is described in this chapter.

In Section 6.1 we describe the two kinds of information that are used to classify incidents based on the time the incident is detected in the organisation. This research focuses on precursors. In Section 6.2 we describe the two perspectives of precursors followed by the sources of precursors in Section 6.3. This is followed by a discussion on why precursors benefit the incident prevention process in Section 6.4. Finally the main lessons learned from this chapter is summarised in Section 6.5.

6.1 Types of Information

From the perspective of Information Security incidents in organisations, the information are categorised according to the following two types.

1. **Indicators**
   Indicators are a sign that an incident may have occurred or may be occurring now [24]. Indicators are alternatively described as lagging indicators or coincident indicators [85]. It is information that indicates the security condition of the system being assessed with respect to a security baseline. This information is obtained from tools like anti virus software, malware detection systems, network intrusion detection software, etc. The network administrator themselves can notice unusual deviation from typical network traffic flows or see filenames with unusual characters. This information triggers an incident response process in the organisation. Therefore, indicators are inputs for Information Security Risk Management [55].

2. **Precursors**
   Precursor is a sign that an incident may occur in the future [24]. The research reviewed

also describes it as leading indicators representing the security state of the system before the occurrence of the incident [85]. For security practitioners, the identification of precursors before the incident would be an ideal case of Information Security. They would be able to pre-empt an incident from occurring by altering the security control measures according to the risk assessment.

By looking internally at the vulnerabilities, organisations can assess its own risk according to this precursor. However, the interpretation of precursors from an attackers perspective remains a challenge even with the current advances in technology [24]. This is because there are various factors motivating an attacker. Research also indicates that precursors are obtained by looking externally, described in Section 6.3.

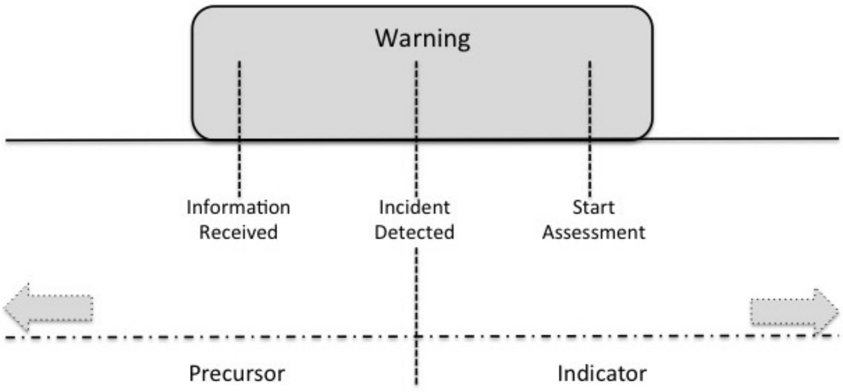


Figure 4: Classification of Information, derived from [83]

The distinction in the classification of incident information is clearly illustrated in Figure 4, *Classification of Information*, [83]. An incident lifecycle is described in six stages of a crisis model [86]. This includes the warning phase; followed by risk assessment, initial response, management, resolution and recovery, and learning. Here information plays a critical role across the six stages. However there is a very clear distinction between when information is considered as a precursor and as an indicator. The generic incident notification timeline start only once the security incident or *"indicator"* is confirmed and recorded in the system [83]. This is the time between the detection of the incident and the start of the risk assessment process. The time between receiving information and detecting the incident is used to define information as a *"precursor"*. The early notification, detection and interpretation of information not affecting the organisation are inputs for incident prevention. The next Section 6.2 will describe the perspectives according to which precursors should be considered.

6.2 Precursor Perspectives

This section will describe the two distinct perspectives according to which the information defined as precursors are analysed.

1. **Source of Attack**
   Precursors viewed from the attackers' perspective are described as the source of attack.

Organisations often struggle to assess threats accurately. This is because the motivation of the attacker is not known. The *"why"*; *"who"*; *"what"*; and *"how"* of the attack is known only to the attacker. They are influenced by a number of factors enumerated below.

- Based on the *"why"*
  Liu and Cheng (2009) [87] describe the why as a combination of software bugs, configuration defects and design flaws that leads to vulnerabilities in the organisation. This in turn leads to exploits and breaches.
- Based on *"who"* the attacker is
  An attacker can be inside or outside the organisation [87]. Insiders are generally disgruntled employees witnessed in the Maroochy cyber incident [88]. Outsiders are individual hackers, organised crime groups, hacktivists, national governments, etc. [89, 83].
- Based on *"what"* the attacker is after
  They are motivated by personal, financial, ideological interests or state interests [83]. Apart from the motives, the means to carry out an attack and the opportunities that exist are strong factors that contribute towards cyber attacks taking place [87].
- Based on the "how"
  Attackers use a variety of tools to target organisations. They conduct reconnaissance, scan targets and after foot printing, exploit vulnerabilities [87]. The threat vectors are diverse and it is not easy to completely protect oneself.

Organisations are ill equipped to protect itself from a highly motivated attacker. With a wide range of combinations of attack possible, the motivation of attackers is beyond the scope of the organisation's Information Security Risk Management practise. However, using the information already available, this offers a field-tested analysis of threat that affected another organisation. This means the precursor here is a cumulative analysis of risk on another organisation. Thereby value is derived from this information.

For example, let us consider the example of Target data breach. The information retrieved is the attacker using BlackPOS Malware as a threat vector propagated through the Point of Sale (PoS) system. A similar organisation using this precursor can actively monitor for possible malware affecting the Point of Sale (PoS) system, thereby reducing its risk. However, we see that a similar data breach via the same threat vector affected Home Depot.

In this example, it shows that Home Depot could have learned from this precursor about the data breach at Target. Similarly, one can utilise information about incidents in other organisations to derive value for itself. Information about the threat, its propagation and intended targets can instigate a review of ones control measures. It is important to note that the motivations of the attacker might be different. Organisations are targeted for reasons that are not directly related to its impact. For example, hacktivists are motivated by different causes. Therefore, an incident in another organisation may not necessarily materialise in your own organisation. However, using precursors your organisation would have raised its overall security awareness with the information.

2. **Target of Attack**
   Precursors from the target organisations point of view are vulnerabilities in the IT environment. Vulnerabilities inherently exist in every organisation because of the complexity of

interconnected systems, technology, process and interaction with people. With new technological advances and its adoption in business, there exist more vulnerabilities waiting to be exploited. For example, the integration of BYOD (Bring You Own Device) in the workplace creates potential security vulnerabilities. The IT department has to manage many operating systems, applications, unique number of devices, etc. that increases risk to data integrity. This is because information is accessed by devices not managed by the IT department [90].

Information on vulnerabilities in information systems are readily available. This information is retrieved both externally and internally. Alerts and security notifications are external sources while risk assessments are internal sources for the organisation. The information on vulnerabilities is within the control of the organisation, as compared to information from the source of the attack, described earlier. This is because precursors as vulnerabilities indicates a weak control in the information security environment and the organisation has the ability to change security control measures based on its risk appetite.

For example, let us consider the Heartbleed bug in the OpenSSL cryptographic software library. The notification of this security vulnerability prompted operating system vendors, appliance vendors, independent software vendors, etc. to offer a fix [8]. With this vulnerability, the organisation using the affected OpenSSL service was at risk for data leakage. IT administrators can mitigate this risk by updating its affected systems proactively. However Community Health Systems Inc. suffered a data breach that was exploited via this bug [91].

The above example shows that control measures are strengthened depending on the likely impact of risk. However, a proactive process of assessing risk based on the information of vulnerabilities has to exist in the organisation. These precursors need to be effectively utilised in the organisation's risk assessment process. This is also because there can exist vulnerabilities that may not be know to the attacker. This increases risk since attacks gradually increase with time after a patch release [92, 80]. Therefore, a proactive process towards risk assessment can create the difference between a successful attack and a secure IT environment.

6.3 Precursor Sources

With an understanding of the two distinct perspectives of precursors in Section 6.2, this section will now focus on the how we can obtain this information in our organisation. Organisations have to proactively address cyber incidents and precursors are a source to achieve this goal. Therefore, active scanning of the environment is critical, and the focus should not be in obtaining information from traditional sources only [93, 94]. There are various sources of precursors [24]. However, for the sake of simplicity, the sources are categorised as follows.

1. **System generated**

   System generated sources of precursors are alerts and logs of the system information. The value obtained by this information depends on both the effectiveness of tools and users interpretation of the alerts and logs. For example, these alerts are obtained from intrusion detection and prevention systems, anti virus, anti malware software, etc. File integrity software logs can detect changes to systems and application files. Others include operating system logs, service logs, application logs, network logs, etc. Logs are a rich source of input from the information system and describe the state of the system at different times.

All notifications of potential threats have to be assessed and evaluated in the IT environment. This process is time consuming. By not reacting to the alert from the system, organisations are allowing it to be open to risk. For example, the report on the Target data breach indicates that the security team did not react to the alerts by its malware detection system [49]. This created the environment suitable for attackers to infiltrate the system. Another challenge faced by IT administrators is the interpretation of false positives. With a high number of false positives, the effectiveness of the overall process is affected. This becomes an uphill challenge for IT administrators with the large volumes of information generated by the system.

System generated information already exists in organisations. This information has to be effectively utilised to achieve a secure IT environment. The development of sophisticated tools and automatic alert mechanisms are enabling organisations to be more secure. However, organisations have to react to these alerts and develop the necessary skills to interpret the information. This proactive approach is a measure that would prevent Information Security incidents from occurring.

2. **Public available information**

   There is a wide range of information available in this category. The most common source is government Information Security vulnerability alerts. These include alerts posted by the national vulnerability database (NVD), UK-CERT, US-CERT, EISAS, etc. Computer Emergency Response Team's (CERT) was created with the goal of sharing vulnerability information in an attempt to help administrators better protect their systems and networks [54]. For example, announcements of the Heartbleed (CVE-2014-0160) and Shellshock (CVE-2014-6271) vulnerabilities via the National vulnerability database website is an active public data source of vulnerabilities [95].

   Other sources of information include reports and trends provided by various security firms [23], independent security consultants [96], etc. They provide inputs on the vulnerabilities and threats after having analysed the information in detail. For example, both Google's security team and Codenomicon first reported the recent OpenSSL bug named Heartbleed, independently [97].

   Moreover, public declarations by an attacker itself can warn the target of an impending attack. For example, the hacktivist collective Anonymous announced a cyber attack on oil and gas companies before its attack [98].

   Another source is the distribution of incident information between organisations [99]. This process is an effective way of sharing information on cyber related incidents that affect their respective organisations. An example in the financial sector, is the Financial Services Information Sharing and Analysis Centre that shares incident information among its financial institution members [100].

The above sources indicate the availability of precursors. The relevance and the integrity of the information still have to be verified. This is a challenge that Information Security experts face. They have to assess the source of information, the information itself and the reason behind the publication of the information. Organisations sharing the information may have ulterior motives for sharing the information. For example, information may be a phishing fraud or it could be to create a false sense of urgency. Sometimes the information is not available and remains unknown. The information may not be shared because organisations can claim plausible deniability in case of a breach or even benefit from the data breach affecting others.

However, there is a different dilemma that exists for organisations becoming part of the value chain of sharing information. On one hand, organisations face the compulsions to report security incidents under the regulatory and legal environment for fear of prosecution. On the other hand, this is a deterrent in notifying attacks for fear of repercussions in the form of fines or loss of reputation.

Publicly available information offers an easy opportunity to assess the latest threats in Information Security. Since information is assessed in hindsight, the focus should be on incidents affecting similar organisations. An active scanning of the public information available related to incidents will create a proactive mechanism for assessment of risk. This information here changes the perspective of risk assessment from backward looking to forward looking.

6.4 Challenges of Precursors

The precursors are characterised as *"unknown"* because the information represents a future state of the system that may or may not occur. Zero-day attacks best describe this *"unknown"* characteristic. For example, the breach at RSA compromising the effectiveness of the firm's two-factor authentication SecurID tokens was accomplished with a zero-day attack [101] and the infamous Stuxnet worm combined not one but four zero-day attacks to target vulnerabilities in industrial control systems [102]. However, zero-day attacks last a lot longer and its impact is significantly higher [103], therefore the challenge is to interpret and priortise this information.

Organisations fail to react to information that is available and are therefore, prone to attacks. Let us illustrate this with an example by using *"precursors"* to detect potential security risk in the organisation. In April 2014, Home Depot was affected by a data breach that had the same signature and systems affected as a high profile breach 4 months earlier at Target. The breach at Home Depot could have possibly been avoided with the proactive approach of using the precursor that the *"Point of sale (PoS) systems are infected with malware at Retailers"*. However, what followed was another high profile data breach where the lax in security controls was highlighted and millions of users credit and debit cards information were stolen by the attackers. Even with sufficient availability of information, the organisation failed to prevent this attack on its system.

Furthermore, information on vulnerabilities is available through information sharing networks. For example, operating system and application software is regularly updated through various government cyber security systems described in Section 6.3. Software vendors using the affected code perform an assessment of the vulnerabilities in their software and provide security updates for the affected software. This is noticed in all major software vendors who regularly provide patches to vulnerable software because of the likely chances of being exploited by attackers. Therefore, the organisation has to actively scan for information about its information systems. With the complexity in these systems, it is not easy to manage in organisations. Furthermore, even though information is available, it is often overlooked creating an impression of ineffective controls. However, the correct interpretation of information by the organisation is critical here.

This brings us to the conclusion that information availability is not the problem. However, how does an organisation prioritise which information to address? With the huge volumes of information that it has to analyse and interpret, it leaves many organisations susceptible to security breaches. Rather than working on all the available information, its easier to focus in a specific area that offers a big chance of success in mitigate potential high impact risk. Therefore, organisations should define precursors that are most likely to raise its information security posture.

6.5 Summary

In this chapter, we firstly make a clear distinction between indicators and precursors (Figure 4, *Classification of Information* on page 33). The analysis indicates that precursors are not actively pursued in the incident response lifecycle. This source is a small piece set of the big information pie and precursors as a source of information present a unique opportunity to explore in this research.

The precursors are signs that an incident may occur in the future and is characterised as *"unknown"* to the organisation. It is *"unknown"* because the information represents a future state of the system that may or may not occur. However, practice shows that when this information leads to an incident, the impact is high. Therefore, the focus on selecting precursors as a source of information is useful.

With a clear understanding of this information as a source of input towards early detection of potential threats or vulnerabilities, organisations can proactively protect themselves from incidents. Precursors, which are information on incidents, are known threats that have affected a similar organisation. The possible attack vector, threat signature, vulnerability and impact is known. Vulnerability information as precursor is detected flaws in the systems deployed in organisations. This is usually provided with risk mitigation measures as well and is an advantage. The variety of information sources available as precursors described in Section 6.3 indicate that it can be an effective source if interpreted correctly.

If the organisation looks externally at the impact in another organisation and can learn from those mistakes, appropriate control measures can be recommended and implemented. The information availability on incidents is diverse, complex and unstructured. Sifting through unreliable and unknown information is still a big challenge but an opportunity as well to convert the unknowns to knows. Therefore, in an effective process, precursors are detected by actively scanning for information related to potential threats and vulnerabilities and is interpreted by skilled personnel, thereby, being valuable to the incident prevention process.

7 | Ingredient 2: Template, Trigger & Twitch

The information in Chapter 3 & Chapter 4 describes the current state of organisational measures adopted towards incident response. These are reactive measures done after the occurrence of incidents. In Chapter 5, we described the gap in the current ISRM process. However, the use of precursors described in Chapter 6 will enable proactive Incident Response. By using the elements (*Trigger, Template & Twitch*) from Vigilant Information Systems (VIS) [93], the gap described is addressed in this chapter. This helps to create a shared understanding of information for Information Security teams decision-making process. In this chapter we further extend the terms, by introducing the concept of *Tweak*, to describe the action taken on interpreting the information.

7.1 Vigilant Information Systems

Organisations are at risk when they take decisions in an uncertain environment. This is because information is not always readily available. Even if it is available, the information may not be correct. In these uncertain situations, executives develop their own ad hoc information systems to address uncertainty [93]. Here, Walls, et al. (1992) introduced the meta-requirements for Vigilant Information Systems according to Information System Design Theory (ISDT) to address this gap [93]. To develop artifacts for information systems we can use ISDT. This introduces an effective and feasible design process. This prescriptive process is an effective means for executives to take decisions by being vigilant[5].

Today, the nature of threats and their interactions in organisations are complex. These complex interactions create a chaotic working environment. There is uncertainty and decisions have to be taken in such an environment. Therefore, we can use the concept of vigilance combined with the early detection of precursors to initiate proactive action. However there is a lack of development of a socio-technical process using precursors. This can be used towards proactive Information Security risk identification and mitigation. Therefore, this research will focus on using the concepts introduced in Vigilant Information Systems to help interpret information. The following are the design elements described in Vigilant Information Systems [93].

- Template
- Trigger
- Twitch

7.2 Template

The template is the frame of reference through which organisational processes are described [94]. In this research, we use the template to describe the security baseline from risk maturity levels of

[5] Vigilance is defined as the *"state of being alert and watchful for the detection of emerging threats and opportunities in the organisational environment and to initiate further action based on such detections"* [93]

the organisation. It also maps out information system architecture details and the interaction of various elements in the information system environment. These help to identify what organisations consider as key information systems.

There are various characteristics of the information captured in the template. El Sawy, et al., (1988) describes the characteristics of information captured in the template [94]. We use this as a starting point to describe the template, however, these characteristics are not restricted to those specified and is modified based on inputs from industry experts. The three characteristics described below offers an overview of information that can define the security baseline.

1. Theme
   This describes the overarching goals and objectives of organisations. This is high-level goal describing the unifying idea describing the processes in organisations. For example, ensuring the Information Security principles of confidentiality, integrity and availability is a high-level goal in organisations compliant to ISO 27001:2013 standard [33].

2. Construct
   Constructs help to determine the relative positioning of the security maturity levels of the current state of the system as well as the future state. This is measured on a qualitative scale enabling ease of decision-making. For example, the CobiT maturity levels from Non-existent (0) to Optimised (5) determines the relative positioning of security maturity levels [104].

3. Framework
   The organisation has a variety of information systems interconnected in cyber space. These information systems are used to achieve the business goals. Therefore, the framework describes the process, the interconnections and various control mechanisms that exist. For example, the CobiT framework maps the information systems of an organisation according to four domains and 34 processes [104].

For example, let us assume that an organisation has implemented CobiT Management Guidelines. This system helps the organisation to manage information systems in a structured methodology. It describes the information systems against criteria for the effective governance of information systems. It further describes the IT environment compared to high-level control objectives defined in CobiT [104]. This information is the framework in the template. CobiT defines maturity levels ranging from Non-existent (0) to Optimised (5). It considers its processes to follow a regular pattern related to Information Security placing its maturity level at Repeatable (2). However, it wishes to be in line with industry best practices at maturity level (3) [105]. This generic maturity model is able to define and capture both the theme and construct of the baseline security for this organisation. The risk appetite of the organisation is mapped in this template.

The characteristics of theme, construct and framework best describe the template. Organisations can use their own risk assessment and control systems to describe the template. The template is the frame of reference according to which any changes in the system security environment are identified by the IPT proposed in Chapter 8. And this template should be regularly updated to reflect knowledge gained by this team.

7.3 Trigger

Trigger is defined as the stimuli that when interacting with the template may cause a shift in the template [94]. By definition, any event influencing the security baseline is termed as a trigger.

These events are both positive and negative. In this research, we focus on Information Security incidents having a negative impact to an external organisation being assessed. Therefore information described as precursors in chapter 6 are considered here as triggers.

El Sawy, et al., (1988) describes the characteristics of trigger [94], however, these characteristics are not restricted to those specified and is modified based on inputs from industry experts. The three characteristics used to define triggers are.

1. Source
   The trigger source is from where the information comes. Here the trigger sources are from precursors. Precursors are obtained by active scanning of the environment. This environmental scanning can help supplement and guide the decision-making process. However, not all information are considered as trustworthy precursors. Attackers are known to use social engineering to spread false information and gain access to organisations. Therefore, the trustworthiness of the data source is crucial since it helps the organisation to prioritise the information received from this source.

2. Information
   The trigger information is a narrative description of the information that the trigger conveys [94]. Every organisation has different information systems depending on its business requirements. Therefore, the relevant information related to organisation's information systems are important characteristics of the information to be assessed in triggers. This is because confidence in decision-making increases with the availability of relevant information. Moreover, the completeness and accuracy of information is crucial towards sound decision making. Another important factor is the consistency of the information across the various sources.

3. Latency
   The latency is defined as the time from the notification of incident to the organisation reacting to it. The time allowed for the threat to affect the organisation is a lost opportunity in incident prevention. This information can define a critical factor in determining the effectiveness of the Incident Prevention Team's proactive approach to incident scanning.

For example, let us consider a retailer using the Point of Sale (PoS) system. This organisation on scanning the environment detects a data breach using the point of sale system that affected a competitor. However, the CERT notified this information two months earlier. Here the data source is from a trusted government agency, and is accurate and complete. Moreover, the information was reiterated by security agencies that analysed the incident and is consistent. Since the retailer uses the same Point of Sale (PoS) system, it is relevant to the company. With the team now detecting the incident, the latency of information is two months. All this information triggers organisations to assess risk to Information Security.

The trigger works as an early warning system to the organisation. The IPT identifies a potential threat or vulnerability from the incident information that could affect its organisation. These precursors trigger a shift in the template. The completeness, accuracy, availability and consistency of the information are characteristics of the trigger. From an understanding of organisation systems, the relevant information is scanned from trusted data sources. The organisation can also move a step further in developing alternative data sources proactively.

7.4 Twitch

The twitch is defined as the result of the trigger influencing the template by causing a change in the template [94]. This change in the template adversely affects Information Security environment in the organisation. The identification of the twitch is an important element. This is because it identifies the vulnerabilities in the organisation. This identification helps the organisation move towards an improved security posture. Organisations today adopt a variety of methods towards the assessment of risk. Ionita (2013) describes the applicability of a variety of risk assessment methodologies and suggests guidelines for selection [35].

As discussed in the literature from El Sawy, et al., (1988), twitches have both causes and effects [94]. The twitch is described with the following three characteristics.

1. Descriptor
   Twitch descriptors are used to describe the nature of the twitch. This is the effect it has on the template. There are both direct and indirect affects of the twitch in the information system.

2. Magnitude
   The twitch magnitude is a quantitative measure describing the effect of the twitch. It is defined as the relative aggregate modification in a template due to a cumulative trigger effect in a chosen period of elapsed time [94].

3. Driver
   The twitch drivers are causes that can influence the template to twitch. We see that the most significant driver is the root cause of the problem. Moreover, organisations have to generate a detailed assessment of risk to identify the underlying root cause to be controlled. Threats are external influences but these, in combination with internal vulnerabilities, create risk to the organisation.

For example, a retailer described earlier using the Point of Sale (PoS) system is vulnerable to attacks since attackers are targeting this system. The attackers use malware to infect the system. The system was running on an out-dated software version. The effect of a successful attack on this system would lead to a data breach of the information in these systems. Therefore, the descriptors are characterised by the effect of a data breach. Organisation's Information Security baseline is affected. This is quantified with the help of the template where the maturity level for this vulnerability moves from repeatable (2) to non-existent (0). The cause of this data breach is the software not updated in the Point of Sale (PoS) system. This leads to the root cause identification. There exists the possibility that a targeted attack would be successful since the organisation may not identify the source of attack in time and will have to respond after the incident. However, in this case an updated system would generate the necessary controls for the organisation to mitigate this potential risk. This example indicates an increase in risk to the organisation. The organisation has to adopt a strategy to either increase the risk appetite or reduce the vulnerability to maintain the risk maturity level at repeatable (2).

The twitch is more informative than the template itself. The affect of the trigger on the template indicates the twitch. This change in template is indicative of the existence of vulnerabilities. The effect of change on the template is a powerful learning tool for the organisation. Thereby an early twitch is proactively used to reduce vulnerabilities in the organisation. The IPT can use the precursor to assess risk in the organisation in a controlled environment. This measure is an effective learning mechanism utilised to improve Information Security.

7.5 Tweak

We will now extend the concept of Vigilant Information Systems with Tweak. We use Tweak to describe the action taken after interpreting the information because this information about incidents is incomplete without referring to the action taken during cyber incidents. There are various means to negate the effect of the twitch. Organisations can either remove the cause of the twitch or modify the template to reflect the twitch. Organisations like to maintain a stable risk posture. In an uncertain threat environment organisations need to make decisions. With the limited influence, that organisations have on the threat, the modification of template is recommended. Changing the control mechanisms of the system affected is tweaking the template. This is achieved through different solutions. However, by using precursors, this tweak is a proactive control mechanism used by the IPT.

We need to now identify elements that can capture the nature of actions. With the nature of actions being outcomes to counter the twitch in templates, the framework for In-context Information System research by Braa & Vidgen (1999) is used [106]. Therefore the following descriptive dimensions are used to operationalise these elements actions.

1. Change
   Change is described as an intervention action to the template. With identification of drivers for twitch in template, a change measure is recommended. These are short term or long-term actions depending on the strategy adopted. This measure describes the immediate control mechanism ensuring that risk levels are not affected. This measure usually includes a change in controls to compensate for vulnerabilities or a correction in the vulnerabilities to maintain the risk level.

2. Prediction
   Prediction is described as a positivist approach in the literature by Braa & Vidgen (1999) [106]. This is a reduction mechanism to prepare for a potential risk in the organisation. The adaptive nature of controls is seen in this descriptive element.

3. Understanding
   Understanding is described as an interpreter approach. This helps in promoting a shared understanding of knowledge. Here, the lessons learned from risk analysis and control identification is used to improve the overall Information Security awareness.

For example, the retailer on assessing risk to Information Security can address the vulnerability by updating the software version used in the Point of Sale (PoS) system. This is a change mechanism. However, a residual risk to the information system still exists. Here, the proactive measure is to introduce two-factor authentication on these information systems to strengthen the security controls and thereby, reduce the level of risk. The increase of acceptable risk maturity level for the information systems from Repeatable (2) to Industry Best Practice (3) is considered as a predictive measure. Any change in risk posture has to be updated in the template and communicated through the organisation. Finally, the lessons learned on Information Security shared using the implemented knowledge management systems increases the understanding of risk in the organisation.

The action performed to negate the twitch in template can help to maintain the risk posture in the organisation. These measures help the organisation in the prevention of Information Security incident and at the same time contributes towards the incident response process. The action of change and prediction are measures that are implemented, however the dimension of understanding offers to create security awareness in organisations.

7.6 Summary

With increased complexity, problem solving in organisations requires a high degree of vigilance. The elements of Vigilant Information Systems offer a unique way to help the IPT to address this challenge. The information in the template is a structured approach helping to determine the organisation's information flow in information systems. It also helps to determine the goals and risk appetite of the organisation. This forms the basis for the organisation to assess the environment for triggers. A risk assessment helps to identify the twitch in the template. Finally, tweak describes the control actions implemented to achieve Information Security. While offering a method to structure information, it also creates an easy understanding and sharing of information. This offers the organisation the flexibility to develop a process towards the prevention of incidents. Therefore, these elements can be used by the IPT towards the development of an incident prevention process.

8 | Design: Incident Prevention Team

The Chapter 6 & Chapter 7, in Part III of this report describes the ingredients for the development of an Incident Prevention Team (IPT). With an increasing trend in cyber related crime, organisations have to be more vigilant towards Information Security as indicated in Section 7.1. Therefore, this chapter will now describe the establishment of an IPT and the process to prevent incidents by this team. Section 8.1 of this report describes how to establish the Incident Prevention Team. This includes the pre-requisites, goals, skills and expertise required in members of the IPT. This is followed by Section 8.2 describing the process to be used by IPT and finally summarised in Section 8.3.

8.1 Establishing an Incident Prevention Team

The Incident Prevention Team should be available within the organisation to actively pursue information that pertains to its Information Security. Therefore, the Incident Prevention Team or IPT can be defined as *"a team set up for the purpose of actively determining information related to information security that may influence the cybersecurity status of the organisation"*.

In the proposed design, the IPT will make use of precursors, the first ingredient described in Chapter 6, to determine what information has to be gathered. The ingredients of trigger, template and twitch described in Chapter 7 will enable the IPT to process and structure the information related to incidents. The success of the IPT depends on the interpretation of information. Therefore, this classification of information will enable the IPT to efficiently and effectively prevent incidents in the organisation. In this section, we describe the pre-requisites that need to be fulfilled before such a team is established. The identification of the IPT's objectives and structure is also elaborated in this section.

8.1.1 Pre-requisites

Top-Management Support

The IPT should be set up with the support of the top management in the organisation. Without their support, such a team would fail in achieving its goal. With the current trends in cyber incidents, there is increased awareness in top-management for more robust Information Security measures. This makes it easier for the organisation to set up such a team.

Re-use Information Security Risk Management elements

Implementation of change in organisations requires a change management process to enable people to acclimatise to change. The communication of change and deriving a shared understanding of the new process is time consuming. Therefore, the IPT would reuse Information Security Risk Management tools discussed in Chapter 3 in its process. With the re-use of elements of both Risk Management and Incident Response, an IPT can be easily set up, thereby, reducing the time taken to implement this change.

The preparation phase is described to have a prevention activity in the preparation phase of the incident response lifecycle as discussed in Chapter 4. Therefore, the IPT should add value to this process. This can be done by setting up the IPT in this phase and not create a separate structure adding to the complexity of organisational systems.

Furthermore, it should be set up with the help of current members of the IRT. We can easily set up the IPT in this phase, because the IRT responds only during an incident. Therefore, there expertise is used in the new process in the preparation phase to prevent incidents. Furthermore, this reuse of expertise creates a flexibility in the setup of IPTs, thereby creating a proactive process to respond to incidents.

8.1.2 Goals

The main goal of the Incident Prevention Team is *"to prevent potential Information Security incidents"*.

- By actively scanning for potential threats and vulnerabilities (*hereinafter referred to as precursors*)
- By prioritising precursors
- By assessing risk to information systems, and
- By formulating control strategies based on the risk assessment

This goal, helps to be compliant to Information Security aspects of confidentiality, integrity and availability as stated in ISO 27001:2013 standard [33], and simultaneously raises the overall security awareness in the organisation.

8.1.3 Team Formation

The skill and expertise required by the IPT is an important aspect in team formation. The IPT should be staffed with the same personnel as the incident response team described in Section 4.2.1. This is because both teams perform similar roles. While the IRT is backward looking, the IPT will be forward looking. Moreover, there are limited resources in the organisation and the creation of separate teams is not feasible.

Team Leader

Like the IRT, the IPT should have a team leader capable to manage both technical aspects of Information Security incidents as well as the process approach to managing Information Security across the organisation. This person should have the necessary knowledge and experience to be able to take decisions in an uncertain environment. This person should be able to direct and manage the IPT. This person should also be able to bridge the gap between IPT and IRT and integrate the lessons learned in Information Security Management system.

Technical support staff

The technical support personnel can include specialist in database security, server security, storage, operating system knowledge, network security, etc. The IT system administrator is also part of this team. These resources may be in-house or outsourced from third party security service providers.

Process support staff

Personnel trained in risk assessment techniques are a valuable resource in the IPT. There expertise is used in activities described in the incident prevention process in Section 8.2.

Other Members

The Chief Information Security Officer (CISO) and Business Process Manager are key stakeholders in this team. The CISO is generally apprised of the key Information Security challenges. Business Process Manager's are consulted on the impact to the business during the risk assessment process. The access to legal counsel, internal communication team, HR personnel, etc. are other resources that the IPT can seek out during the incident prevention process.

8.2 Process

There is uncertainty associated with information regarding cyber incidents. The IPT has to take decisions in this environment. Since the objective of the IPT is *"to prevent potential Information Security incidents"*, we incorporate the key ingredients described in Chapter 6 & Chapter 7 in the incident prevention process. Precursors are used as an input by the IPT. The elements of Trigger, Template, Twitch and Tweak are used to operationalise this incident prevention process integrating the different aspects of incident information together.

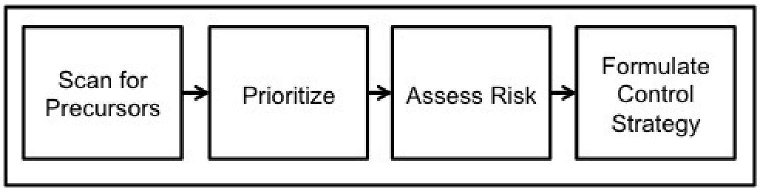


Figure 5: High Level Incident Prevention Process

The Figure 5, *High Level Incident Prevention Process*, illustrates the key steps that the IPT performs during incident prevention. This process addresses the lack of attention given to the present incident prevention process. The input, activities and output for each step of the process are enumerated in the sections below. This is followed by the operational questions that the IPT can use to implement the incident prevention process in organisations.

8.2.1 Step 1: Scan for Precursors

The Figure 6, *Scan for Precursors*, represents the first step in the incident prevention process. In this step, the IPT actively scans the environment for precursors a key ingredient discussed in Chapter 6. This activity performed by the IPT differentiates itself from other incident response processes.

The input for this activity is the knowledge of the information system and Information Security environment in the organisation. This knowledge is to help the IPT have a baseline understanding of the organisation's information systems. The activities that the IPT performs in this step include

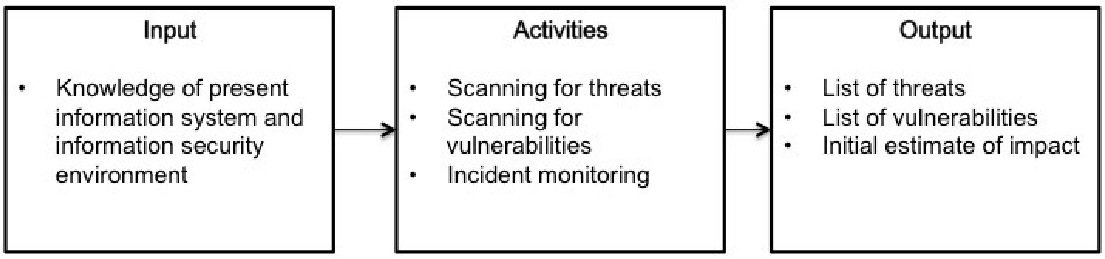

Input
• Knowledge of present information system and information security environment
Activities
• Scanning for threats
• Scanning for vulnerabilities
• Incident monitoring
Output
• List of threats
• List of vulnerabilities
• Initial estimate of impact

Figure 6: Step 1, Scan for Precursors

the scanning for threats and vulnerabilities and the monitoring of incidents affecting other organisations. This activity is a key characteristic feature of the incident prevention process because it is forward looking. The IPT should attempt to retrieve complete, accurate and reliable information.

The IPT can effectively and efficiently gather precursors from trustworthy information sources. The IPT defines trustworthy information sources as those sources from which there is value derived from the information available. Here, the IPTs understanding of the organisation's information system and its experience as incident handlers, will strengthen the identification and interpretation of precursors. The outcome of this process is a preliminary list of threats and vulnerabilities considered as precursors. The IPT also makes an initial estimate of impact of the incident.

The information retrieved is now categorised as triggers. The source, information itself and latency are the characteristic elements of triggers, used to operationalise this incident prevention process. These characteristic elements are used because precursors by itself are raw data. The shared understanding of the information in context with Information Security requirements will add value to the information, triggering the next step of the process.

The following generic questions are asked by the IPT when scanning for precursors. These questions serve as stimuli towards generating triggers to assess the current Information Security environment in the organisation.

I Does the information come from a trustworthy data source?

II Is the information complete, accurate and reliable?

III Is the information relevant to the present organisations system, process or people?

IV Is the information consistent?

V How long has the information been available?

8.2.2 Step 2: Prioritise

The Figure 7, *Prioritise*, represents the next step in the incident prevention process. The list of triggers identified is prioritised in this step by the IPT.

The input to this step is derived from the output of the previous step, i.e. list of triggers. Furthermore, information about the information system, described using a template is also used as input. As described in Chapter 7, template is characterised by a theme describing the critical Information System security objectives, the constructs describing the Information Security maturity level desired and the description of the Information System architecture. Input to the template is obtained from the most recent risk assessment activity as well as lessons captured from post

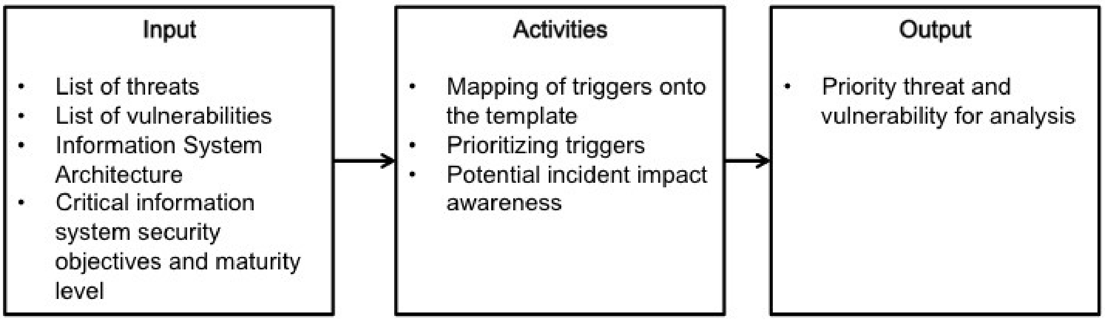

Input
• List of threats
• List of vulnerabilities
• Information System Architecture
• Critical information system security objectives and maturity level
Activities
• Mapping of triggers onto the template
• Prioritizing triggers
• Potential incident impact awareness
Output
• Priority threat and vulnerability for analysis

Figure 7: Step 2, Prioritise

incident phase of the incident response lifecycle. These inputs are used because it comprehensively describes the security baseline of the organisation.

The activities performed by the IPT in this step of the process are as follows. The IPT maps the trigger onto the template. For example, vulnerability in the list of triggers is mapped onto the organisation's information system to assess the potential impact a threat might have on that information system. The trigger with the highest impact is prioritised by the IPT. Here, the IPT needs consensus on the impact of triggers on the business objectives of the organisation. By having consensus it establishes the priorities for risk assessment in the next step. Therefore, the outcome is a list of priority triggers made up of information on threats and vulnerabilities, agreed by the IPT.

In this step, the IPT focuses on comparing the information from triggers and templates. This step is useful since it is a high level prioritisation performed by the IPT. It is high-level process because there are large volumes of information that the IPT has to process and a risk assessment of all triggers is not feasible. There has to be a filter to segregate information. Therefore, in this step the team identifies triggers that it considers a priority. The operational questions to determine this priority are enumerated below.

VI Does the Incident Prevention Team have consensus on the priority?

VII Can the Incident Prevention Team justify why the other triggers are not considered as a priority?

8.2.3 Step 3: Assess Risk

The Figure 8, *Assess Risk*, represents the next step in the incident prevention process. The IPT determines the risk in this step of the incident prevention process.

The input to this activity is the prioritised list of threats and vulnerabilities determined in the previous step. Additionally Information Security risk assessment results from earlier risk assessments are used to compare the change to Information Security status.

In this step, the IPT carries out a risk assessment[6]. In the risk assessment process, the vulnerable information systems are evaluated on the Information Security principles of confidentiality,

[6] Risk computation: *Risk(Threat,Asset)=Likelihood(Threat)XVulnerability(Threat,Asset)XImpact(Threat,Asset)* Risk is defined as the likelihood that a certain threat will engage in an attack, the vulnerability of the target (asset) to the threat and the potential impact that the attack might have on the asset [35]

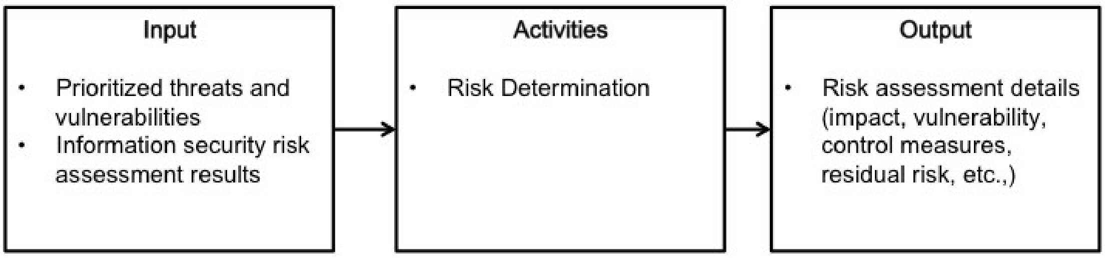

Input
• Prioritized threats and vulnerabilities
• Information security risk assessment results
Activities
• Risk Determination
Output
• Risk assessment details (impact, vulnerability, control measures, residual risk, etc.,)

Figure 8: Step 3, Assess Risk

integrity and availability. This step is a reiteration of the Information Security Risk Management (ISRM) process within the organisation.

The IPT determines the level of abstraction required for this risk analysis because it is not feasible to perform a complete risk assessment. The IPT focuses on assessing Information Security risk of only the information system likely to be affected. It does not require all the resources used in traditional ISRM processes. Therefore, it is an agile incident prevention process.

Therefore, the output is a detailed risk assessment of the information system affected. These details include the vulnerabilities in the information system identified, the control measures associated, the potential impact of the risk, residual risk from the threat, etc.

In this step, the IPT focuses on the twitch in template caused by triggers. The assessment of the risk posture identifies the magnitude (impact) and drivers (vulnerabilities) of the twitch. These details are useful towards understanding the complexity in information systems and the risk associated with them. Therefore, organisations move from compliance based risk assessment to awareness based risk assessment. The operational questions that the IPT can ask in this step of the process are enumerated below.

VIII Is there a likelihood of threat?

IX Is there a vulnerability in the information system?

X What is the potential impact of risk in the organisation?

8.2.4 Step 4: Formulate Control Strategy

The final step of the incident prevention process is depicted in Figure 9, *Formulate Control Strategies.* The IPT formulates control strategies in this step of the process.

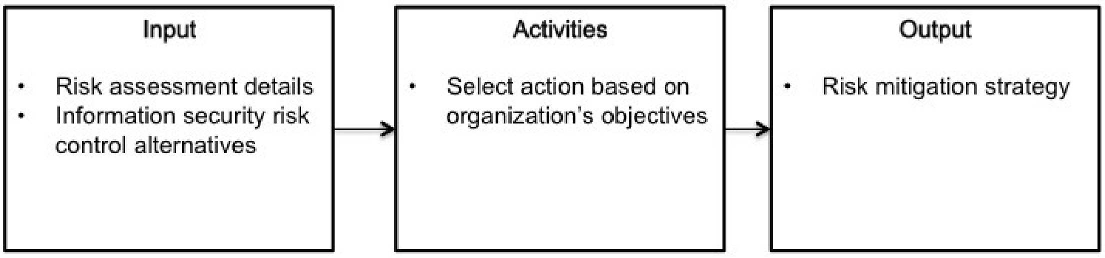

Input
• Risk assessment details
• Information security risk control alternatives
Activities
• Select action based on organization's objectives
Output
• Risk mitigation strategy

Figure 9: Step 4, Formulate Control Strategies

The input to this activity is the detailed risk assessment information from the previous step and a list of Information Security control measures. If the trigger indicated a twitch in status quo of the template, remedial action should be taken to return the template to a stable risk posture. The IPT along with the management can determine the appropriate control strategies based on the organisation's risk appetite. These risk strategies described can be achieved by assumption of the risk, avoiding the risk, limitation of the risk, planning for the risk or risk transference. Therefore, the output of this step is a risk mitigation strategy to address the risk in the organisation.

The failures in Information Security are due to ineffective implementation of controls measures, resulting in significant risk to the organisation. Therefore, this activity is needed to integrate the lessons learned from the risk assessment process with the implementation of Information Security controls in the organisation by formulating effective control strategies. This step is crucial to incident prevention, because, it determines the organisation's ability to react to Information Security risk. An agile process will transform the organisation, enabling it to adapt to changing security conditions, thereby making it more adaptive. The operational questions asked by the IPT are enumerated below.

XI Is there a mechanism to implement the control strategy determined? If not, how can the IPT help implement the control strategy?

It is important to note that the IPT is not responsible for implementing Information Security controls. There are mechanisms in place that address this in the organisation. However the IPT can assist in the implementation of control strategies should the need arise.

8.3 Summary

The incident prevention process is performed in the preparation phase of the incident response lifecycle (Figure 3 on page 15) by the IPT. Therefore, at the end of these 4-steps, the prevention mechanism of the preparation phase is made more robust. There is an active feedback mechanism in place in the overall incident response lifecycle, therefore, this process does not require a feedback cycle itself. This process makes use of input from previous risk assessments, and at the same time actively monitors the environment. The triggers identified from precursors initiate the IPT to perform an ad hoc risk assessment to determine the risk in the organisation. Therefore, this incident prevention process benefits the Risk Assessment and Incident Response process in organisations.

This incident prevention process is a proactive approach to problem solving in comparison to traditional incident response processes. The success of this process is on the timely and accurate implementation of control measures identified from the risk assessment. Moreover, the gathering of precursors to assess risk increases the overall Information Security awareness level in the organisation, thereby, ensuring resilience against Information Security incidents.

Part IV

Evaluation

9 | Evaluation

The last part of this report focuses on the evaluation of the proposed Incident Prevention Team as described in Chapter 8. The goal is to validate the need for an Incident Prevention Team and show the effectiveness of the process suggested in organisations. This is done with two cyber incident example scenarios described in Section 9.1. These scenarios are fictitious and have been validated by a security expert. Additionally, we examine the quality of the proposed design by an interview with a security expert in Section 9.2. The expert interview also serves as the first step in the process of communication of the research findings.

9.1 Evaluation through Scenarios

9.1.1 Scenario 1

In Scenario 1, let us assume a public hospital in USA offering health care services across the country hereinafter referred to as Org-A. In 2013, Org-A performed an Information Security risk assessment. It was found to be compliant to ISO 27001:2013 standards. Since then, there have been no changes in its information systems. Now in 2014, no risk assessment has been conducted but the organisation is still compliant since its last risk assessment.

Org-A's policy on frequency of performing a risk assessment is that *"a risk assessment is carried out every 2 years or whenever there is a major change in any of the organisation's information systems"*.

Org-A's Incident Prevention Team

Org-A has established an Incident Prevention Team as suggested by this research. This team consists of members with different skills and expertise (Section 8.1.3). The team leader has 10 years of experience in incident handling and is aware of the information systems and associated policies of the organisation. From the technical support staff, members include IT administrators, server and database security specialist and network security specialist. Org-A has support staff in the event of an incident on-demand from its IT service provider. The process staff is capable of conducting Information Security risk analysis according to the risk assessment procedure defined.

Goal

The goal of the IPT is *to proactively gather information related to cyber incidents affecting other health care service providers and assess the risk to Org-A*. This is done with the expectation that Org-A can learn from these external incidents and prevent similar incidents.

Scope

The IPT focuses on gathering information about hospitals in USA where Org-A is located. This is because data privacy laws vary from country to country [107]. The Health Insurance Portability and Accountability Act (HIPAA) is the law applicable for Org-A in this example. According to HIPAA, data breaches affecting 500 or more individuals have to be notified and published.

Incident

In August 2014, the Heartbleed flaw was used to hack and steal information from Community Health Systems, the second-biggest for-profit U.S. hospital chain. The flaw was published in April 2014, by US-CERT in the National Vulnerability Database (NVD) [95]. Control measures for data protection against this vulnerability of OpenSSL were also published and software vendors provided updates to OpenSSL to mitigate the risk of this vulnerability in their software.

Incident Prevention Process in Org-A

The blue roman numerals (I - XI) indicate which questions are answered from the various steps of the incident prevention process described in Section 8.2.

Step 1: Scan for precursors

Input: The IPT is aware of the information systems present in Org-A and the Information Security status of these systems. The template is updated and is referred to as and when the need arises.

Activities: The IPT actively scans for precursors, i.e., information on threats and vulnerabilities in the health care sector.
(I - V) The IPT downloads the latest data breaches in health care organisations from the website of US Department of Health & Human Services (HHS) (Figure 10, *HHS database of data breaches* [108]). This website publishes incident information that the IPT considers as precursors and is relevant to Org-A. It includes the date of breach, location of breach as well as the number of individuals affected due to the breach.

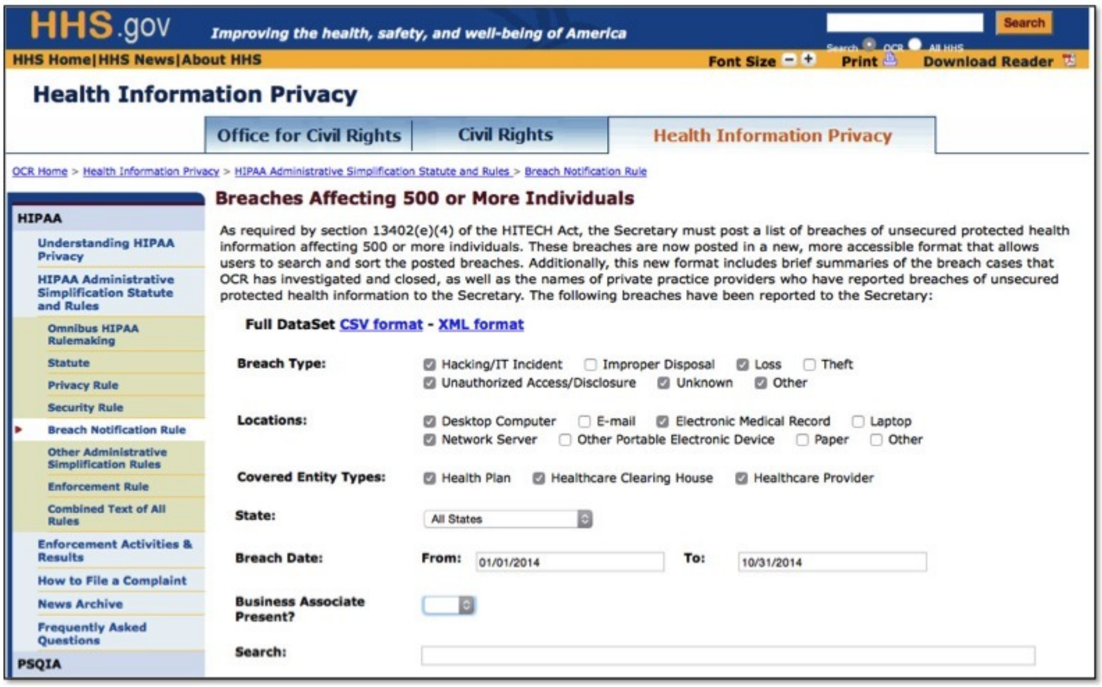
Similarly, the US-CERT regularly publishes information on vulnerabilities detected in information systems (Figure 11, *National Vulnerability Database* [95]). It is a repository of standards based vulnerability management data and is a reliable data source. Furthermore, the information available from this source is complete and accurate. Both the websites are trustworthy government data sources. Furthermore, the information is consistent across these two sources.

Output: The information published can be retrieved in comma-separated value (CSV) or extensible mark-up language (XML) file formats. This generates an extensive list of threats and vulnerabilities for the IPT to review (Figure 12, *List of Triggers*). Now the IPT has to assess if any of the precursors in the list, triggers a change in Org-A's template.

Step 2: Prioritise

Input: The two files downloaded in the previous step and the Org-A's template (Figure 13), are inputs in this step.

Activities: Using the list of threats and vulnerabilities, the IPT has to prioritises the information. Here, the knowledge and experience of members of the IPT play a major role in prioritising information. This is done by determining the potential impact of each trigger mapped onto Org-A's information systems. The team leader, with 10 years of experience is


HHS.gov
Improving the health, safety, and well-being of America
Search
Search ● OCR ○ All HHS
HHS Home|HHS News|About HHS
Font Size − +
Print
Download Reader
Health Information Privacy
Office for Civil Rights
Civil Rights
Health Information Privacy
OCR Home > Health Information Privacy > HIPAA Administrative Simplification Statute and Rules > Breach Notification Rule
HIPAA
Understanding HIPAA Privacy
HIPAA Administrative Simplification Statute and Rules
Omnibus HIPAA Rulemaking
Statute
Privacy Rule
Security Rule
Breach Notification Rule
Other Administrative Simplification Rules
Enforcement Rule
Combined Text of All Rules
Enforcement Activities & Results
How to File a Complaint
News Archive
Frequently Asked Questions
PSQIA

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full DataSet CSV format - XML format

Breach Type: ☑ Hacking/IT Incident ☐ Improper Disposal ☑ Loss ☐ Theft ☑ Unauthorized Access/Disclosure ☑ Unknown ☑ Other

Locations: ☑ Desktop Computer ☐ E-mail ☑ Electronic Medical Record ☐ Laptop ☑ Network Server ☐ Other Portable Electronic Device ☐ Paper ☐ Other

Covered Entity Types: ☑ Health Plan ☑ Healthcare Clearing House ☑ Healthcare Provider

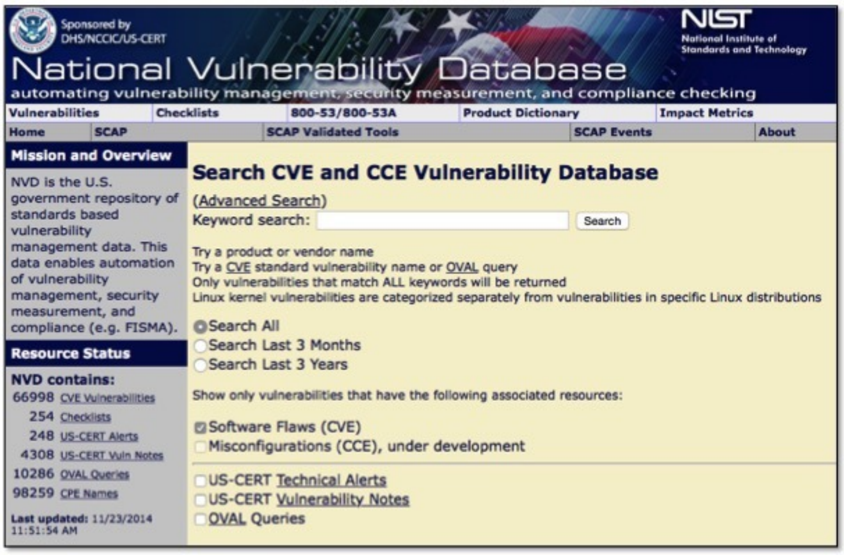
State: All States

Breach Date: From: 01/01/2014 To: 10/31/2014

Business Associate Present?

Search:

Figure 10: Precursor Source 1, HHS database of data breaches [108]


Sponsored by DHS/NCCIC/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53/800-53A
Product Dictionary
Impact Metrics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Mission and Overview
Resource Status
Search

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

NVD contains:
66998 CVE Vulnerabilities
254 Checklists
248 US-CERT Alerts
4308 US-CERT Vuln Notes
10286 OVAL Queries
98259 CPE Names

Last updated: 11/23/2014 11:51:54 AM

Search CVE and CCE Vulnerability Database

(Advanced Search)
Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

● Search All
○ Search Last 3 Months
○ Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

☑ Software Flaws (CVE)
☐ Misconfigurations (CCE), under development

☐ US-CERT Technical Alerts
☐ US-CERT Vulnerability Notes
☐ OVAL Queries

Figure 11: Precursor Source 2, National Vulnerability Database [95]

able to interpret the triggers effectively to determine the priority trigger to be assessed in the next step.

Mapping of triggers, indicate attackers targeting a flaw in OpenSSL. The US-CERT had published information about this vulnerability in its report CVE-2014-0160 (Heartbleed Bug) [109]. From the health care industry, 4.5 million social security numbers were stolen from Community Health Systems by attackers targeting the same vulnerability [91].

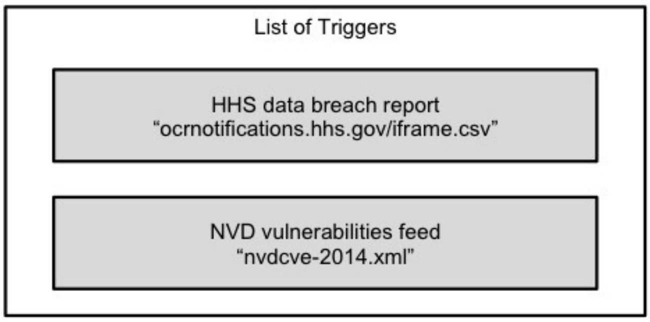


Figure 12: List of Triggers

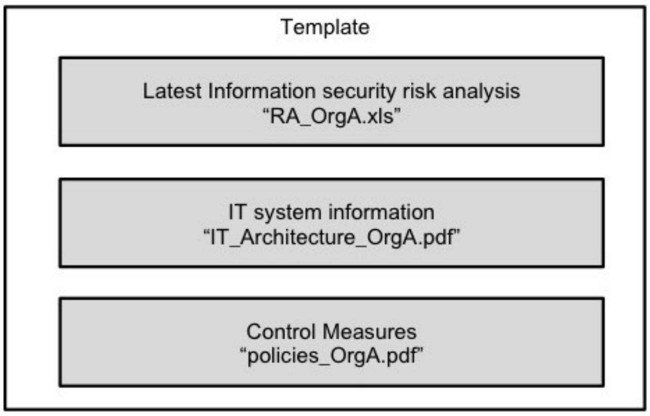


Figure 13: Org-A’s template

(VI - VII) This is reported as high-impact vulnerability because it could be used to disclose sensitive private information to an attacker. The IT system administrator confirms the use of OpenSSL in its legacy system software within the organisation. A third party vendor developed the software that was last updated 2 years ago. On learning this, all members of the IPT agreed that this was a high priority trigger. Other vulnerabilities and threats in this list were also mapped onto the template but were not a match and therefore disregarded.

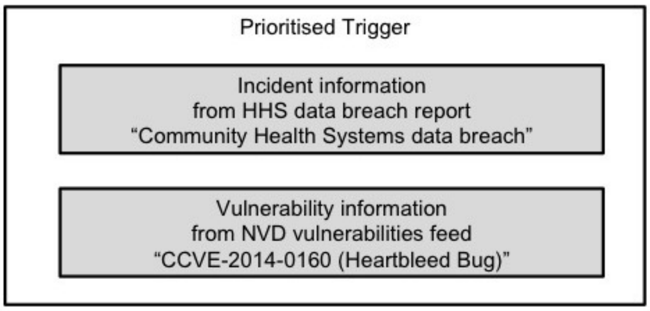

Prioritised Trigger
Incident information
from HHS data breach report
“Community Health Systems data breach”
Vulnerability information
from NVD vulnerabilities feed
“CCVE-2014-0160 (Heartbleed Bug)”

Figure 14: Org-A’s trigger prioritised

Output: Therefore, the data breach at Community Health Systems affected by the Heartbleed Bug is prioritised for the risk assessment (Figure 14 *Org-A's trigger prioritised.*

Step 3: Assess Risk

Input: The prioritised trigger of the OpenSSL vulnerability and Org-A's Information Security risk assessment results are input in this step of the process.

Activities: A detailed risk assessment of Org-A's information systems are performed utilising the information gathered about the OpenSSL vulnerability. IPT identifies a possible threat vector for this vulnerability as the third party software used in its information system. With this threat vector, the IPT analysis the integrity of this software's control measures.

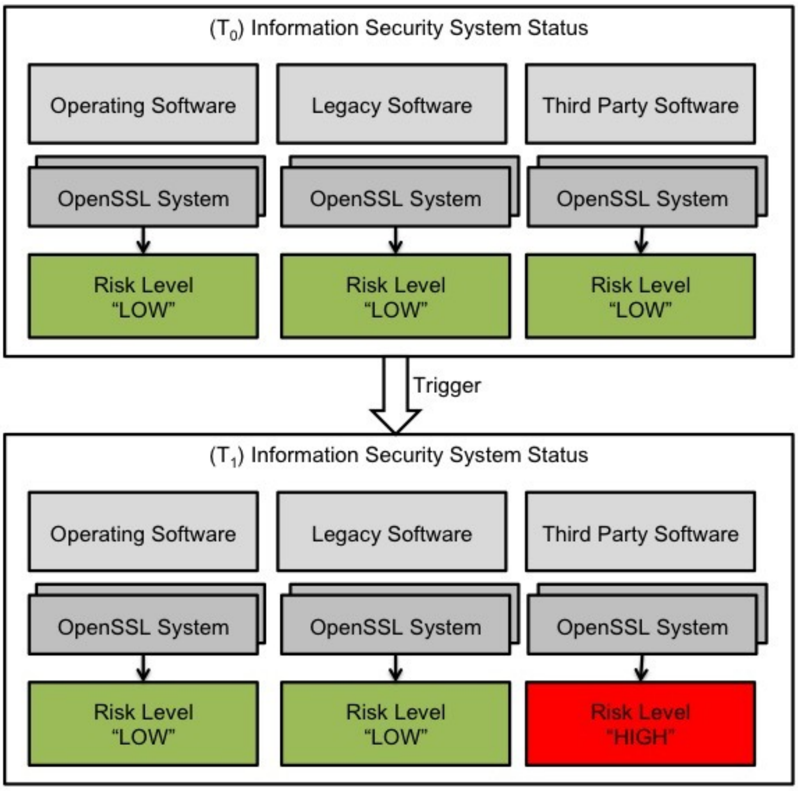


Figure 15: Twitch in risk maturity level

(VIII - X) There is a twitch in Information Security status. The IPT finds that using this threat vector, the likelihood of attacker gaining access to patient data is high. The risk level increases from LOW at time T_0 to HIGH at time T_1 as shown in Figure 15, *Twitch in risk maturity level.* This is a high impact risk to the organisation because the confidentiality principle of Information Security is affected. The IPT concludes that updating the OpenSSL version in the third party software can control this risk. However, the residual risk still exists and a control strategy has to be developed to mitigate this risk.

Output: The detailed results of risk assessment are enumerated in the risk assessment report. Information about the threat, threat vector, vulnerability, information system impacted, control measure failure, recommended control, residual risk, indirect and direct impact, etc. are compiled for further action by the relevant Information Security team.

Step 4: Formulate Control Strategy

Input: The input to this step are the risk assessment details determined in the previous step by the IPT.

Activities: The IPT has to determine the appropriate control strategy to mitigate the risk. The following reasoning helps to determine the strategy. There is a negative shift (twitch) in the risk maturity level. This twitch is caused by vulnerability in the software version provided by a third party vendor. While the application and operating systems software was up-to-date, the third party software was still using an older version. This indicates ineffective control measures adopted towards this software. This is because, the software is part of the organisation's legacy system and it is not feasible to replace. Furthermore, the frequency of updates in this software is low, thereby, increasing the risk. Therefore, this requires an immediate remedial action from the third party software vendor as well as ensuring that the organisation's third party software is regularly updated.

Output: The strategy to put in place control measures to regularly update third party software was added to Org-A's IT procedure.

(XI) IT procedures are implemented by the IT system administrator. Therefore, the mechanism to ensure that the control strategy is implemented exists. The learning from this incident prevention process was also communicated to the management team. Therefore, Org-A is able to prevent a possible attack by implementing controls for the Heartbleed vulnerability.

9.1.2 Scenario 2

In Scenario 2, let us assume that Org-B is a Datacenter located in the Netherlands. The organisation is compliant to TIA-942-2 standards issued by Telecommunications Industry Association (TIA), in conjunction with the American National Standards Institute [110]. TIA tier standards include both physical as well as network specific compliance requirements.

This data centre has to maintain a specific range of temperature to be compliant with the aforementioned standard. To achieve this, Org-B uses a climate control system. It is maintained by a third party industrial control system provided by Tridium. This system will be evaluated in this scenario.

Org-B's Incident Prevention Team

Org-B has established an Incident Prevention Team as suggested in the research. The team consists of members trained in IT security management. Org-B has a variety of skills and resources in-house, because of its Information Security centric business model. The team consists of specialist in IT system administration, server, database and network security. Furthermore, it has a team of experts in the field of risk analysis.

Goal

The IPT in Org-B has the objective *"to proactively assess the integrity of data centre and advice the management on change in Org-B's Information Security status"*. The IPT is critical to Org-B's operations. It helps to achieve the business objective of providing state-of-the-art data security at its data centre.

Scope

The scope for the IPT is to gather information on threats and vulnerabilities of both its client as well as vendors. In this example, the IPT focuses its search for precursors on its industrial control system vendors.

Incident

In April 2013, the US-CERT reported an attack on the energy management system of a New Jersey manufacturer [111]. However earlier in July 2012, independent security researchers had identified multiple vulnerabilities in the Tridium Niagara AX Framework software and the vulnerability was notified by ICS-CERT [112].

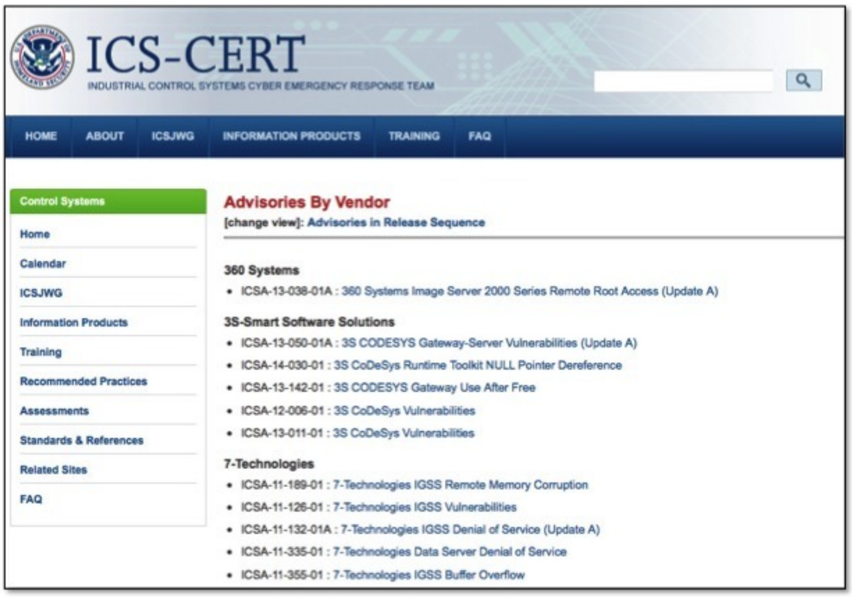
Incident Prevention Process in Org-B

The blue roman numerals (I - XI) will again indicate which questions are answered from the various steps of the incident prevention process described in Section 8.2.

Step 1: Scan for precursors

Input: The input to this step is the awareness of Information Security system status of Org-B.

Activities: The IPT in Org-B undertakes an active scan of the environment for information related to data centres. With a number of Information Security systems outsourced, the IPT actively monitors potential threats and vulnerabilities of its vendor's information systems. It also gathers information of threats and vulnerabilities related to its client's information systems.



Advisories By Vendor

[change view]: Advisories in Release Sequence

360 Systems

- ICSA-13-038-01A : 360 Systems Image Server 2000 Series Remote Root Access (Update A)

3S-Smart Software Solutions

- ICSA-13-050-01A : 3S CODESYS Gateway-Server Vulnerabilities (Update A)
- ICSA-14-030-01 : 3S CoDeSys Runtime Toolkit NULL Pointer Dereference
- ICSA-13-142-01 : 3S CODESYS Gateway Use After Free
- ICSA-12-006-01 : 3S CoDeSys Vulnerabilities
- ICSA-13-011-01 : 3S CoDeSys Vulnerabilities

7-Technologies

- ICSA-11-189-01 : 7-Technologies IGSS Remote Memory Corruption
- ICSA-11-126-01 : 7-Technologies IGSS Vulnerabilities
- ICSA-11-132-01A : 7-Technologies IGSS Denial of Service (Update A)
- ICSA-11-335-01 : 7-Technologies Data Server Denial of Service
- ICSA-11-355-01 : 7-Technologies IGSS Buffer Overflow

Figure 16: Precursor Source, ICS-CERT notification of vulnerabilities [112]

.

(I - V) In this example, the IPT scans for information about industrial control systems used within Org-B for climate control, fire suppression, etc. The IPT gathers the information available on the website of ICS-CERT (Figure 16, *ICS-CERT notification of vulnerabilities* [112]. This is a trusted data source for the IPT. Furthermore, SCADA and Control Systems Information Exchange (SCSIE) is facilitated by Centre for the Protection of National Infrastructure (CPNI) [113]. The information across both these sources are consistent, accurate and provide a complete analysis of vulnerabilities detected in industrial control systems.

Output: The information from ICS-CERT [112] and CPNI [113] is retrieved in extensible mark-up language (XML) file format. These sources generate a list of triggers for the IPT to prioritise.

Step 2: Prioritise

Input: The input is the list of triggers and the template. The template is information about Org-B's objectives, its information system architecture and details of the last risk assessment (Figure 17, *Org-B's template*).

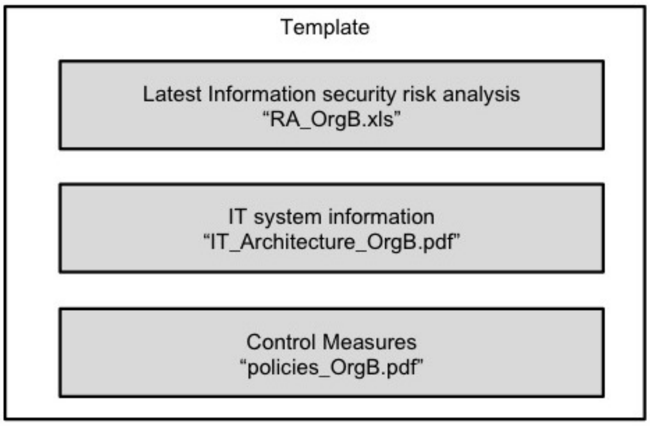
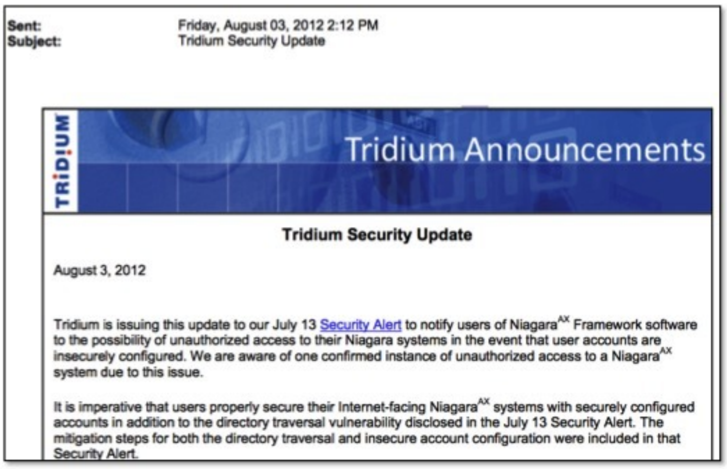


Figure 17: Org-B's template

Activities: Using the list of triggers generated in the previous step, the IPT now has to prioritise the information. A quick scan of the information shows that the energy management system exploited by attackers, used vulnerabilities in the Tridium Niagara AX Framework software. This is the same system used by Org-B. The vulnerability is described as directory traversal and weak credential storage remotely exploitable [112]. This information provided with proof of concept indicates the ability of the attackers to control the climate system [114]. With limited knowledge on industrial control systems, the IPT also scans the Tridium website (Figure 18, *Tridium's vulnerability notification*). The advisory notified in the July 2012, warns of the possibility of unauthorised access with the vulnerability in their system. Furthermore, the information has been available for nine months before the date of the incident reported by US-CERT [111].

Output: (VI - VII) With this impact affecting the integrity of data centres climate control facility, a critical operational feature of the data centre, it was considered a high priority by the IPT. With no other vulnerability in the list of triggers related to operations, the vulnerability in climate control system was selected. Therefore, the vulnerability in Tridium



Sent: Friday, August 03, 2012 2:12 PM
Subject: Tridium Security Update

Tridium Security Update

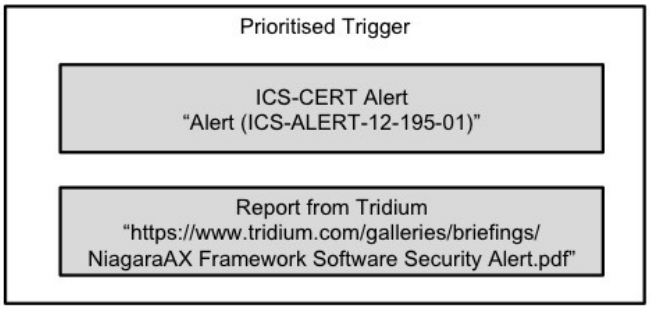
August 3, 2012

Tridium is issuing this update to our July 13 Security Alert to notify users of Niagara^{AX} Framework software to the possibility of unauthorized access to their Niagara systems in the event that user accounts are insecurely configured. We are aware of one confirmed instance of unauthorized access to a Niagara^{AX} system due to this issue.

It is imperative that users properly secure their Internet-facing Niagara^{AX} systems with securely configured accounts in addition to the directory traversal vulnerability disclosed in the July 13 Security Alert. The mitigation steps for both the directory traversal and insecure account configuration were included in that Security Alert.

Figure 18: Tridium's vulnerability notification (Dated August 3, 2012)

Niagara AX Framework software is prioritised. This information is used for risk assessment of the climate control system of Org-B in the next step of the process (Figure 19 *Org-B's trigger prioritised*).



Prioritised Trigger
ICS-CERT Alert
"Alert (ICS-ALERT-12-195-01)"
Report from Tridium
"https://www.tridium.com/galleries/briefings/
NiagaraAX Framework Software Security Alert.pdf"

Figure 19: Org-B's trigger prioritised

Step 3: Assess Risk

Input: The IPT utilises the results of the previous risk assessment and the priority trigger determined in the previous step.

Activities: The risk assessment on the climate control system at Org-B is carried out. It is used to determine if the vulnerability in Tridium Niagara AX Framework software creates a twitch in its Information Security status.
(VIII - X) In the risk assessment process, the IPT determines the threat vector, i.e., remote access that would allow attackers to override the temperature controls. There is a twitch in Information Security status because an out-dated version of the software is currently running on the climate control system. The IPT determines that the likelihood of an attack using this threat vector is high. Furthermore, a change in operational parameters of climate data will create a high impact to the integrity of the data centre's operations. The IPT concludes that with an updated software version, the risk to data centre through this threat vector would not exist.

Output: A detailed report on the impact, threat, vulnerability and control measure is compiled as output for further action by the relevant Information Security team.

Step 4: Formulate Control Strategy

Input: The input to this step are the risk assessment details determined in the previous step.

Activities: The IPT has to determine the appropriate control strategy to mitigate the risk to Org-B's climate control system. The following reasoning helps it to determine the strategy. The risk assessment in Step 3 indicates that the likelihood of an attack using this threat vector is high because the information about the vulnerability was publicly notified. The energy management system exploited by attackers, nine months after the notification of vulnerability, shows that the vulnerability still exists in organisations with out-dated software. The risk assessment shows that Org-B is also at risk. This indicates that Org-B's control measure is ineffective. Therefore, this requires a strengthening of controls in its critical climate control systems.

Output: Therefore, a risk mitigation strategy is developed by the IPT to implement additional checks on its critical climate control systems. These checks would be performed by the utilities Information Security administrator. As an immediate risk control measure, an update of the software version is recommended.
(XI) There exist different teams managing different aspects of Information Security in Org-B. IT security, utility security, data base security, physical security, etc. Therefore, the mechanism to ensure that the control strategy is implemented, exists.

9.1.3 Discussion

The two scenarios discussed above illustrate the incident prevention process followed by the proposed Incident Prevention Team. The examples show an ideal case of incident prevention where the process adds value to the organisation. However, this needs to be compared to the real world situations. Here, we notice that there are some challenges that can prevent such an Incident Prevention Team from making organisations resilient to Information Security incidents.

Step 1: Scan for precursors

In the first step, the IPT actively scans for precursors after it has identified its scope. These examples portray that information is readily available; it is also complete and accurate; and is obtained from a trusted data sources. They show that precursors are comprehensive and used to achieve better Information Security in the organisation. With an established Incident Prevention Team, both Org-A and Org-B were able to easily scan for information relevant to its organisation.

However, in reality this step is not as easy as just looking up information available from public data sources. A basic understanding of both the information systems and its interactions in cyberspace is required to understand what information should be looked at. Organisations may not have the necessary resources in place and even if they do, the likelihood of the resources knowledge on information systems might be limited.

Furthermore, the information itself may not exist publicly. In such situations, the organisation will have to develop alternative information sources. It is here that information sharing is crucial in the development of reliable sources. The organisation from the perspective of sharing information, has to also address what information it can share and what is sensitive to the organisation. However, if there is an active information sharing network, it will create a shared understanding of Information Security risk for both the organisation and its sources.

Even with these limitations, the step offers a unique opportunity to organisations. The scan for precursors enables the organisation to look at information that was previously not considered. The activity of scanning itself makes the people in the organisation aware of the Information Security environment beyond its information system boundaries. By understanding the environment, in which it operates, the organisation can move towards better security awareness.

Step 2: Prioritise

In this step, the precursors were prioritised, based on the skill and expertise of members of the IPT. The examples indicate that the members of the IPT have years of experience in the field and are able to evaluate interpret the precursors and reach a consensus on the trigger. Both examples show that the experience and knowledge of the IPT members played a crucial role in how smoothly the process moves forward.

However, without some expertise, the interpretation of information is a challenge. Up-to-date knowledge on the information systems, organisations goals, etc. is required by the IPT. We acknowledge that the members of the IPT may not know everything. But they should be able to make an approximate estimation of the information's validity and prioritise the precursors to arrive at triggers. The team should also be able to agree on what to prioritise. Different perspectives are bound to exist with members of the IPT having diverse backgrounds. It is also possible that the team will not be able to agree on what to prioritise for fear of having overlooked information that might later be a risk to the organisation. Therefore, it is important that the members of the IPT have a shared understanding of the organisation's objectives. This step of the process, does not describe how to arrive at this shared understanding because it is influenced by the organisations culture and group dynamics between members in the IPT. This aspect is beyond the scope of this research.

Step 3: Assess Risk

During the risk assessment performed by the IPT of the affected information systems, a detailed risk assessment report of the potential incident is generated. Since only the affected system is assessed, this creates an agile process. The examples show that the IPT is able to identify a likely threat, its potential path of propagation, and the vulnerability in the system and the Information Security control associated. The risk assessment also brings to light residual risk that raises the overall awareness of information system security.

When the risk assessment process is assessed from a practical perspective, this process does not appear to be as easy and straight forward as described in the literature [17]. The risk assessment process is a comprehensive process and cannot be initiated with any team. People trained to perform the risk assessment have to be assembled together. These skills may not be available in house and may have to be out-sourced.

Moreover, the tools to perform the risk assessment may not exist and even the testing of some information systems may not be possible. For example, testing of embedded software requires different activities to be performed, variety of techniques and actors, and poses many complex challenges which makes it increasingly difficult and expensive [115]. Furthermore, the cost of the risk assessment itself might not justify the need for such an assessment. The risk assessment process itself might not produce any results. There might be many unknowns requiring additional information not available to the IPT. Therefore, incomplete information may create an inadequate level of detail for the management to take decisions.

The limitations described above are the same with any risk assessment, therefore, the incident prevention process performed by the IPT focuses on affected information systems, determined in the previous step of the process. However, the risk of focussing on specific information systems is of inaccurately identifying it. The trigger might be for a different information system, making the risk assessment results invalid and thereby being ineffective.

Step 4: Formulate Control Strategies

Finally, the control measures are suggested for both long-term and short-term risk by the IPT in this step of the process. The examples show that alternative are easily suggested by the team and is presented to the management. Decisions on the risk mitigation strategy is taken hence preventing a potential incident. The IPTs in both scenarios adapts the security controls preventing an attack, making the organisation more resilient to Information Security threats.

The formulation of control strategies after a risk assessment does not only depend on the results of the risk assessment. The objectives of the organisation, financial considerations, reputation implication, etc. also play a role. The IPT can take decisions based on the information it has at that time. However, the decision's effectiveness can only be evaluated in hindsight. There can also be unintended consequences with new risk created because of the strategy adopted. However, this process does not focus on the effectiveness of the control suggested because this incident prevention process is part of the preparation phase in the incident response lifecycle. The monitoring of controls is part of the overall Information Security Risk Management process and these activities are performed in the next phases of the ISRM process, therefore beyond the scope of this prevention process.

A limitation identified, is that the process does not focus on what the organisation should do with the information it did not prioritise. However, the risk still exists and has to be monitored as part of the incident prevention process.

9.2 Evaluation through expert interview

It is beneficial to validate the design process with security experts. It should be easy to set up the team, within the boundaries of the existing organisation. The organisation has to be willing to move from compliance to a security driven approach, hence creating an effective Information Security Risk Management system in the organisation.

Keeping this requirement in mind, the Incident Prevention Team was pitched to the director of a data protection firm during a 1.5-hour interview. This firm offers a unique insight because its perspective is to ensure Information Security in other organisations. It offers data security as a service to clients. Therefore, this company perceives the threat to Information Security proactively. This gave us a good opportunity to assess the benefit of the proposed Incident Prevention Team as compared to incident response teams within the company, and find insights into the process that may require improvements.

However, we acknowledge that some bias does exist in the results presented as a result of this interview. With the interviewee, from the field of security itself, his views are skewed towards the need for more security. A more balanced result can be obtained with more interviews with experts across different fields. However, this was not possible due to the limitations in the research set-up.

The design of the Incident Prevention Team and process was introduced in the beginning of the interview followed by a step-by-step evaluation of the process itself. This was further concluded with a discussion on the following questions.

1. Can the proposed Incident Prevention Team be established in organisations?
2. What is the added value of such an Incident Prevention Team in organisations?

The discussion the incident prevention process, establishing an IPT and its added value is summarised below.

9.2.1 Feedback overview

The interviewee from the company provided the following feedback on the proposed IPT. An IPT does not exist in the company interviewed. This feedback gives the following insights of the challenges likely to be faced by the IPT as perceived by the interviewee.

Step 1 on scanning for precursors, is a new approach in cyber incident management. The questions are based on cyber intelligence and are not easy to answer. While the questions III & V help to answer the core activity in this step, the questions I, II & IV are intelligence based. There is no right source. There is no complete, accurate, reliable and consistent information either. The value of the information depends on its interpretation by the IPT. However, these questions have to be asked to point the IPT in the right direction. Over time, the IPT would be able to develop the skills necessary to effectively and efficiently interpret the information. Therefore, these questions serve as a starting step towards scanning for precursors.

Step 2 on prioritise, is a subjective activity performed in this step by the IPT. Ideally, consensus is achieved in a perfect process. However, this depends on the organisation culture and dynamics between members of the IPT. Nevertheless, when decisions have to be taken under uncertain conditions, information is prioritised by the subjective preferences of the members in the IPT. Both questions VI & VII are valid questions and help to determine prioritise precursors in this step.

Step 3 on assess risk, is already in place within the company. In addition, questions VIII, IX & X are valid in this step, because it helps to determine risk in the organisation.

Step 4 on formulate control strategies also exists within the organisation but is part of the risk management activity. The interviewee acknowledges that often failure is due to a lack of correct implementation. Moreover, these control strategies have to be communicated, to raise the level of Information Security awareness in the organisation. In addition, question XI is valid, but the mechanism to ensure correct implementation has to be robust itself.

A key learning in the discussion about the process was the differentiation between the company performing the incident prevention process for the first time and then repeating the process. While the process designed is valid for the first time, there is a difference when the process is initiated thereafter. Since the scan for the information reveals new information, this process is relatively shorter. This is because there might be single precursors or only a few precursors since the last scan. Here we can see that Step 2, Prioritise and Step 3, Assess risk can tend to overlap with each other, with the precursors being triggers themselves. However, these steps are still valid since even with few precursors, the information has to be prioritised. A risk assessment on all information retrieved is not feasible and a distinction is made in this step. Nonetheless, there is always room for improvement as discussed in the challenges. The evaluation of the process was then followed by a discussion on the following two questions.

9.2.2 Establishing the Incident Prevention Team

Can the proposed Incident Prevention Team be established in organisations?

According to the interviewee, the proposed Incident Prevention Team can be established easily. The Incident Prevention Team can be implemented within organisations if there is flexibility in design allowing them to change it to suit their needs. This follows closely with the line of reasoning in this research that an Incident Prevention Team should be able to reuse the various elements of Information Security response as recommended in Section 8.1.1 on pre-requisites. Furthermore, there should be a direct link between top management and the IPT. This will help in quick decision-making or else the same cycle of incident response continues.

However, the interviewee also mentions that the establishment of IPT in the organisation depends on a number of factors. These include perceived economic benefits, political considerations, etc. For example, a distinction has to be made on whether it is set up internally or outsourced. This distinction depends on financial factors and resource availability.

Finally, the interviewee also commented that for his own organisations as an Information Security service provider, this IPT can be offered as a Information Security service to its clients. The scope of implementing this add-on-solution to data security is a business opportunity in itself.

9.2.3 Added value of the Incident Prevention Team

What is the added value of such an Incident Prevention Team in organisations?

The interviewee discussed that the value of the IPT is the outcome of the changes made on the recommendation of the IPT. These outcomes are also measurable. For example, the proof of concept can be witnessed if the organisation actually acts on the perceived threats to its information systems and prevents an incident that has a negative impact in another organisation. However, it is difficult to sell security, since it is not tangible and cannot be seen. According to the interviewee, the decision to implement an IPT can be justified to the management when the IPT presents its report on the threat analysis that it prevented.

The IPT adds further value because it is an on going process. The mind-set of the team is towards proactively ensuring Information Security. This is different from incident response teams, set up only when there is an incident of interest detected in the organisation.

Furthermore, the interviewee also commented that this approach offer a “niche” solution currently not available in the market, therefore justifying the research into the development of an IPT.

9.2.4 Interview Summary

After the discussion with the interviewee, the added value of the establishment of the Incident Prevention Team is justified from the perspective of the company as well. The need for Information Security depends on the perceived threat to the organisation. Even if the perceived threat is high, the decision on implementing state of the art security controls are motivated by different economic, political and other factors. These play a major role in how organisations are likely to implement such an Incident Prevention Team.

However, the interviewee mentioned that since not all incidents can be prevented, the concept of incident prevention has to be presented with the right expectations to the management. The success of the IPT should be measured in evaluating its risk as compared to the external organisations risk. This outcome is the real value of the Incident Prevention Team recommended in this research.

Moreover, the suggestion of the Incident Prevention Team offered as a service to other organisations was an interesting perspective that I did not consider in this research. The reuse of such an approach offers new business opportunities to organisations dealing in handling cyber incidents.

9.3 Summary

In this chapter, we performed the final phase of this research. The applicability of the Incident Prevention Team in organisations was tested with the help of two scenarios. The two scenarios offer a snapshot of the present case in cyber security indents today. These scenarios were further validated with an expert in the field. Changes to the scenario were made on the expert's suggestion. Therefore, these scenarios are comparable to present day Information Security practices. The scenarios helped to evaluate the incident prevention process followed by the Incident Prevention Team. The establishment of the IPT and its added value was further evaluated with a security expert from an Information Security organisation in the Netherlands.

The two example scenarios discussions reveal the effectiveness as well as the challenges in setting up an Incident Prevention Team. The differentiating factor in the process followed by the IPT as compared to other processes is the scanning for precursors required to prioritise information. In these first two steps, we see a proactive way of addressing Information Security. The final two steps, Information Security risk assessment process and formulation of control strategies are processes already familiar in the organisation. Therefore, these steps are easy to adapt in the incident prevention process. The characteristics of trigger, template, twitch and tweak help to differentiate different aspects of incident information for the IPT. This is a crucial aspect for the success of this team because it changes the perspective of how organisations view incidents. It also makes it easy to understand and therefore interpret information.

The expert interview also further helped in reaffirming the above lessons learned from the example scenarios. It also helps us understand the challenges associated with the implementation of an Incident Prevention Team. We also received feedback on its overall value. The major learning was the how this team can be operationalised by other companies as well to offer incident prevention as a service. In addition, a key learning was the differentiation between organisations performing the activity for the first time as to the subsequent incident prevention process performed in the organisation.

10 | Conclusion and Discussion

In this research, we propose the establishment of an Incident Prevention Team in organisations to proactively address the increasing demand for more resilient information systems. Using the phases of the Design Science Research Cycle, this research was structured. The research process aligned the theoretical concepts of risk management and incident response using the TIP design perspective with inputs from industry security experts for the design of the Incident Prevention Team.

The main research question, *"**How can an incident prevention process be developed to proactively use information available to complement Information Security Risk Management in organisations?**"* was answered. This research proposes to ***Establish an Incident Prevention Team*** aligning elements of Information Security Risk Management in a 4-step ***Incident Prevention Process*** (Figure 5 on page 47). The input, activities and output for each of the step of the process were further described in detail in Chapter 8 *Design: Incident Prevention Team.*

10.1 Reflection on Research Goals

This section of the report will now reflect upon the goal knowledge obtained in the form of answer to the various research sub-questions described in Section 2.1 *Research Goals.*

(SQ 1) *What is the missing link in Information Security Risk Management?*
The inability to address dynamic information was identified as the missing link in Information Security Risk Management, described in Chapter 5 *Aligning Risk Management and Incident Response.* The research identified that organisations struggle to manage incidents even after the establishment of Incident Response Teams. A literature review on the subject of Information Security Risk Management showed that the process is backward looking, therefore failing to fully achieve its goal. Therefore, precursors was identified as the characteristic of incident information to prevent incidents. A differentiation is made between precursors and indicators as the first ingredient in Chapter 6.

(SQ 2) *What characteristics can be used to interpret incident information?*
In Chapter 7 we identify triggers, templates and twitch from Vigilant Information Systems as a means to interpret incident information. This is further extended by tweak to describe the action taken by the Incident Prevention Team. Since the team consists of different members, with a variety of skills, there should be a common understanding of information to interpret information.

(SQ 3) *What are the main operational tasks to be performed?*
A 4-step incident prevention process is proposed for the Incident Prevention Team to perform its function. In Step 1 precursors are scanned and triggers determined; Step 2 is to prioritise triggers for Step 3, the risk assessment process. Finally, in Step 4 the IPT formulates control strategies to manage the risk determined in the risk assessment step.

These steps elaborated in Chapter 8 of the report, were designed to structure the incident prevention process to be incorporated in the preparation phase of the incident response lifecycle.

(SQ 4) *What is the added value of the design solution in case of cyber incidents?*
Establishing the Incident Prevention Team adds value in the preparation phase of the incident response lifecycle for cyber incidents. This is because the current preparation phase does not focus on incident prevention. Therefore the incident prevention process can effectively prevent incidents with the help of precursors because it changes the perspective of how the organisation views information about incidents.

The process of incident prevention is evaluated in Chapter 9 with cyber incident scenarios and an expert interview. The benefit to Information Security is seen in the forward-looking perspective of actively scanning and interpreting information readily available.

Reflecting upon the operation knowledge of the proposed Incident Prevention Team, we find that the use of TIP design perspectives helped to develop the incident prevention process. The technical artifacts described in risk assessment and incident response was reused. Specifically, the risk assessment was used in the 3rd step of the incident prevention process, while the resources of the incident response team is used to set up the incident prevention team. However, the institutional artifact at Level 4 about the norms and values of Information Security requires major change. This is done with the support of the top management designed as a pre-requisite for the establishment of the IPT. If the IPT is successfully established in the organisation, the norm of proactive Information Security can be achieved through the active scanning of precursors, which also increasing the awareness of cyber incidents within the organisation. Therefore, creating a forward-looking perspective of viewing cyber incidents from its current approach.

We will now summarise the main recommendations derived from this research, the scientific contributions, the research limitations and suggest potential ideas for future research in the next sections of this chapter.

10.2 Contributions

This research contributes to the existing field of Information Security research. The main scientific contributions is that this research addresses the lack of attention given to Incident Prevention. It brings attention to the need for focus on incident prevention in the preparation phase of the incident response lifecycle. We summarise the main contributions of this work below.

1. Firstly, the research describes the organisation's approach to managing incidents today. From the current state of Information Security Risk Management, we find that organisations are backward looking and struggling to manage incidents. This is indicated by the increasing trend of cyber incidents. However, it also finds that in some cyber incidents, the information was available prior to incident. Therefore, the need for a forward-looking approach of incident prevention.

2. The research makes a clear demarcation of incident information. It differentiates between precursors and indicators with respect to the time of detection of incidents, described in Figure 4, *Classification of Information* on page 33. This helps us to select precursors as the information source according to which the process of incident prevention can be carried out.

It also helps to understand the dynamic nature of information that can be used to proactively address Information Security risk.

3. Furthermore, this research makes use of triggers, templates and twitch from Vigilant Information Systems [93], to structure incident information. This was further extended by the concept of tweak describing the action to be taken by the incident prevention team to mitigate risk. These concepts, offer new insights into the interpretation of information and helps to create a shared understanding of information for Information Security professionals. With diverse stakeholders in Information Security Risk Management, these characteristics translate raw information into value, thereby easing the decision making process.

4. Finally, we integrate the key findings and recommend organisations to establish an Incident Prevention Team. The key activities performed by this Incident Prevention Team to achieve its goal is described in a 4-step *Incident Prevention Process* (Figure 5 on page 47). This addresses the lack of attention given to incident prevention. Therefore the discrepancy in balance between the prevention and detection of Information Security incidents is reduced, thereby, being very relevant to maintaining Information Security.

By establishing the Incident Prevention Team, it creates an agile structure within the organisation that proactively understands risk to Information Security. It is agile because the incident prevention team is set up along similar lines of present incident response teams using the available resources. Furthermore, the Risk management tool of Risk Assessment is reused on the affected information system. Therefore, this process can be easily integrated into the organisation. Furthermore, the Incident prevention process is a structured process. The step-by-step approach, offers a guide for the Incident Prevention Team to follow in order to perform its function effectively and efficiently. It also includes key questions that the IPT can ask while performing the activities enumerated in the individual steps of the process described in Chapter 8 *Design: Incident Prevention Team*.

However, the aim of such a team is not to prevent all incidents. This is not possible. But the goal is to be able to prevent high impact incidents using information available by interpreting signs in the information of incidents already taken place. Thereby we can conclude, with this forward looking approach the proposed establishment of an Incident Prevention Team, can create a more resilient Information Security Risk Management system in the organisation. This will increase the awareness of Information Security of both the internal and external environment simultaneously therefore benefiting society as a whole.

10.3 Limitations

Every research has its limitations and this section will now describe the major ones identified in this research. The main limitation and hence opportunity for further research, is the lack of empirical testing of the proposed Incident Prevention Team. This process requires time, resources, expertise and flexibility for researchers to test findings in a practical environment. This was not possible during the thesis project due to its setup.

Furthermore, this research was not designed with a specific organisation's business requirements. The design of the proposed team and its process was generalised to allow for the designs adoption in any organisation. This also brings in limitations to testing the effectiveness of the Incident Prevention Team. While questions are suggested to help the IPT perform the activities in the process suggested, it is not a comprehensive list. These questions can be further detailed depending on the organisation's requirements.

Even though two Information Security experts (External Supervisors) from two diverse organisations provided input to this research, the scope was still on a high level approach to incident prevention. One security expert is a consultant with 20 years of experience in the field; hence, his input was a valuable source of information. However, this also means that some amount of bias does exists in the research findings both from me as a researcher as well as from the security expert. Furthermore, the expert interview was also from a security firm, therefore making the results of this research biased towards the need for such an Information Security approach.

Another limitation identified is the lack of a cost-benefit analysis on establishing the IPT. During the expert interview, we found that it is easy to establish such an Incident prevention team. Even with the IPT designed utilising common resources from the IRT, there is still a cost associated with the set up of such a team, which is not explored in this research. Furthermore, the goals and perspective of the incident prevention team is different compared to IRTs. Therefore, the difference from a social aspect of organisational research is not addressed.

10.4 Future Research

The establishment of an Incident Prevention Team is not described in the literature on Information Security. Therefore, there is still a lot to research and implement in this area.

The limitations mentioned in the previous section can be used to continue researching Information Security incident prevention from an organisational perspective. The socio-technical aspect of the incident prevention team is a promising field of research that can be explored further. The learning's can then be used to further improve the incident prevention process.

More companies could be asked for feedback on the incident prevention process to see its applicability across a variety of industries. This research was validated with a security expert in the field and there exists certain bias in the results presented. Furthermore, empirical testing can be used to validate the proposed incident prevention process.

While a number of tools exist that perform the same function of incident prevention, it is primarily described in the preparation phase of the Incident Response process. However, this research, introduces the lack of attention given to incident prevention which can be further extended in subsequent research.

We acknowledge that not everything can be prevented. During the research we noticed that the success of the proposed IPT depends on the availability of information. Therefore, the further categorisation of precursors to determine the extent to which information is available, for incident prevention is a possibility for further research. A few other possibilities of future research, based on the feedback received from Information Security experts, was to extend the scope of IPTs. The method of red teaming, in which the IPT will test the Information Security effectiveness by method of active penetration testing, was suggested. These methods can then be used to develop and extend the capabilities of the Incident Prevention Team.

Appendices

A
Diversity of security threats

We now describe the diversity of security threats based on different literature, summarised in Chapter 1.

Based on online attacks

Hypponen (2011), states that threats can be grouped together on the types of online attacks in cyberspace [13]

- Online criminals who are motivated by money, fame, peer approval, etc.
- Hacktivists who are motivated by personal or popular causes.
- Nation States who now wage war in the 5th domain of cyberspace.

Based on threat vectors

Organisations are targeted by a variety of threat vectors as well. These are broadly categorised in to supply chain and vendor access, remote access, proximity access, and insider access [14].

- **Supply Chain and Vendor access**
  With the interconnected nature of the global supply chain systems, organisations have a steep challenge in addressing not only its security vulnerabilities but also the vulnerabilities of partners across the value chain. For example, the data breach at Target in December 2013 was done via a malware email phishing attack sent to employees at an HVAC firm leading to access of the Point of Sale System at Target. This resulted in an estimated loss of $200 million [49].
- **Remote Access**
  The commonly detected source of threat is external intrusions. Here we see that there are many software tools able to detect and highlight potential intrusions in a network. However the challenge still remains in accurately identifying and mitigating the threat before it is executed. For example, the hacking of Snapchat in December 2013 by Gibson Security, exposed the vulnerability in the photo sharing app [116].
- **Proximity Access**
  This refers to the ability of adversaries to access the internal networks of an organisation by being close to a network source and not physically inside the network. For example, a hacker repeatedly hacked into his neighbours Wi-Fi network and used it to send threatening emails to politicians [117].
- **Insider Access**
  Employees, contractors and trusted service and business partners have the unique opportunity of posing potential harm to the organisation. This provides a unique challenge since these

people know gaps in the companies policy enforcement. For example, from February to April 2000 an ex-employee intentionally caused raw sewage to spill out into local parks and rivers on at least 46 occasions in Queensland, Australia [118].

Based on target

Based on the target both public and private targets are susceptible to attacks. This is illustrated in the examples below.

- **Public**
  Government and public organisations are frequently the target of many attacks. From political adversaries to hacktivist, these institutions are frequently attacked. Examples include, the Estonian government networks were attacked by a denial of service attack in April 2007. The computer networks in Georgia were hacked and graffiti appeared on the websites in August 2008. Israel's Internet infrastructure was attacked in January 2009. Stuxnet was discovered in Siemens Industrial control systems targeting Iran's nuclear facilities in October 2010. South Korean financial institutions had their networks infected in March 2013 [7].

- **Private**
  Both large and small businesses are targeted without distinction. Reports indicate that these businesses are more prone to attacks with the lack of sophisticated security control measures. Symantec [119] reports that the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees with 31% of all attacks targeted them. For example, the Heartland Payment Systems were impacted in March 2008 when 134 million credit cards were exposed. Sony's PlayStation Network was affected in April 2011 when 77 million PlayStation Network accounts were hacked. The University of North Carolina was affected in February 2012 when over 350,000 records were breached in two separate incidents [120, 121].

- **Personal**
  Cryptolocker ransomware was discovered in 2013 that used high-grade encryption against victim's files.

B | Dynamic changes to Information Security environment

We now describe the dynamic changes to the Information Security environment on the basis of technology and work environment, summarised in Chapter 1.

Technology

The following examples illustrate the dynamic changes in technology to the security environment.

- Mobile Internet has become increasingly inexpensive. This technology has gained great strides with capability of mobile computing devices and Internet connectivity given to every user with a phone. People around the world are using this technology and businesses have had to react to this change. Often implemented before they are secured [15].
- Cloud computing is the use of computer hardware and software resources as a service delivered over a network or the Internet [15]. This reduces cost of set up and maintenance of large IT services. A number of start-ups use this technology since it offers a low entry barrier into businesses. However they run the risk of non-secured services and create a potential risk to their businesses.
- BYOD (bring your own device) are often implemented before they are secured. With increased mobility of IT devices, employees increasingly want to use their own personal mobile devices to conduct work. Use of technology generally lags behind personal devices used. BYOD creates an attractive option to reduce cost and at the same time increase employee productivity. The risk landscape here is across areas of mobile devices, mobile apps and the mobile environment itself [122]. Thereby creating serious challenges to security.

Work Environment

The following examples illustrate the dynamic changes in the work environment in organisations today.

- Work Environment has a certain cyclic nature with the changing environment of work during the day is different from that during the night. Security permissions are different in theses environments. With people working from home, organisations have to be flexible to allow for this change to happen. However this also creates the need for different security control measures that have to be implemented to cater to this change.
- With an International outlook, information flows across servers located around the world. Various security controls have to be created for each of the areas that the business operates. They have to further comply with local laws and regulations and with changing political, legal and regulatory requirements constantly across the world. This creates a challenge in ensuring that multiple security control measures are implemented across the system.

C | Data breach analysis

The Table 1 below compares the data breaches between Target and Home Depot against different categories used as input in Chapter 1.

Categories	**Target (TGT)**	**Home Depot (HD)**
Business	Retailer	Home Supply Retailer
Timeline	Nov. 27 - Dec. 15, 2013	April 2014 - Sept 2014
Detected	Dec 12, 2013 by external organisation	September 2014, by external organisation
Public Notification	Dec 19, 2013	Sept 8, 2014
Time Period	3 Weeks	6 Months
Attack Origin	network access to a third-party vendor HVAC	Investigation in progress
Type of Attack	Malware	Malware
Attack Tool	BlackPOS	Backoff or alleged BlackPOS
Business System	POS systems	POS systems running Microsoft Windows
Impact	40 Million Credit + Debit Cards (+ additional 70 million Customer personal information)	60 Million Credit + Debit Cards
Estimated Losses	$200 million	$2 Billion
Counter Measures	Will introduce chip-and-PIN technology by 2015	Roll out of Chip + Pin security at stores
Failure in Policies	Didn't respond to warnings from automated anti intrusion software. Vendor credentials moved from less sensitive areas to customer data.	Older antivirus software used on the PoS system. (Investigation in progress)

Table 1: Target Vs. Home Depot, data breach comparison, [49, 123, 124, 96, 125, 126]

Bibliography

[1] R. L. Daft and K. E. Weick, "Toward a model of organizations as interpretation systems," *Academy of management review*, vol. 9, no. 2, pp. 284–295, 1984.

[2] S. Barrett and B. Konsynski, "Inter-organization information sharing systems," *MIS Quarterly*, pp. 93–105, 1982.

[3] M. Alavi and D. E. Leidner, "Knowledge management systems: issues, challenges, and benefits," *Communications of the AIS*, vol. 1, no. 2es, p. 1, 1999.

[4] M. Castells, *The rise of the network society: The information age: Economy, society, and culture*, vol. 1. John Wiley & Sons, 2011.

[5] E. Brynjolfsson, "Wired for innovation: How information technology is reshaping the economy," *MIT Press Books*, vol. 1, 2011.

[6] G. L. Kovacich and E. P. Halibozek, *Security metrics management: How to measure the costs and benefits of security.* Butterworth-Heinemann, 2006.

[7] NATO, "The history of cyber attacks - a timeline." [Online], Retrieved on 10th April, 2014, Available: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, 2014.

[8] Codenomicon, "Heartbleed." [Online], Retrieved on 15th Sept, 2014, Available: http://heartbleed.com, 2014.

[9] J. Ma, C. Wang, and Z. Ma, "Adaptive security policy," in *Security Access in Wireless Local Area Networks*, pp. 295–329, Springer, 2009.

[10] K. D. Loch, H. H. Carr, and M. E. Warkentin, "Threats to information systems: today's reality, yesterday's understanding," *MIS Quarterly*, pp. 173–186, 1992.

[11] M. E. Whitman, "In defense of the realm: understanding the threats to information security," *International Journal of Information Management*, vol. 24, no. 1, pp. 43–57, 2004.

[12] T. Rid, "Cyber war will not take place," *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5–32, 2012.

[13] M. Hypponen, "Three types of online attack." [Online], Retrieved on 15th Sept, TEDxBrussels, TEDX, Editor, 2011.

[14] S. R. Chabinsky, "Cybersecurity strategy: A primer for policy makers and those on the front line," *J. Nat'l Sec. L. & Pol'y*, vol. 4, p. 27, 2010.

[15] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*, vol. 180. McKinsey Global Institute San Francisco, CA, 2013.

[16] T. L. Friedman, *The world is flat: The globalized world in the twenty-first century.* Penguin London, 2006.

[17] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *NIST Special Publication*, vol. 800, no. 30, pp. 800–30, 2002.

[18] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-K. Lee, and H. Lee, "Enforcing access control using risk assessment," in *Universal Multiservice Networks, 2007. ECUMN'07. Fourth European Conference on*, pp. 419–424, IEEE, 2007.

[19] Verizon, "2014 data breach investigations report," tech. rep., Verizon Enterprise, 2014.

[20] pwc, "Managing cyber risks in an interconnected world," tech. rep., pwc, 2014.

[21] S. Caponi, "Cybersecurity trends for 2014." [Online], Retrieved on 1st October, 2014, Available: http://www.corporatecomplianceinsights.com/cybersecurity-trends-for-2014/, 2014.

[22] L. Marinos, "Threat landscape 2013, overview of current and emerging cyber-threats," tech. rep., ENISA, 2013.

[23] P. Wood, "Internet security," Tech. Rep. 19, Symantec Corporation, 2014.

[24] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, p. 61, 2012.

[25] S. Mitropoulos, D. Patsos, and C. Douligeris, "On incident handling and response: A state-of-the-art approach," *Computers & Security*, vol. 25, no. 5, pp. 351–370, 2006.

[26] F. C. Freiling and B. Schwittay, "A common process model for incident response and computer forensics," *IMF*, vol. 7, pp. 19–40, 2007.

[27] B. Horne, "On computer security incident response teams," *Security & Privacy, IEEE*, vol. 12, no. 5, pp. 13–15, 2014.

[28] ISO/IEC27005:2011, "Information technology - security techniques - information security risk management," Geneva, Switzerland, 2011.

[29] ISO/IEC27035:2011, "Information technology - security techniques - information security incident management," Geneva, Switzerland, 2011.

[30] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, nist800-30 and microsoft's security management guide," in *Availability, Reliability and Security, 2009. ARES'09. International Conference on*, pp. 726–731, IEEE, 2009.

[31] B. Kuechler and V. Vaishnavi, "On theory development in design science research: anatomy of a research project," *European Journal of Information Systems*, vol. 17, no. 5, pp. 489–504, 2008.

[32] P. W. Bots and C. E. van Daalen, "Designing socio-technical systems: Structures and processes," in *proceedings of Third International Engineering Systems Symposium*, 2012.

[33] ISO/IEC27001:2013, "Information technology - security techniques - information security management systems - requirements," Geneva, Switzerland, 2013.

[34] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *proceedings of 2001 workshop on New security paradigms*, pp. 97–104, ACM, 2001.

[35] D. Ionita, "Current established risk assessment methodologies and tools," Master's thesis, Universiteit Twente, 2013.

[36] R. Murray-Webster *et al.*, *Management of risk: guidance for practitioners.* The Stationery Office, 2010.

[37] G. Locke and P. D. Gallagher, "Managing information security risk," 2011.

[38] D. Wawrzyniak, "Information security risk assessment model for risk management," in *Trust and Privacy in Digital Business*, pp. 21–30, Springer, 2006.

[39] G. E. Apostolakis, "How useful is quantitative risk assessment?," *Risk analysis*, vol. 24, no. 3, pp. 515–520, 2004.

[40] L. Sun, R. P. Srivastava, and T. J. Mock, "An information systems security risk assessment model under the dempster-shafer theory of belief functions," *Journal of Management Information Systems*, vol. 22, no. 4, pp. 109–142, 2006.

[41] T. O. Group, "Requirements for risk assessment methodologies." [Online], Retrieved on 10th October, 2014, Available: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12158,, 2009.

[42] ENISA, "Inventory of risk management / risk assessment methods." [Online], Retrieved on 10th October, 2014, Available: http://rm-inv.enisa.europa.eu/methods, 2014.

[43] W. Al-Ahmad and B. Mohammad, "Addressing information security risks by adopting standards," *International Journal of Information Security Science*, vol. 2, no. 2, pp. 28–43, 2013.

[44] E. Humphreys, "Information security management standards: Compliance, governance and risk management," *information security*, vol. 13, no. 4, pp. 247–255, 2008.

[45] K. P. Kossakowski, J. Allen, C. Alberts, C. Cohen, and G. Ford, "Responding to intrusions," tech. rep., DTIC Document, 1999.

[46] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "Pfires: a policy framework for information security," *Communications of the ACM*, vol. 46, no. 7, pp. 101–106, 2003.

[47] C. Prosise, K. Mandia, and M. Pepe, *Incident response and computer forensics.* McGraw-Hill/Osborne, 2003.

[48] R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: the diagnostic work of it security incident response," *Information Management & Computer Security*, vol. 18, no. 1, pp. 26–42, 2010.

[49] S. J. Rockefeller, "A kill chain analysis of the 2013 target data breach," tech. rep., Committee on Commerce, Science and Transportation, 2014.

[50] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams - challenges in supporting the organisational security function," *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[51] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "Organizational models for computer security incident response teams (csirts)," tech. rep., DTIC Document, 2003.

[52] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security," *Reliability Engineering & System Safety*, vol. 92, no. 6, pp. 745–754, 2007.

[53] J. Wiik, J. J. Gonzalez, H. F. Lipson, and T. J. Shimeall, "Dynamics of vulnerability-modeling the life cycle of software vulnerabilities," in *Proceedings of 22nd International System Dynamics Conference*, 2004.

[54] G. B. White and D. J. DiCenso, "Information sharing needs for national security," in *in proceedings of 38th Annual Hawaii International Conference on System Sciences, HICSS'05.*, pp. 125c–125c, IEEE, 2005.

[55] B. R. Pandey, "Indicators for ict security incident management," Master's thesis, Norwegian University of Science and Technology, 2013.

[56] J. J. Gonzalez, "Towards a cyber security reporting system–a quality improvement process," in *Computer Safety, Reliability, and Security*, pp. 368–380, Springer, 2005.

[57] O. E. Williamson, "Transaction cost economics: how it works; where it is headed," *De economist*, vol. 146, no. 1, pp. 23–58, 1998.

[58] J. Koppenjan and J. Groenewegen, "Institutional design for complex technological systems," *International Journal of Technology, Policy and Management*, vol. 5, no. 3, pp. 240–257, 2005.

[59] D. Smith, "Forming an incident response team," in *Proceedings of the FIRST Annual Conference*, 1994.

[60] E. E. Schultz Jr, D. S. Brown, and T. A. Longstaff, "Responding to computer security incidents: Guidelines for incident handling," tech. rep., Lawrence Livermore National Lab., CA (USA), 1990.

[61] ISO/IEC27032:2012, "Information technology - security techniques - guidelines for cybersecurity," Geneva, Switzerland, 2012.

[62] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," *Journal of Information Security*, vol. 4, p. 92, 2013.

[63] N. C. S. Centre, "Checklist security of ics/scada systems," 2012.

[64] N. C. for Security and Counterterrorism, "National cyber security strategy 2, from awareness to capability," 2013.

[65] Y. Poullet, "Eu data protection policy. the directive 95/46/ec: Ten years after," *Computer Law &amp; Security Review*, vol. 22, no. 3, pp. 206–217, 2006.

[66] S. Posthumus and R. Von Solms, "A framework for the governance of information security," *Computers &amp; Security*, vol. 23, no. 8, pp. 638–646, 2004.

[67] D. Ashenden, "Information security management: A human challenge?," *Information Security Technical Report*, vol. 13, no. 4, pp. 195–201, 2008.

[68] A. Hopkins, "Studying organisational cultures and their effects on safety," *Safety Science*, vol. 44, no. 10, pp. 875–889, 2006.

[69] S. L. Barton and P. J. Gordon, "Corporate strategy and capital structure," *Strategic management journal*, vol. 9, no. 6, pp. 623–632, 1988.

[70] P. Zhang, M. Scialdone, and M.-C. Ku, "It artifacts and the state of is research," *International Conference on Information Systems*, no. 14, 2011.

[71] C. D. Ittner and D. F. Larcker, "Coming up short on nonfinancial performance measurement," *Harvard business review*, vol. 81, no. 11, pp. 88–95, 2003.

[72] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[73] J. Eloff and M. Eloff, "Information security architecture," *Computer Fraud &amp; Security*, vol. 2005, no. 11, pp. 10–16, 2005.

[74] N. Feng and M. Li, "An information systems security risk assessment model under uncertain environment," *Applied Soft Computing*, vol. 11, no. 7, pp. 4332–4340, 2011.

[75] G. V. Post and A. Kagan, "Evaluating information security tradeoffs: Restricting access can interfere with user tasks," *Computers & Security*, vol. 26, no. 3, pp. 229–237, 2007.

[76] W. H. Baker and L. Wallace, "Is information security under control?: Investigating quality in information security management," *Security &amp; Privacy, IEEE*, vol. 5, no. 1, pp. 36–44, 2007.

[77] A. G. Kotulic and J. G. Clark, "Why there aren't more information security research studies," *Information & Management*, vol. 41, no. 5, pp. 597–607, 2004.

[78] D. B. Parker, "Risks of risk-based security," *Communications of the ACM*, vol. 50, no. 3, p. 120, 2007.

[79] Reuters, "Microsoft fixes 19-year-old windows bug." [Online], Retrieved on 26th Nov, 2014, Available: http://www.reuters.com/article/2014/11/12/microsoft-cybersecurity-idUSL3N0T260H20141112, 2014.

[80] S. S. Nagaraju, C. Craioveanu, E. Florio, and M. Miller, "Software vulnerability exploitation trends," tech. rep., Microsoft Corporation, 2013.

[81] C. Pak and J. Cannady, "Asset priority risk assessment using hidden markov models," in *Proceedings of the 10th ACM conference on SIG-information technology education*, pp. 65–73, ACM, 2009.

[82] A. Ekelhart, S. Fenz, and T. Neubauer, "Ontology-based decision support for information security risk management," in *proceedings of Fourth International Conf. on Systems*, pp. 80–85, IEEE, 2009.

[83] O. Kulikova, R. Heil, J. van den Berg, and W. Pieters, "Cyber crisis management: A decision-support framework for disclosing security incident information," in *proceedings of 2012 International Conference on Cyber Security*, pp. 103–112, IEEE, 2012.

[84] R. Nicolas, "Knowledge management impacts on decision making process," *Journal of knowledge management*, vol. 8, no. 1, pp. 20–31, 2004.

[85] W. Jansen, *Directions in security metrics research.* DIANE Publishing, 2010.

[86] R. C. Chandler, "Message mapping: How to communicate during the six stages of a crisis," tech. rep., Everbridge, 2009.

[87] S. Liu and B. Cheng, "Cyberattacks: Why, what, who, and how," *IT professional*, vol. 11, no. 3, pp. 14–21, 2009.

[88] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Critical Infrastructure Protection*, pp. 73–82, 2007.

[89] ICS-CERT, "Cyber threat source descriptions." [Online], Retrieved on 22nd June, 2014, Available: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions, 2014.

[90] B. Morrow, "Byod security challenges: control and protect your most sensitive data," *Network Security*, vol. 2012, no. 12, pp. 5–8, 2012.

[91] R. Westervelt, "Heartbleed attack linked to community health systems breach." [Online], Retrieved on Sept 10th, 2014, Available: http://www.crn.com/news/security/300073776/heartbleed-attack-linked-to-community-health-systems-breach.htm, 2014.

[92] A. Arora, A. Nandkumar, and R. Telang, "Does information security attack frequency increase with vulnerability disclosure? an empirical analysis," *Information Systems Frontiers*, vol. 8, no. 5, pp. 350–362, 2006.

[93] J. G. Walls, G. R. Widmeyer, and O. A. El Sawy, "Building an information system design theory for vigilant eis," *Information systems research*, vol. 3, no. 1, pp. 36–59, 1992.

[94] O. A. El Sawy and T. C. Pauchant, "Triggers, templates and twitches in the tracking of emerging strategic issues," *Strategic Management Journal*, vol. 9, no. 5, pp. 455–473, 1988.

[95] NIST, "National vulnerability database." [Online], Retrieved on 20th Sept, 2014, Available: http://nvd.nist.gov, 2014.

[96] Krebs, "In wake of confirmed breach at home depot, banks see spike in pin debit card fraud." [Online], Retrieved on 10th Sep, 2014, Available: https://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/, 2014.

[97] B. Grubb, "Heartbleed disclosure timeline: who knew what and when." [Online], Retrieved on 15th Sept, 2014, Available: http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html, 2014.

[98] J. Heller, "Anonymous announces oppetrol attack on local oil and gas companies." [Online], Retrieved on 10th September, 2014, Available: http://www.ibtimes.com/anonymous-announces-oppetrol-attack-local-oil-gas-companies-video-1267817, 2013.

[99] E. H. Spafford, "A failure to learn from the past," in *proceedings of 19th Annual Computer Security Applications Conference*, pp. 217–231, IEEE, 2003.

[100] B. Yurcan, "Staying prepared for cyber attacks." [Online], Retrieved on 13th October, 2014, Available: http://www.banktech.com/fraud/staying-prepared-for-cyber-attacks/a/d-id/1297718, 2014.

[101] R. Koch, B. Stelte, and M. Golling, "Attack trends in present computer networks," in *proceedings of 4th International Conference on Cyber Conflict (CYCON), 2012*, pp. 1–12, IEEE, 2012.

[102] D. Kushner, "The real story of stuxnet," *Spectrum, IEEE*, vol. 50, no. 3, pp. 48–53, 2013.

[103] M. R. Baer, "Cyber disarmament treaties & the failure to consider adequately zero-day threats," in *The Int'l Conference on I-Warfare & Security*, 2013.

[104] J. W. Lainhart IV, "Cobit™: A methodology for managing and controlling information and information technology risks and vulnerabilities," *Journal of Information Systems*, vol. 14, no. s-1, pp. 21–25, 2000.

[105] W. Van Grembergen, "Strategies for information technology governance," tech. rep., IGI Global, 2004.

[106] K. Braa and R. Vidgen, "Interpretation, intervention, and reduction in the organizational laboratory: a framework for in-context information system research," *Accounting, Management and Information Technologies*, vol. 9, no. 1, pp. 25–47, 1999.

[107] D. Dimov, "Differences between the privacy laws in the eu and the us." [Online], Retrieved on 24th Oct, 2014, Available: http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/., 2013.

[108] HHS, "Breaches affecting 500 or more individuals." [Online], Retrieved on 24th October, 2014, Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html, 2014.

[109] US-CERT, "Cve-2014-0160." [Online], Retrieved on 15th Sep, 2014, Available: https://www.us-cert.gov/ncas/alerts/TA14-098A, 2014.

[110] V. Avelar, "Guidelines for specifying data center criticality/tier levels," *Lamda Hellix*, 2007.

[111] J. Mello, "Control system hack at manufacturer raises red flag." [Online], Retrieved on 24th Oct, 2014, Available: http://www.csoonline.com/article/2133252/application-security/control-system-hack-at-manufacturer-raises-red-flag.html., 2013.

[112] ICS-ALERT-12-195-01, "Tridium niagara vulnerabilities." [Online], Retrieved on 24th October, 2014, Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-195-01, 2012.

[113] CPNI, "Information exchanges." [Online], Infomation Retrieved on 10th October, 2014, Available: http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/, 2014.

[114] Z. Zetter, "Vulnerability lets hackers control building locks, electricity, elevators and more." [Online], Retrieved on 25th Oct, 2014, Available: http://www.wired.com/2013/02/tridium-niagara-zero-day/., 2013.

[115] A. Bertolino, "Software testing research: Achievements, challenges, dreams," in *2007 Future of Software Engineering*, pp. 85–103, IEEE Computer Society, 2007.

[116] J. Vincent, "Snapchat hack: 4.6 million users have been affected." [Online], Retrieved on 10th Sep, 2014, Available: http://www.independent.co.uk/life-style/gadgets-and-tech/snapchat-hack-46-million-users-affected-9033983.html, 2014.

[117] D. Kravets, “Wi-fi-hacking neighbor sentenced to 18 years.” [Online], Retrieved on 15th Sept, 2014, Available: http://edition.cnn.com/2011/TECH/web/07/13/wifi.hacking. neighbor. sentenced. wired/, 2011.

[118] M. Abrams and J. Weiss, “Malicious control system cyber security attack case study–maroochy water services, australia,” tech. rep., McLean, VA: The MITRE Corporation, 2008.

[119] Symantec, “Internet security,” Tech. Rep. 18, Symantec Corporation, 2013.

[120] DarkReading, “6 biggest breaches of 2012 so far.” [Online], Retrieved on Sept, 2014, Available: http://www.darkreading.com/application-security/database-security/6-biggest-breaches-of-2012-so-far/d/d-id/1137899?, 2012.

[121] T. Armerding, “The 15 worst data security breaches of the 21st century.” [Online], Retrieved on Sept, 2014, Available: http://www.csoonline.com/article/700263., 2012.

[122] EY, “Bring your own device security and risk in mobile device programs,” tech. rep., EY, 2013.

[123] P. Clark, “How main street will pay for home depot’s data breach.” [Online], Retrieved on 10th Sep, 2014, Available: http://www.businessweek.com/articles/2014-09-16/home-depot-breach-why-small-merchants-will-pay., 2014.

[124] N. Bose, “Home depot confirms security breach following target data theft.” [Online], Retrieved on 10th Sep, 2014, Available: http://www.reuters.com/article/2014/09/09/us-usa-home-depot-databreach-idUSKBN0H327E20140909., 2014.

[125] M. Lipka, “Home depot hack could lead to $3 billion in fake charges.” [Online], Retrieved on 10th Sep, 2014, Available: http://www.cbsnews.com/news/credit-monitoring-company-home-depot-breach-could-result-in-2b-in-fraud/., 2014.

[126] VenkatB., “Data security dos & don’ts from the target breach.” [Online], Retrieved on 10th September, 2014, Available: http://www.darkreading.com/attacks-and-breaches/data-security-dos-and-donts-from-the-target-breach-/d/d-id/1113830., 2014.

THE INCIDENT PREVENTION TEAM

A proactive approach to Information Security

Submitted on January 6th, 2015