

Hidden A. Ynion

Internal Information Security Management

Creating a Practical Security Process for a BPO

Helsinki Metropolia University of Applied Sciences

Master's Degree

Industrial Management

Master's Thesis

06 May 2016

Coming to this foreign land is the biggest adventure of my life. Taking the plunge to apply in a master's degree and to be accepted in one of the countries' universities is an opportunity of a lifetime. Moving to our new house in the middle of the thesis is excitingly crazy. Now it's the end of the line, and I am glad that I've survived all those grueling months.

I would like to express my heartfelt 'Thank You' to the university and to the people who, at one point or another, made this journey worthwhile.

To all of my instructors, I am in constant awe of the amount of knowledge, experience, and expertise you demonstrate in different areas of industrial management. A special shout out to:

- Dr. Rohweder, who tirelessly listens to my concerns during those meetings we had to discuss my thesis. Thank you for the encouragement and all those cheers and words of praise during presentations.
- Dr. Teerikangas, who exhibits an aura of positivity, energy, and genuine enthusiasm to teach and mentor, some attributes that I would want to emulate.
- Ms. Zinaida Grabovskaia and Ms. Sonja Holappa, who patiently understands my texts and help me in writing them the 'thesis way'. ☺

To my classmates, especially to my constant companions, I cherish those chats, the lunch-outs, and exchange of thoughts we had. I am grateful for the friendship I've made with most, if not all, of you, and I am appreciative of this chance to learn with you.

To my case company and to those interviewees from other companies who trusted me with the information that shouldn't have left the corners of their office, thank you.

To my parents, who always believe that I can make things happen, '*salamat*'.

To my buddy and my occasional chef, also known as my husband ☺, thank you for the treats on my little victories, for constantly inspiring me, and for putting up to all my whining moments when in reality I just really wanted to weep. Now I can spend more time with you strolling and enjoying those movie marathon nights.

This is one great experience I had with all of you. Thank you from the bottom of my heart.

Hidden Arroyo-Ynion
Helsinki, 06 May 2016

Author(s) Title	Hidden A. Ynion Internal Information Security Management Creating a Practical Security Process for a BPO
Number of Pages Date	89 pages + 12 appendices 06 May 2016
Degree	Master of Engineering (MEng)
Degree Programme	Industrial Management
Instructor(s)	Dr. Thomas Rohweder , DSc, Principal Lecturer Zinaida Grabovskaia, PhL, Senior Lecturer
<p>Information security is vital in any organization and for every individual. Most companies, particularly those that provide outsourcing services as in the case of the case company, have access to proprietary and confidential information. If this information is not properly managed, the result could be detrimental to the individual and the business. Thus, the objective of this Thesis is to propose a practical internal information security management process that could help the case company protect the confidentiality and integrity of this information.</p> <p>Existing literature on information security management, mostly inspired by ISO27001, provides valuable information in drafting the conceptual framework of the Thesis. The framework is used as a baseline during the interviews with the case company's stakeholders to understand the current state of the business. The data from the interviews, along with the best practices gathered from stakeholders of other companies and those from the literature were merged to draft the proposal on the process that was provided to the case company.</p> <p>The information security management process which is the outcome of this thesis fits the need of the case company. The process consists of different elements from setting security policy, managing assets, and operations, establishing access controls, reporting incidents, up to conducting the security audit. To commence the process, action items were identified for each of these elements, and owners are assigned. Implementation of the process can help provide structure to ensure proper security management of clients' and customers' information that can be beneficial for the case company and its daily operations.</p>	
Keywords	Information Security Management, Security Policy, Asset Management, Access Controls, Incident Reporting, Audit

Contents

Preface

Abstract

Table of Contents

List of Figures

Acronyms

1	Introduction	1
1.1	Key Concepts	1
1.2	Case Company Background	2
1.3	Business Challenge	4
1.4	Objective and Scope	4
2	Method and Material	6
2.1	Research Approach	6
2.2	Research Design	7
2.3	Data Collection and Analysis	10
2.4	Validity and Reliability Plan	15
3	Existing Knowledge on Improving the Information Security Management Process	17
3.1	Information Security and Information Security Management: Concepts	17
3.2	Information Security in Business Process Outsourcing (BPO)	18
3.3	Impact of Security Management on Business: Incidents and Data Breach	19
3.4	Elements of the Information Security Management (ISM) Process	22
3.4.1	Setting Security Policies	24
3.4.2	Managing Assets	25
3.4.3	Managing Operations	28
3.4.4	Establishing Access Controls	33
3.4.5	Reporting Incidents	35
3.4.6	Ensuring Business Continuity	36
3.4.7	Conducting Security Audit	37
3.5	Information Security Management Process' Conceptual Framework	39
4	Current State Analysis (CSA) of the Case Company's ISM Process	43
4.1	Overview of the CSA Stage	43
4.2	Description of the Case Company's Current Process in Relation to the Concepts of Information Security Management	44
4.3	Case Company's Strengths and Weaknesses	52

4.3.1	Strengths in Information Security Management	53
4.3.2	Weaknesses in Information Security Management	54
4.4	Summary of Key Findings	58
5	Building the Information Security Management Process	60
5.1	Overview of the Proposal Building Stage	60
5.2	Setting Security Policies	63
5.3	Managing Assets	63
5.4	Managing Operations	64
5.5	Establishing Access Controls	68
5.6	Reporting Incidents	70
5.7	Ensuring Business Continuity	70
5.8	Conducting Security Audit	71
5.9	Summary of the Proposal	71
6	Validation of the Proposed Process	74
6.1	Overview of the Validation Stage	74
6.2	Stakeholders' Opinions on the Prototype Process	74
6.3	Final Proposal	75
6.4	Recommendation / Next Steps	76
7	Discussion and Conclusions	78
7.1	Summary	78
7.2	Practical/ Managerial Implications	79
7.3	Evaluation of the Thesis	79
7.3.1	Limitations of the Thesis	80
7.3.2	Outcome vs. Objective	81
7.3.3	Reliability and Validity	81
7.4	Closing Words	83
8	REFERENCES	84

Appendices

- Appendix 1. Questionnaire used in CSA Stage
- Appendix 2. Questionnaire used during the gathering of best practices with stakeholder from other companies
- Appendix 3. Overview of Important Incidents (*Data Loss Prevention*,

- Ernst & Young 2011: 5)*
- Appendix 4. Training Questionnaire Sample for Email Usage (*Appendix 1 on Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, Puhakainen & Siponen 2010*)
- Appendix 5. Sample Email Validation for Employees' Access
- Appendix 6. New Hire IT Checklist
- Appendix 7. Employee Transfer and Off-boarding IT Checklist
- Appendix 8. Information Security Responsibilities (*Information Security. Practical guidance on how to prepare for successful audits, IT Compliance Institute 2006: 6*)
- Appendix 9. Security audit checklist sample on areas of awareness and training, and maintenance (*Information Security. Practical guidance on how to prepare for successful audits, IT Compliance Institute 2006: 17, 20*)
- Appendix 10. Security audit checklist sample on the area of access controls (*Information Security. Practical guidance on how to prepare for successful audits, IT Compliance Institute 2006: 25*)
- Appendix 11. Poster for Awareness Campaign
- Appendix 12. Summary of the initial proposal (first draft)

List of Figures

Figure 1. Organization structure of the case company	2
Figure 2. List of services offered by the case company (case company's website)	3
Figure 3. Case Study Framework (Yin, 2009)	6
Figure 4. Research design of the information security management process.....	8
Figure 5. Plan-Do-Check-Act (PDCA) Model (ISO27k Forum).....	18
Figure 6. The average number of breached records (Ponemon Institute 2013).....	20
Figure 7. Distribution by industry segment (Ponemon Institute 2013).....	21
Figure 8. Average organizational cost of data breach (Ponemon Institute 2013).....	21
Figure 9. Data loss risks, causes and effects in the business (Ernst & Young 2011) ..	22
Figure 10. Threat/Vulnerability flowchart (Harris 2003 as cited in Lomprey 2008)	23
Figure 11. Types of data security incidents (Information Commissioner's Office 2016).....	30
Figure 12. Distribution of root causes of data breach (Ponemon Institute 2013)	31
Figure 13. Information Security Continuous Monitoring (ISCM) cycle (National Institute of Standards and Technology 2011)	32
Figure 14. Audit communication flow (IT Compliance Institute 2006).....	38

Figure 15. Information security management process' conceptual framework.....	40
Figure 16. Case company's current process on information security management	45
Figure 17. Label used by the case company for its PCs and laptops	46
Figure 18. Document labelling and recording of changes made.....	47
Figure 19. Non-disclosure agreement signed by the case company's employees	48
Figure 20. Screenshot of the case company's CRM system	50
Figure 21. IT Application System Access Form as provided by one of the clients.....	51
Figure 22. Unlabelled asset (headset)	55
Figure 23. Summary of case company's strengths and weaknesses	59
Figure 24. Summary of the initial proposal on information security management	62
Figure 25. Information security awareness process flow	65
Figure 26. Email and Internet Guidelines (Bidgoli 2006).....	66
Figure 27. Password Guidelines (Bidgoli 2006).....	66
Figure 28. Poster on security awareness.....	67
Figure 29. Access request flow	68
Figure 30. User access request form sample	69
Figure 31. Email feedback of MS-AS-OP-03 on the initial proposal	75

Acronyms

BPO	Business Process Outsourcing
CRM	Customer Relationship Management
CSA	Current State Analysis
HTTPS	HyperText Transfer Protocol Secure
ISCM	Information Security Continuous Monitoring
ISMS	Information Security Management System
ISO	International Organization for Standardization
NDA	Non-Disclosure Agreement
PDCA	Plan-Do-Check-Act
PII	Personally Identifiable Information
SME	Small and Medium Enterprise
SPI	Sensitive Personal Information

1 Introduction

Information security is a top priority for small and large companies alike as well as for every individual. For companies that provide services for businesses wishing to outsource some of their processes, access to proprietary and confidential information is part of every employee's work. Acquiring more clients to stay in business is of paramount importance for these companies. This can be problematic, however, since many possible clients are concerned about information security issues when outsourcing their internal processes. The aim of this Thesis is to provide the case company with a proposal for a practical internal information security process to protect its clients and its client's customers, as well as the case company's employees, and the whole organization on issues related to the data breach. Having information security improved will help the case company to attract more clients and grow its business according to the company's business strategy.

1.1 Key Concepts

There is widespread concern over data breaches, with customers feeling vulnerable about being exposed to various threats after handing over their personal and login credentials such as biometric and fingerprints data, passport, credit card information, driver's license, social security number, and even their health records. These types of personal data are referred to as *personally identifiable information* (PII), also known as *sensitive personal information* (SPI) that can be linked to an individual or can be used to trace one's identity. It is the responsibility of the companies and their employees to ensure that the information the customers are providing is protected and kept confidential to retain their trust.

In *business process outsourcing* (BPO), customer information is stored in a database for the employees' reference before providing the service in question. BPO offers contact centre services through a phone, email, or chat support, and their employees provide technical support, customer service, and billing, among other services. In doing so, employees have access to this information every single day. Hence, companies need to have a stringent process for these employees to protect their customers from possible data breaches.

1.2 Case Company Background

The case company of this Thesis is a multimedia contact centre in Singapore providing outsourcing services to its clients operating in industries such as telecommunications, healthcare, electronics, transportation, manufacturing and food and beverages. It employs around 80 employees who are engaged in handling customer needs for their clients. Figure 1 shows the organizational structure of the case company by designations.

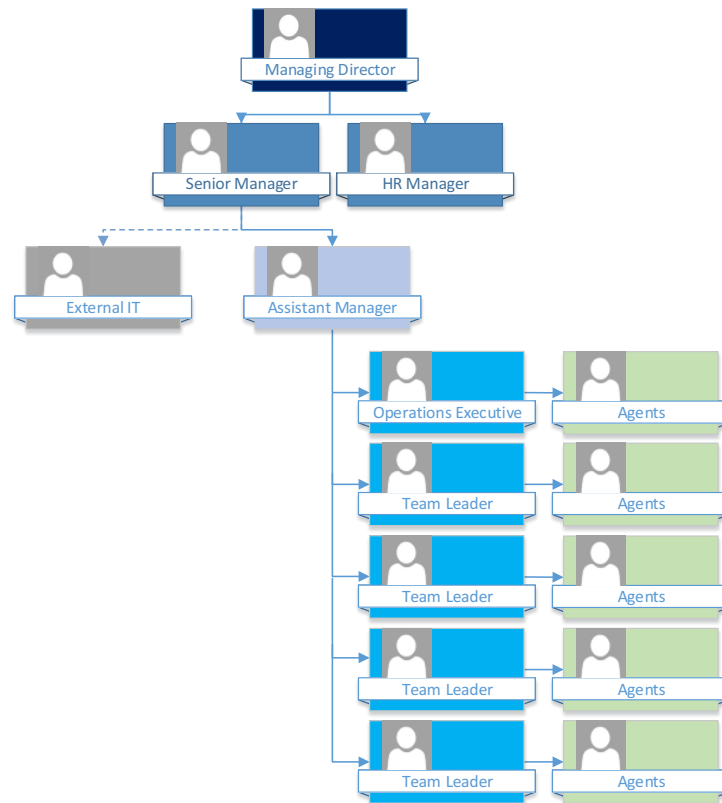


Figure 1. Organization structure of the case company

As shown in Figure 1, the company is managed by the managing director who is also the company owner. The senior and HR Managers who directly report to him share responsibilities in overseeing the entire operations with the former extending her scope to the external IT. The assistant manager is directly involved in managing the clients and team leaders with the latter supporting the technical support and customer service representatives.

The technical staff and customer service representatives also referred to as agents, provide 24/7 support depending on the client's hours of operation. Phone, chat, and email channels are the media of communication to support customers. Additionally, the company also provides IT services such as system development, one-way or interactive SMS

messaging and releases customer satisfaction surveys on behalf of the client. The complete list of services offered is shown in Figure 2.

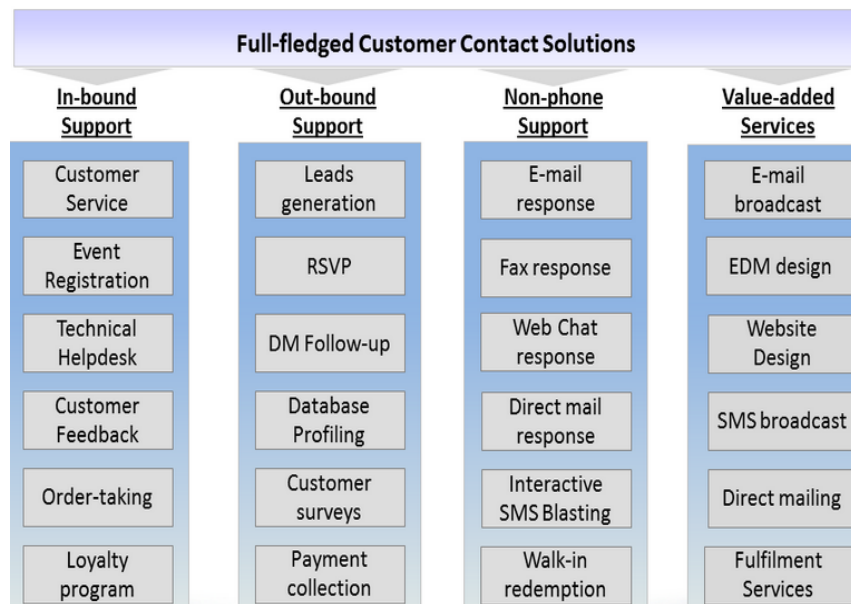


Figure 2. List of services offered by the case company (case company's website)

Figure 2 shows the flexibility and scalability of the company when it comes to the services it can provide to the client. On top of the internal support it provides to the case company, it also extends its scope to services that are requested by the clients. Some of these services could be ad-hoc requests from existing clients or those from external clients who have no existing contracts with the case company.

The company has been operational for 13 years. Previously, the internal IT staff of the case company creates the systems for in-house human resources, customer relationship management (CRM), and call logs which are still utilised by its employees. In 2016, the case company has outsourced its IT team along with the processes.

The case company has a total of 21 clients supported by its multi-skilled agents within Singapore and other two partners in the Philippines and Indonesia. To increase employee productivity for the company, one staff member is trained to handle from 8 up to 12 clients in an 8-hour shift. This means that the employee has access to various customer information throughout the day.

1.3 Business Challenge

The case company has been supporting the customers of various clients from different industries. Over the years, despite its experience in this business, there is no structured and documented process regarding customer information security. Technical support and customer service representatives, also referred to as *agents*, who assist the clients, tend to come and go, and there is no assurance that the client or customer data is secured and has no chance of being leaked. Moreover, the employees have access to the internet; they can freely use their phone in the working area, and they can bring any device they want to the company premises. In other words, there are several ways that customer data can be copied or transferred, without the consent of the client or the company.

Although there are some security measures in place, it is not enough for current information security requirements. For example, there are currently no guidelines for employees to follow to ensure that their customer information is secured. Nor there is any awareness campaign related to the importance of protecting the customer's identity in the company. Even the IT department has not exercised consistency in ensuring that the software programs are up-to-date, and security requirements are regularly audited.

If this type of information is not properly managed, it will entail a significant risk of data misuse. Although the company has the necessary established technology to prevent the misuse of customer information, there is still a possibility of incidents of data breaches in this context. It seems that despite available technology, the case company may have major issues in its fundamental data management processes.

1.4 Objective and Scope

The objective of this thesis is to **propose a practical internal information security management process** for the case company to use in its daily operations. This process should help to assure the existing and future clients that the company has the necessary security measures in place. Additionally, it can assist the company deal with possible information misuse in the future in a more professional and structured way. The outcome of this thesis is a structured process for information security management. This process will provide the case company a guide on the different activities or individual processes that have to be in place to fulfil the requirement for each element of information security management.

The research method used in this thesis is a case study.

This thesis is written in seven sections. Section 1 provides an introduction to the industry where this study is conducted. It focuses on the background of the case company and the challenges it is facing concerning information security. Section 2 introduces the research design structure, data collection and analysis of the data gathered. Additionally, it also presents the validity and reliability plan that are fundamental criteria for any research. Section 3 explores various best practice and existing knowledge that can be used to provide justification and theoretical basis for the proposal for the improved internal information security process. Section 4 presents the current state of the company based on the result of the data collected and analysed in this initial stage. Section 5 provides the result of the second data collection that leads to the drafting of the proposal for the case company. Section 6 evaluates the proposed process based on the third data collection which means feedback from the case company. It also expands the proposal with the actions suggested in the validation session with the key stakeholders from the case company. Section 7 summarizes and concludes the study and discusses the results, starting from the identification of the business challenge, evaluation and analysis of the current state, and the outcome of the drafting of the proposal. In other words, this section provides closure to the entire journey of this study.

2 Method and Material

This section discusses the various steps involved in completing this research. The research design presents the summary on how this thesis will be approached as well as the description of the content for each step. Additionally, the different data that will be collected and how they should be analysed will also be included in this section.

2.1 Research Approach

This thesis adopts the concept of a case study as the researcher studies and understands the real-life situation of the case company when it comes to its information security management process. A case study is initiated to analyse current circumstances of the case company. Additionally, the Thesis wants to get answers to the questions of how information security management is implemented and understood by employees and why it is important for the organization.

Blaxter et al. (2006: 72) further justify the suitability of the case study for a small-scale research where the focus is on a small number of individuals, which is the case here. As described by Yin (2009 cited in Aberdeen 2013: 69-71), a case study is a linear but iterative process. Additionally, he also points out that each stage can stand alone but is linked together as the researcher reviews and re-examines previous decisions. Yin's case study framework as shown in Figure 3 presents the stages of the research process.

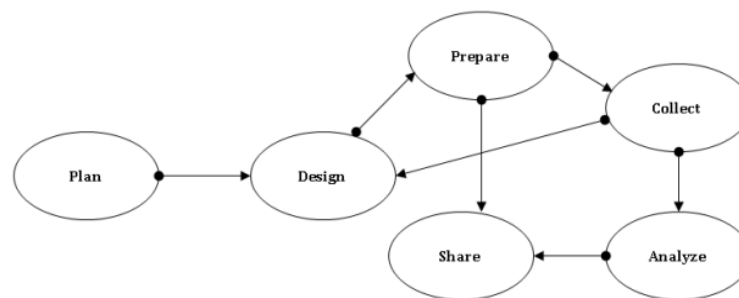


Figure 3. Case Study Framework (Yin, 2009)

Planning is when the researcher decides the kind of research method that is appropriate for the phenomenon at hand. For Yin (2014: 4), case study research focuses on the answers to the questions of the “how” and “why”. **Designing** is when the researcher comes up with the logic of the study through the research design (Yin 2014: 26). **Preparing** is when the researcher has to consider the different preparations necessary to

start the process. The skills needed, the training that is necessary, the procedures to follow, among other things to consider (Yin 2014: 70). **Collecting** is when data and evidence are gathered. This is where the researcher has to take into account the principles to follow in either working with multiple sources of information, among which are interviews and documentation, or maintaining a database of materials, and keeping a chain of evidence (Yin 2014: 102). **Analysing** is familiarizing with the data. Researcher looks for patterns, considers analytic techniques, and interprets evidence. The result is dependent on the researcher's style of rigorous thinking since the analysis of case study evidence is one of the least developed aspects of case studies (Yin 2014: 133). Finally, **sharing** is the stage where the conclusion is presented either orally or in writing to the defined audience, reviewed and feedbacks are gathered, and if deemed necessary, revised until feedbacks are taken into account and the case study is closed (Yin 2014: 177).

Schramm (1971: 6) believes that the essence of the case study approach is to illuminate a decision or set of decisions as why they were taken, how they were implemented, and with what result.

This study does not only focus on what is wrong but rather finds ways to continuously improve the process and practice by looking at evidence and taking action. As real case studies benefit from multiple data sources (Yin 2004: 9), this evidence come mostly from, but are not limited to, remote interviews with individuals who are familiar and in direct contact with the process, focus group discussion with agents, and review of some existing process documents. Patton (1990) and Yin (2003) (as cited in Baxter and Jack 2008: 554) also added that the use of multiple data sources enhances data credibility. Once this evidence is completely gathered, qualitative data analysis is used to interpret the result.

2.2 Research Design

This research study has six stages as illustrated in Figure 4. It starts with the identification of the business challenge where the objective is set. Once the objective is set, the outcome is taken into account. The conceptual framework then follows where ideas come from existing literature. Of which, is the current state analysis of the case company. Once done, the study proceeds to the building of the proposal, then validating it. The outcome is the last stage of the research where the final proposal is completed.

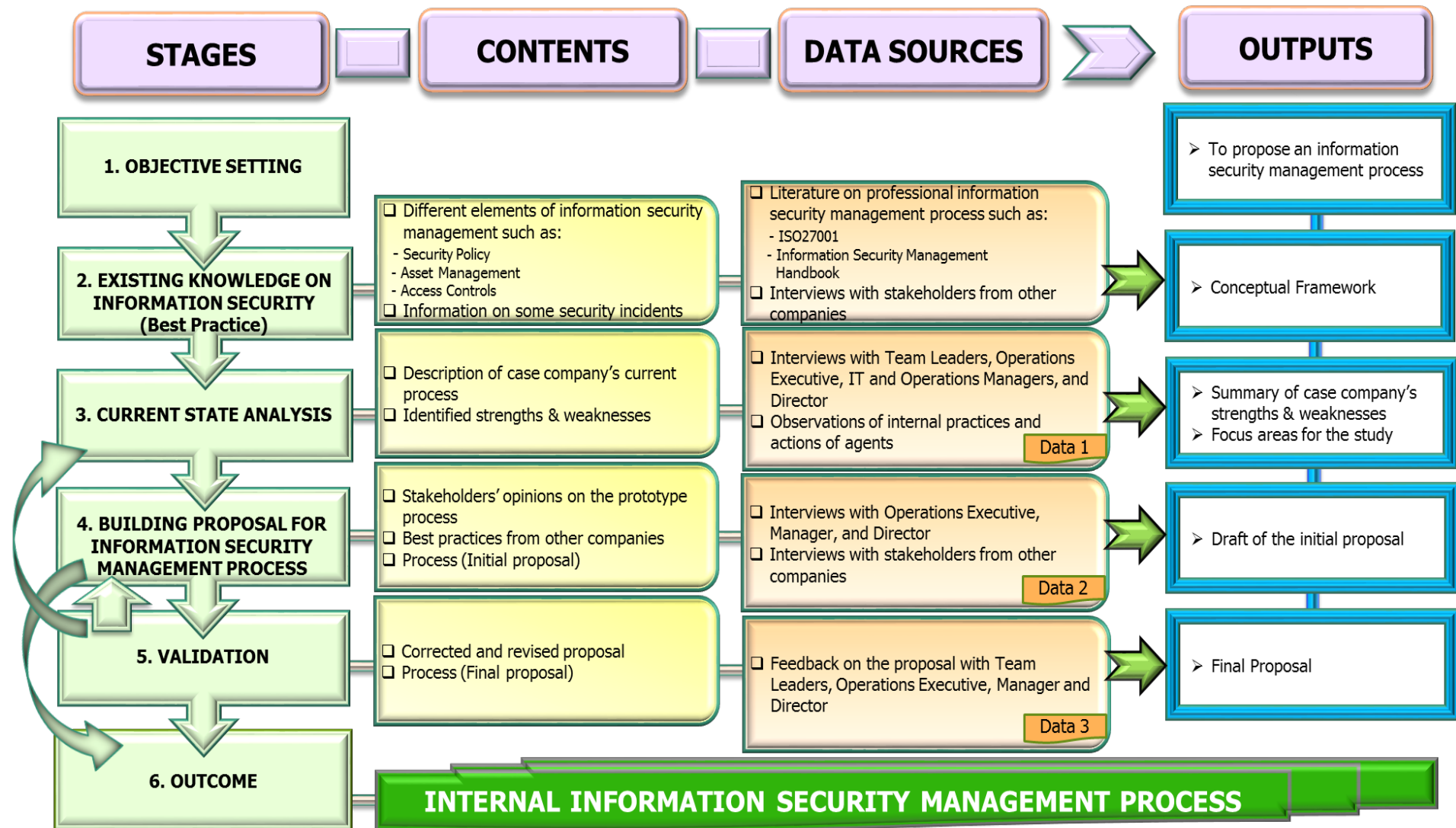


Figure 4. Research design of the information security management process

Stage 1 is the identification of the business challenge that triggers the whole process. In this stage, the problem is identified and presented to the case company. With the identified problem, an objective is formed that also prompted the outcome expected from the completion of this research.

Stage 2 is the formulation of the conceptual framework through various literature where best practices and ideas to be benchmarked can be gathered. Before knowing the current state of the business, existing knowledge is checked through literature sources to know and understand how a professional information security management process should look. On top of this, interviews with stakeholders of other companies are conducted. The intention is to benchmark from best practices of other industries that will prove beneficial for the case company. These are evidence that could have set these companies apart from competitors and have a structured and stabilized processes related to information security management. The findings are compared to how and what the case company is currently doing regarding ensuring the security of its customer's information.

Stage 3 is the analysis of the current state of the case company. Evidence that will be gathered through interviews of the will paint a picture of the company's strengths and weaknesses, along with the gaps to fill. Moreover, the observations on the internal practices and actions of the agent will add more information. Since existing ideas on best practices from the literature were already determined, this stage will enable the researcher to compare and find the missing link that will be taken into account in building the proposal for the information security management process.

Stage 4 is the building of the initial proposal where everything will come together. Evidence gathered from the previous stage, along with ideas taken from benchmark activities and literature will be merged. Combining this information will allow the generation of the proposal that fits the need of the case company.

Stage 5 is the validation of the proposal made. This is where the meeting of the minds happens to review, ask questions, offer insights and feedbacks, and assess the entirety of the proposal. During this stage it is expected that some ideas might be rejected, a part of the process might be questioned, among other things. Once all of the information is captured, the proposal will be revised accordingly, or the result of the current state analysis will be revisited before the rebuilding of the proposal. The intention of re-checking

of current state result is to ensure that all areas are covered and taken into account when the proposal is rebuilt.

Stage 6 is the final stage that is relevant only to this research. This stage is where the final proposal is completed, capturing the changes and enhancements that are made. It will be submitted to the case company for their utilization.

The implementation of the process is dependent on the case company. They could either decide the proposal for immediate implementation or do it at a later time. For the point of view of the researcher, it is advisable and encouraged to put it in place and make necessary changes to how the case company does things. Doing so will convince and enable the company to see the value of the research and impact of the process to the business. But at the end of the day, this is all dependent on the management's decision as this could entail change and a well-planned communication and implementation needs to be considered.

2.3 Data Collection and Analysis

Data collection consists of three rounds. Data collection 1 was conducted for the CSA stage, Data 2 for proposal building, and Data 3 for validation stages.

The collection of Data 1 commences at the current state analysis (CSA). During this stage, the researcher will analyse how the case company currently handles its information security management process using a set of questions in a questionnaire as found in Appendix 1. Strengths and weaknesses will be identified along with the gaps that need to be filled in. The information will be gathered through series of interviews with IT personnel, team leaders, manager and executive of operations, as well as from the company director. Additionally, the observation of the researcher on practices and actions of the agents will also be considered. Furthermore, some internal documents are reviewed to check on forms, practices, or processes that could influence the building of the proposal.

The collection of Data 2 transpires during the drafting of the proposal where information will come from various sources. The main source of information is still the stakeholders

of the case company. Their suggestions and inputs are crucial in the drafting of the proposal. Additionally, the result of the gathering of best practices with other companies through interviews with different stakeholders also comes in handy as data 2 is collected.

The collection of Data 3 takes place when the proposal is validated through a discussion with stakeholders of the case company, and feedbacks are given. These feedbacks will be used to rebuild the proposal, as deemed necessary, to come up with the final proposal that fits the need of the business.

Table 1 specifies the different data sources as well as some of the topics under each data collection phase.

For the analysis of the interviews and discussions, Qualitative Content Analysis was used using interview transcripts and some recordings.

Table 1. Data Collection 1-3 rounds

DATA	PURPOSE	DATA TYPE	DATA SOURCE	TOPICS	ANALYSIS
Data 1	Identify case company's strengths and weaknesses	<input type="checkbox"/> Internal documents	<input type="checkbox"/> Forms (e.g. Non-Disclosure Agreement) <input type="checkbox"/> IT Policy <input type="checkbox"/> HR document (Employee Handbook)	<input type="checkbox"/> Personally Identifiable Information <input type="checkbox"/> Operations and IT Processes	Section 4, Current State Analysis
		<input type="checkbox"/> Interviews with key stakeholders	<input type="checkbox"/> Interviewee 1-2: Team Leaders <input type="checkbox"/> Interviewee 3: Operations Executive <input type="checkbox"/> Interviewee 4: Operations Manager <input type="checkbox"/> Interviewee 5: Managing Director <input type="checkbox"/> Interviewee 6: IT Manager	<input type="checkbox"/> Initiatives <input type="checkbox"/> Access Rights <input type="checkbox"/> Monitoring <input type="checkbox"/> Network Access <input type="checkbox"/> Audit	
		<input type="checkbox"/> Observation	Observations of internal practices and actions of agents	<input type="checkbox"/> Reporting	
Data 2	Building the proposal	<input type="checkbox"/> Interviews with key stakeholders <input type="checkbox"/> Benchmark with other companies	<input type="checkbox"/> Suggestions/input for building the proposal <input type="checkbox"/> Best practices from other companies	<input type="checkbox"/> Security Policy <input type="checkbox"/> Asset and Operations Management <input type="checkbox"/> Access Controls <input type="checkbox"/> Incident Reporting <input type="checkbox"/> Business Continuity <input type="checkbox"/> Audit	Section 5, Building the proposal
Data 3	Validate the proposal through feedback solicitation	Discussion with stakeholders	Final proposal		Section 6, Validation

As shown in Table 1, the data sources and methods used in this study vary from interviews, review of some internal documents of the case company as well as the personal observation of the researcher on the internal practices and actions of the agent during the two-year work tenure with the case company.

The following tables summarize the details of the data collections that were conducted through interviews of the case company's stakeholders as shown in Table 2, review of internal documents in Table 3, and gathering of best practices from stakeholders of other companies in Table 4.

Interview of Case Company's Stakeholders

Comprehensive information regarding the current and existing process of the case company can be better understood if it comes from various stakeholders who are directly involved in the operations or have access to this information. Series of interviews were conducted as shown in Table 2 from stakeholders holding different positions in the company.

Table 2. Summary of the interviews conducted during the CSA stage

DATE	INTERVIEW STYLE	INTERVIEWEE CODE	DESIGNATION	TOPICS	DURATION (mm:ss)	DOCUMENTED AS
10 th March 2016	Skype Call Interview	BT-AS-OP-01	Team Leader	<input type="checkbox"/> Personally Identifiable Information	40:02	Questionnaire, Field notes and Recording
11 th March 2016	Skype Call Interview	JR-AS-OP-02	Operations Executive	<input type="checkbox"/> Access <input type="checkbox"/> Operations Processes	47:22	Questionnaire, Field notes and Recording
15 th March 2016	Skype Call Interview	MS-AS-OP-03	Assistant Operations Manager	<input type="checkbox"/> Initiatives <input type="checkbox"/> Training	51:15	Questionnaire, Field notes and Recording
16 th March 2016	Skype Call Interview	RC-AS-OP-04	Team Leader	<input type="checkbox"/> Audit <input type="checkbox"/> Reporting	26:33	Questionnaire, Field notes and Recording
16 th March 2016	Skype Video Interview	EN-AS-OP-05	Managing Director	<input type="checkbox"/> Security Policy <input type="checkbox"/> Reporting <input type="checkbox"/> Business Continuity <input type="checkbox"/> Initiatives	37:54	Questionnaire, Field notes and Recording
21 st March 2016	WhatsApp Call	SN-AS-IT-06	IT Manager	<input type="checkbox"/> Security Policy <input type="checkbox"/> Asset and Operations Management <input type="checkbox"/> Access Controls <input type="checkbox"/> Incident Reporting <input type="checkbox"/> Business Continuity <input type="checkbox"/> Audit	39:36	Questionnaire and Field notes

As seen from Table 2, interviews were done through video calls. Various topics related to information security were discussed with the different stakeholders consisting of the team leaders, operations executive, operations manager, IT manager, and the managing director. With the recent turnover experienced by the case company on more tenured members of its management team, the existing employees that were interviewed are the current most tenured in the team who are more familiar with the daily operations. Table 2 presents the relevant information related to the interview.

Review of Internal Documents

On top of the information gathered during the interview, some of the case company's internal documents were also reviewed. The purpose of the document review is to gather some background information about the case company's processes and at the same check if these processes conform to the information security management process. Additionally, document review allows the researcher to check some information that is not noted. Table 3 summarizes these documents.

Table 3. Case company's internal documents

NO.	DOCUMENT NAME	DOCUMENT TYPE	# OF PAGES	DESCRIPTION
1	IT Policy	Policy	10	Case company's security policy which was drafted on December 2011 and revised February 2015. Information found in the document includes but not limited to the responsibility of the user and the guidelines that need to be followed for some processes like incident reporting, IT requests, and utilization of assets, among others
2	Employee Handbook	Handbook	100	Company's policy that summarizes the different rules and regulations employees need to follow as well as the corresponding sanctions for a certain violation
3	IT Application System Access Form	Form	1	Client's document used to request employees new access for client's systems
4	Non-Disclosure Agreement	Document	2	Document employees sign and also required by the client to ensure that employees understand their role and the importance of not improperly divulging or sharing proprietary information

As seen from Table 3, these are the only available documents that the case company has that could be related to information security management. Except for the IT policy that provides some information on the responsibility of IT and the users, and a portion of the employee handbook that requires employee not to disclose any confidential information to a third party, there are no documents on processes related to information security. Even the form of request for access comes from the client and only unique to a certain account.

Gathering of Best Practices from Other Companies

Gathering of best practices is a learning process from the point of view of the researcher. This provides an opportunity to take a glimpse of other companies' practices that are successfully implemented while at the same time learn from their struggles and the challenges they encounter in the process. The information gathered during this activity shed some light on the areas that the case company needs to have and has to work on to be more effective and efficient in their security management process. Table 4 provides a summary of these activities on various stakeholders in the Philippines, Singapore, and here in Finland.

Table 4. Summary of the interviews with stakeholders from other companies

DATE	INTERVIEW STYLE	INTERVIEWEE CODE	DESIGNATION	DURATION (mm:ss)	DOCUMENTED AS
9 th February 2016	Skype Call	<i>Benchmark 1:</i> KC-LK-OP-01	Vendor Manager	32:21	Questionnaire, Field notes and Recording
10 th February 2016	Respondent is not available for interview but responded to the questionnaire	<i>Benchmark 2:</i> GP-TS-IT-02	Systems Architect	-	Questionnaire, Field notes
12 th February 2016	Face-to-face	<i>Benchmark 3:</i> PV-EY-OP-03	Business Manager	32:21	Questionnaire, Field notes and Recording
23 rd February 2016	Phone Interview	<i>Benchmark 4:</i> AN-CE-IT-04	Team Leader	46:57	Questionnaire, Field notes and Recording
26 th February 2016	Face-to-face Group Interview	<i>Benchmark 5:</i> GP-FE-IT-05	2 Managers 1 Lead Researcher	56:08	Questionnaire, Field notes and Recording
29 th February 2016	Respondent is not available for interview but responded to the questionnaire	<i>Benchmark 6:</i> GE-SP-IT-06	Cloud Systems Engineer	-	Questionnaire, Field notes
8 th March 2016	Face-to-face	<i>Benchmark 7:</i> JK-JL-IT-07	Chief Technical Officer (CTO)	36:06	Questionnaire, Field notes and Recording
14 th March 2016	Skype Call	<i>Benchmark 8:</i> AC-AE-OP-08	Manager	41:25	Questionnaire, Field notes and Recording
14 th March 2016	Face-to-face	<i>Benchmark 9:</i> JS-GO-IT-09	Chief Information Officer (CIO)	46:17	Questionnaire, Field notes and Recording

As seen from Table 4, some interviews, focused on gathering best practices on information security management, were conducted with stakeholders of other companies. These activities are insightful as many ideas and evidence were shared that could help improve the case company's process in information security. A set of questions is prepared as shown in Appendix 2.

2.4 Validity and Reliability Plan

The quality of research can be assessed through these two criteria, Validity, and Reliability. The concepts of validity meaning "well grounded" and reliability meaning "sustainable" have relevance for qualitative research as they help to define the strength of the data (Ritchie and Lewis 2003: 270).

Validity is the accuracy and truthfulness of findings or evidence. A valid research demonstrates what exists and whether the measurement truly measures what it is intended to measure (Brink, 1993). To provide validity to the research question, or on this case the objective, to the conclusions, Yin (2009: 94) puts emphasis on data triangulation, precise documentation of the database, as well as maintaining a chain of evidence.

In this study, validity is planned to be measured through the truthfulness of answers given to the questions during the interview. Questionnaires containing relevant questions on information security will gather evidence on how the employees understand the importance of information security. At the same time, these questions test their awareness on the existence of the process. These questions and the answers focus and address the business challenge. Aside from this, valuable ideas coming from various literature prove to be helpful in the course of the study. It starts from the identification of the gaps between the current practices up to the building and completion of the proposal. Furthermore, the best practices that will be gathered from external informants will also enrich the validity of the research and existing practices.

Carmines and Zeller (1979: 11-12) defines *reliability* as an extent to which an experiment, test, or any measuring procedure, yields the same result even if the process is repeated. In other words, it is a tendency towards consistency found in repeated measurements of the same phenomenon. Dependability can be done through inquiry audit and might enhance the reliability of the research. Gibbs (2012) defines it as an investigation that has been carried out by different researchers in various circumstance or time perspective.

This investigation uses the same method and yields the same result. In other words, there is a consistency of information gathered that even if it is redone, the same result will come out. If this is the case, then it can be concluded that the research is reliable. Holtzhausen (2001) also believes that triangulation can strengthen the qualitative research design and makes a powerful tool.

In this study, the reliability is planned to be ensured through interviews with different stakeholders in the case company. Responses from multiple informants like team leaders, managers, and director are sought. Doing so sheds light on the current state of the business concerning information security. Additionally, this process, which will be done in different time perspective, ensures that various levels are well represented. Moreover, this gauges the consistency of the respondents' answers on the current process the case company has on information security. Triangulation will be done through cross verification with several sources to validate the data. As the single method is never enough to shed light on certain issues, using multiple methods will give a clearer understanding on these issues.

In this study, issues of validity and reliability will be evaluated towards the end of the research in Section 7, Discussion and Conclusions.

3 Existing Knowledge on Improving the Information Security Management Process

This section discusses existing knowledge on information security management coming from various literature. Moreover, the benchmarking done with the stakeholders from other companies provided also some helpful insights for this thesis. The information coming from these stakeholders is highlighted in grey. The knowledge obtained through the literature is used to establish a framework to be able to build the proposal for an information security management process for the case company.

3.1 Information Security and Information Security Management: Concepts

Information security is a top concern and of utmost importance for everyday consumers and businesses. With the widespread incident on data breaches, businesses have to understand the importance of information security and find ways to protect the privacy of their respective clients and their clients' customers.

Information security is characterized as the preservation of confidentiality, integrity, and availability (Carlson 2001: 2; Axelrod 2004: 37-38). Thus, information security policies must be present in any organization as this is the cornerstone of the organizations information security program. The absence of these policies and standards related to information security does not allow the company to adequately secure its critical information assets. One of the reasons why these policies are necessary is when an information incident negatively affects 3rd parties, it can be argued that its absence is an evidence of negligence on the side of the company (Stahl & Pease 2011: 3).

As per ISO (2013), *information security management* is a "systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process". Its goal is to align IT and business security and ensure that effective management of the information security is in place in all aspect of services and service management activities (van Bon et al. 2007: 220). The same concept applies in the information security management context of this study.

On the other hand, in the context of this study, information security management process means having a framework in place to actually implement security controls. This process

comprises of sub-processes that cover policy, awareness, access, monitoring, compliance, and strategy (Bayuk 1996: 1). Moreover, information security management process aims to provide direction for the company's activities related to security and ensure that security goals are achieved.

Improving the information security process typically relies on the four stage cycle of any process improvement. The Plan-Do-Check-Act (PDCA) Model or the Deming Cycle as shown in Figure 5 applies at different levels of the information security management system (ISMS) cycle. The same approach is used for quality and risk management. This has been incorporated by ISO/IEC 27001:2005 taking into account that ISMS must remain effective and efficient with the changes in the organization (Carter and Hinson, 2010).

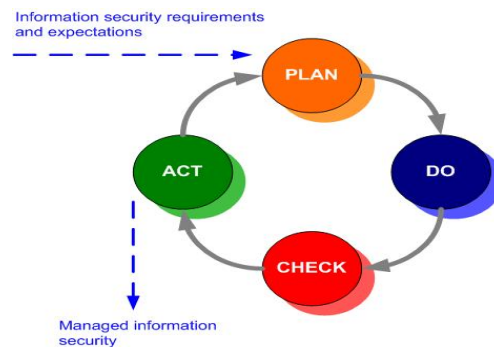


Figure 5. Plan-Do-Check-Act (PDCA) Model (ISO27k Forum)

Plan is where organization defines scope and policy, identify and assess the risks and manage them through a set of controls. **Do**, is where organization formulates and implements plan to mitigate risks. **Check** is where organization perform monitoring of procedures and review ISMS effectiveness as well as conduct audits. Finally, **Act** is where the organization takes appropriate corrective and preventive actions. Additionally, maintain communications with stakeholders and validate improvements.

3.2 Information Security in Business Process Outsourcing (BPO)

The service industry has paved the way for the emergence of business process outsourcing which is a subset of outsourcing. In a BPO, companies contract a third party service provider to do some particular business process. Some of these companies outsource their processes on information technology solutions, accounting, human resources management, supply chain management, debt collection, data collection and

tax processing as well as their contact centre services. Outsourcing to Asian countries is already common as the small labour, and operating cost is the main attraction. This was begun by Silicon Valley firms when they started outsourcing their coding and other software development work to India in the late 1980s. These companies were the first to engage in business process outsourcing (KPMG, 2006).

Business process outsourcing has been gaining popularity in the service business industry. With the advancement in technology to support innovative strategies in creating more value for customers, risks are always present. One of them is the danger of information security specific to massive data fraud/theft where there is wrongful exploitation of private or official data (World Economic Forum, 2015). Recently, as reported by the BBC (2015), AT&T was fined \$25m over customer data thefts. It is the largest fine so far imposed on a company for losing data and violating customer privacy. The incident happened in call centres where the staffs involved abused their log-in credentials to steal data that was then used to request codes which could unlock stolen phones.

The call centre or contact centre is where the customer's experience and attitude towards the company is formed and the interaction between the call centre employee and customers over the phone or email is critical (Prunty et al. 2006). Thus, a heightened emphasis on information security management is necessary for the customer, employee, and the company as a whole. Moreover, Figure 7 also shows that based on the research of the Ponemon Institute (2013: 19), the service industry is ranked the 4th highest of the industrial segments affected by data breach. BPO happens to belong to this segment.

Most companies who are engaged in outsourcing have high levels of security both in process and technology perspective. But there are also others that are still lacking in this area. Thus, when an IT security related incident takes place, these companies tend to react and learn from it instead of being proactive. This has also been the situation with the case company.

3.3 Impact of Security Management on Business: Incidents and Data Breach

Straub and Welke (1998: 442) believe that employees at all level in the organization are not knowledgeable enough of the impact of the risks when security is breached. Hence, information security continues to be ignored. In all cases when a breach happens, there is always that negative impact on the business either on a commercial basis due to cost

that will be incurred or on the integrity of the company and the trust of clients and customers that will be most likely be put in jeopardy.

According to Ernst and Young (2011: 4), the average total cost per data breach has risen to \$7.2 million based on the 2010 Ponemon Institute study. Appendix 3 provides an overview of some important incidents related to data loss that have resulted in high costs for some affected organizations and have caught the attention of the media. In a more recent research Ponemon Institute (2013: 1) conducted, information is gathered from interviews with over 1,400 individuals and 277 organizations globally. Figure 6 presents the average number of breached records per country in a span of just one year while Figure 7 shows the different industry segments that are affected by this incident. Furthermore, with the breach incident, organizations in various business segments from these countries have incurred massive monetary losses as shown in Figure 6.

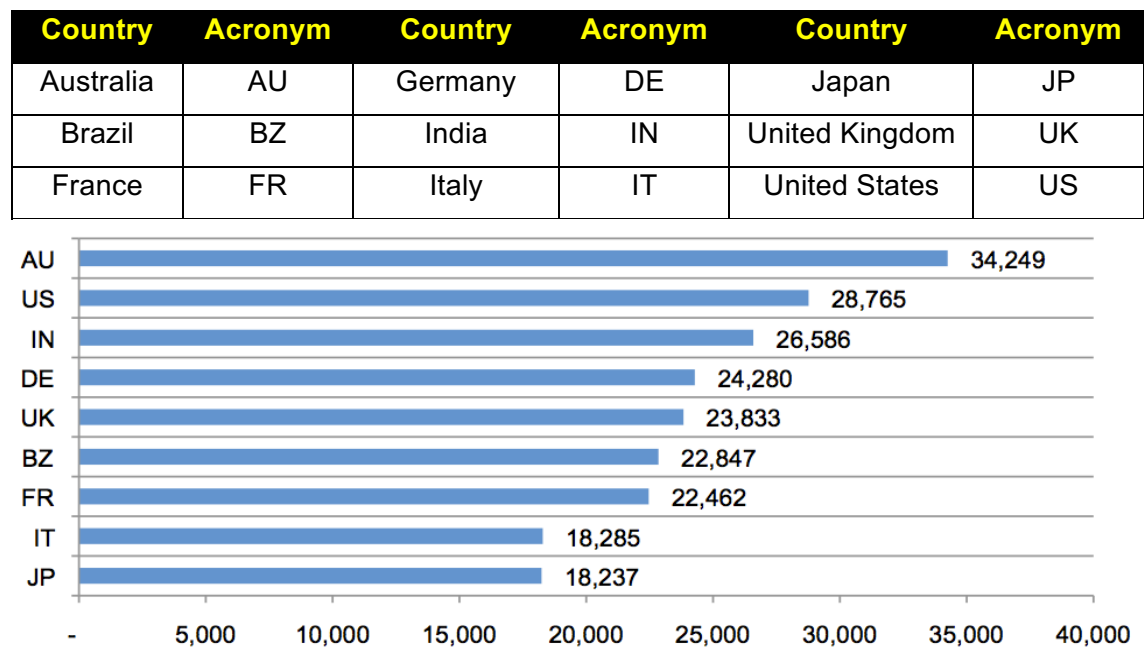


Figure 6. The average number of breached records (Ponemon Institute 2013)

As shown in Figure 6, among these nine countries, Australia has the most incident of breached records mostly due to malicious attacks at 43% followed by the US for the same cause at 41%. Japan, on the other hand, experienced the lowest average number of breached records and also for the same cause.

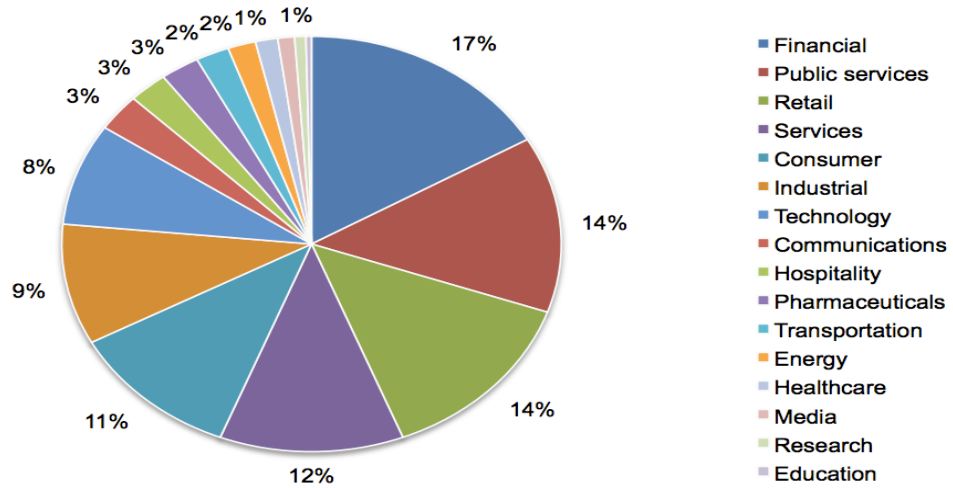


Figure 7. Distribution by industry segment (Ponemon Institute 2013)

It can be seen from Figure 7 above that of the 16 industries; the financial sector is mostly impacted by this breach at 17%. This includes banks, insurance, investment management, and payment processors.

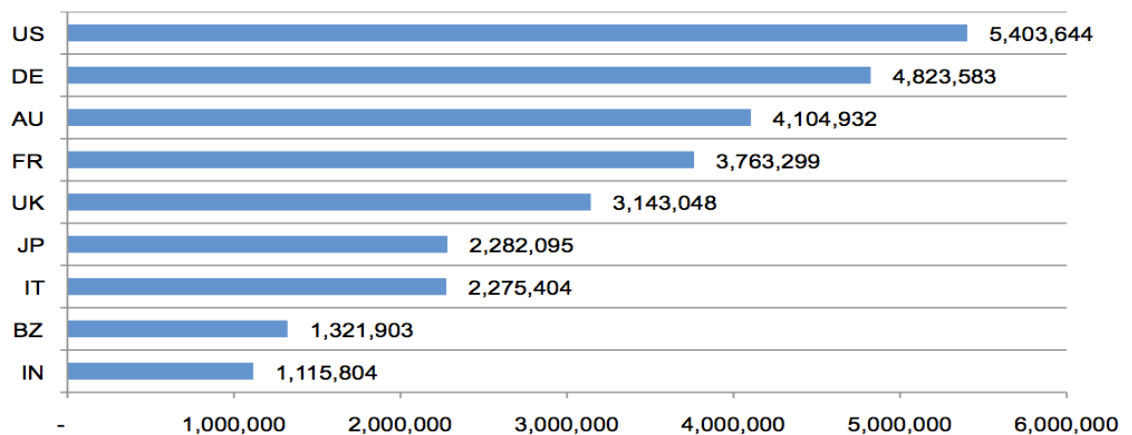


Figure 8. Average organizational cost of data breach (Ponemon Institute 2013)

Data breach is costly for any organization. As can be seen in Figure 8, the US has incurred the highest cost for breach incidents. Some of the expenses involved when this incident transpired are calculated based on escalation and those measures company perform to notify concerned individuals or parties either through an outbound call, email, letters, or general notice about the incident (Ponemon 2013: 20).

Aside from the monetary aspect, there are several other consequences when security is

breached, and data is lost. Figure 9 paints a clear picture of this cause and effect relationship.

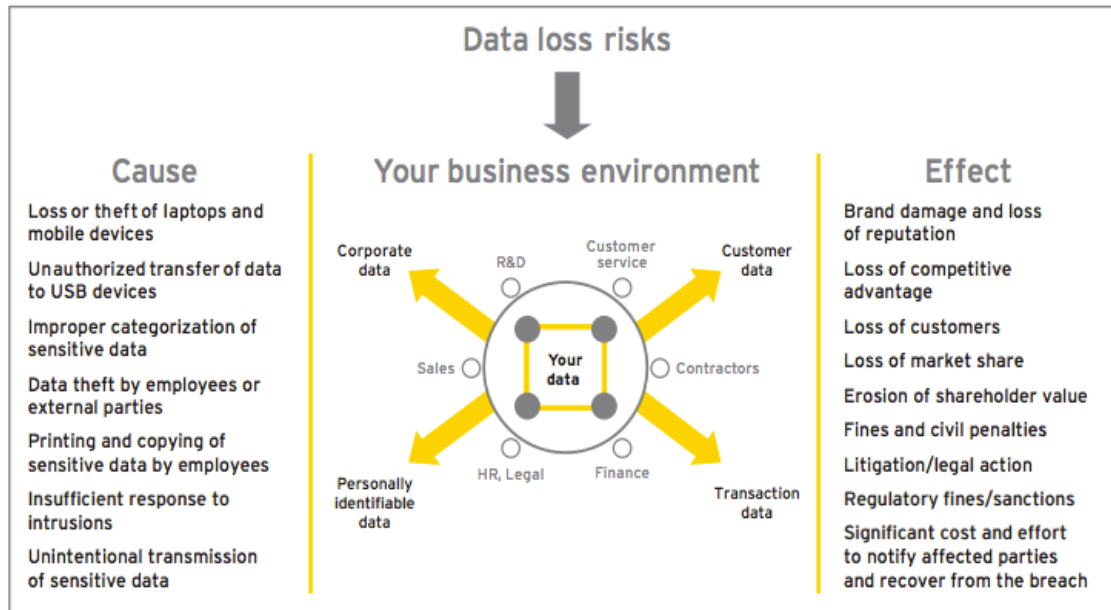


Figure 9. Data loss risks, causes and effects in the business (Ernst & Young 2011)

There are a variety of data loss scenarios that happen globally. No simple solution can address these risks. The resolution could either be through employee education on risks of data loss and their role in protecting this data, implementation of processes that would provide structure in data loss management, having a robust technology, or synergizing the people, process, and technology (Ernst & Young, 2011).

Summing up, the role of information security process is very high in business as it provides a framework which allows the company to properly manage risks on the security of its information. At the same time, it gives the organization, its clients, and even third party entities confidence and peace of mind.

Literature and business practice point to a set of cornerstone actions that need to be taken for setting up a security management process. These cornerstones are described in the following subsections.

3.4 Elements of the Information Security Management (ISM) Process

Lomprey (2008: 56-58) categorized threats agents to security to be either internal or

external. Internal threats could be attributed to malicious or incompetent employees. External threats are those criminal, recreational hackers or even the competitors. Figure 10 illustrates how this threat agent negatively impacts security.

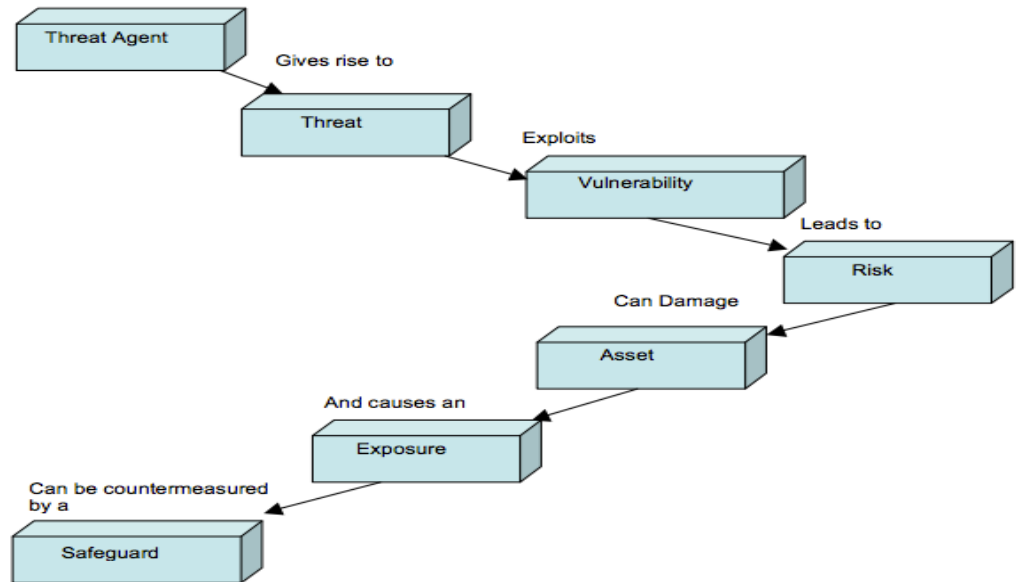


Figure 10. Threat/Vulnerability flowchart (Harris 2003 as cited in Lomprey 2008)

As illustrated in Figure 10, Lomprey (2008: 55-58) further discusses that threat agents give rise to threats. These threats can be further categorized into three areas, and they are natural threats like those electrical storms, earthquakes and other natural disasters, human threats which could cause harm either intentional or unintentional through unauthorized disclosure, misuse, and alteration, of information or information systems, and environmental threats such as power failure. These threats exploit vulnerabilities that could either be known or expected. The former being those that are discovered by testing or reviews of the environment or knowledge of policy weakness while the latter are those that are anticipated to rise in the future such as unpatched software, the personnel turnover that results to less knowledgeable or inexperienced staff who fails to perform security duties satisfactorily. These vulnerabilities lead to a risk that could pose a damage to company's asset.

This clearly demonstrates how crucial information security is in any organization to safeguard its customers and the entire business. Thus, it is equally important that the following elements of information security management be present within the organization to provide the necessary guidelines towards a structured process.

3.4.1 Setting Security Policies

Hamdi et al. (as cited in Bidgoli 2006: 945-946) define security policies as a set of rules that determine how a set of assets should be secured. Moreover, for companies that have set of networked assets, the security policy constitutes the core of the security plan which entails implementation of safety measures and documentation of security incidents.

Wurzler (2013: 7) describes security policy as a written statement with a purpose of protecting the company's information assets from malicious or accidental disclosure, modification, or destruction. He further cites that the policy is important to prevent security incidents and defines responsibilities and expectations regarding user awareness and requirements for the protection of company's assets. Furthermore, the policy is to guide handling incidents in a more efficient and effective manner for the impact of such to be reduced.

In drafting a security policy for an organization, it is important to consider several components as shown in Table 5.

Table 5. Key information security policy components according to Lomprey 2008

No.	Key Information Security Policy Components
1	A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing
2	A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives
3	A framework for setting control objectives and controls, including the structure of risk assessment and risk management
4	A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including: compliance with legislative, regulatory, and contractual requirements security education
5	A definition of general and specific responsibilities for information security management, including reporting information security incidents
6	References to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules with which users should comply

As seen in Table 5, a security policy is a comprehensive statement that should be well documented (ISO-27002 2005: 5, as cited in Lomprey 2008: 77). The document does not have to be technical in nature but rather established to be understood and followed by all employees, contractors, or any other person who have access to the company's information. In other words, the policy has to be realistic and enforceable, has a long-term focus, clear and concise, and role-based which means areas of responsibilities and authority are identified. Additionally, it includes social engineering wherein employees are reminded that sensitive information should never be given out and that the policy is flexible where changes can be made to meet the current needs of the organization (Douglas et al. 2008 as cited in Wurzler 2013: 8).

3.4.2 Managing Assets

The asset is an item of value as defined by Merriam-Webster's Dictionary. While asset management involves discovery, ownership, value, acceptable use, protection, and disposal of information-related assets. Thus, developing and knowing the 4 'Knows' according to Myers (2015) would prove to be helpful to start the whole process,

- "Know what you have" entails reviewing and inventory of assets the company has which could include data centres, hardware, software, information, among others. Once known, spreadsheet needs to be created to list assets in different categories.
- "Know where it is" requires recording the physical location of the asset.
- "Know who owns and maintains it" takes into account identification and recording of owners or custodians for each of the asset.
- "Know how important it is for the company" necessitates review of regulations that requires protecting information resources. This also demands to rate the assets based on criticality.

Classifying and Protecting Assets

Classifying the assets is critical and essential for the company as appropriate decisions regarding the level of security that needs to be provided to protect such asset will be based on its category. Furthermore, the company can determine the degree of redundancy that is necessary to keep an extra copy of the data or server on standby (Kadam, 2002). Table 6 summarizes the different categories of these assets.

Table 6. Categorization of assets according to Lomprey 2008

Categorization of Assets	Description
Information	Databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information
Software	Application software, system software, development tools, and utilities
Physical	Computer equipment, communications equipment, removable media, and other equipment
Service	Computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning
People	Their qualifications, skills, and experience
Intangibles	Such as reputation and image of the organization

As seen in Table 6, assets can fall in six categories, and ISO-27002 (2005: 19 as cited in Lomprey 2008: 78-79) describe each of these assets. Categorizing them enable proper management and security by setting controls necessary to maintain the integrity of the systems.

Destructing Data

Data breach is a costly incident. Thus, hardware containing confidential information of clients or customers need to be properly disposed of that project has ended. The same goes for hard copy materials wherein the most standard practice is shredding. Failure to do so can lead to serious breaches, of data protection and privacy policies, compliance problems and added costs (Violino, 2012). An analyst at a research firm Gartner believes that although big enterprises have an understanding of how to deal with data destruction, there are still many small to midsize businesses that have not considered the risks of undestroyed data.

Violino (2012) also added that data can be destroyed in three ways. Overwriting, degaussing, and physical destruction. **Overwriting** is a cost efficient method where data is destroyed by overwriting the media with new data. This takes a while though especially if an entire high-capacity drive has to be overwritten. **Degaussing** is a process where

the magnetic field of a storage disk or drive is reduced or removed. This process makes the data completely unrecoverable, so it is a convenient method for highly sensitive data. The downside is that Degausser products are expensive, and since they have strong electromagnetic field, they can damage other vulnerable equipment within their proximity. **Physical destruction**, on the other hand, is done by the company in many ways. But some companies engage 3rd party vendors to destroy contents of computers' hard drives and any other hardware that contains confidential information.

Business practices, as evidenced from those collected in this study, confirm these data destruction suggestions. Benchmarks 4 and 7 particularly practice the physical destruction of their hardware that contain confidential data of their customer.

"When a server is taken down from production and hard drives come from that server, firstly erased in a secure manner and then destroy using a sub-contractor that destroys them. When we are talking about documents, we shred them."

(Benchmark 7, JK-JL-IT-07)

"We are providing a service for a customer so that we deliver some devices to the customer premises that have customer configuration. When we are ending the service, we will take the devices here in the company and destroy all those hard drives. We are not going to use them, but we are destroying with other partners that are certified to do that."

(Benchmark 4, AN-CE-IT-04)

Timely elimination of records and data that are not needed is a critical part of securing intellectual property. Companies have to take into account the pros and cons before deciding and considering any methods of data destruction.

Assessing Risk

Lomphey (2008: 58) defines risk assessment as the process used to identify and understand risks related to confidentiality, availability, and integrity of information and the information systems which consists of the identification and valuation of assets and their analysis about potential threats and vulnerabilities.

According to Tipton & Krause (2007: 18), risk analysis may serve as a fundamental justification for the selection and deployment of controls that inhabit the information security management system (ISMS). Moreover, a risk-based ISMS allows for business to accept

risk based on an informed-choice decision making and enables the business to react to their environment.

As cited by FFIEC, there are several risk assessment factors management has to consider. These factors would depend on the size of the company, the complexity of the support, and the nature of the business. Furthermore, some of these factors are, but not limited to, scope and criticality of systems or number of business units affected, transaction volume and its value, impact to data when they are downloaded, read, uploaded, updated, or altered, and number of staff members and their stability and the presence of emerging risks from developing technology or its obsolescence.

3.4.3 Managing Operations

Brophy et al. (2012) explain that in ISO27001, this is considered as the biggest section and a concern of the IT. Managing operations involves standard practices to be documented as procedures, and for procedures and policies to be set, so all employees are clear and follows the same process. This also includes monitoring of activities to make sure that what employees do are appropriate and in accordance with the requirement and expectation of the company.

Managing operations also requires drafting a process to manage for third parties like contractors or suppliers especially if they are supporting the IT infrastructure of the company. This process includes documentation of contracts and making modifications if deemed necessary. The purpose is to ensure that expectations are documented especially if there are service level requirements needed to be met by the third party company (Brophy et al. 2012).

Managing operations is important to create the highest level of efficiency that is possible in performing activities within the company.

Documenting Processes and Establishing Ownership

One way to ensure that operations is properly managed is by documenting operational processes. Operations management entails establishing procedures and responsibilities through documentation. Procedures are essential as they maintain control, ensure consistency and enable training of staff. It could also keep the company out of legislative issues as some procedures may even be a legal requirement (Therault, 2013).

Therhault (2013) further added that procedures or processes need not be complicated. For them to be understood by the concerned individuals, they can be simply written. Some of the things that can be considered in writing these documents are the use of flowcharts to illustrate the procedure. As well as to include checklists to ensure that all steps are taken, and nothing is missed out. Moreover, use graphics and icons for easy visualization. Most importantly, consider to include users wherein they should be able to provide feedback as some instructions may be confusing for users to understand especially if it is written by experts who are well aware of the process.

It is also important to assign responsibilities or owners to every operating procedure that is documented and that these procedures or any document at that is controlled, and changes are authorized by the management.

Creating Awareness

“The first step toward change is awareness. The second step is acceptance.”
– Nathaniel Branden

Change constantly happens in an organization. To manage perception accordingly on the changes to be implemented, employee awareness is vital. To keep employees well informed, may it be related to events, new initiatives, even a recognition of a job-well-done, and especially changes within the organization, effective communication is key.

Effective communication takes repetition, effort, and thoughtfulness (Krantz, 2015). It promotes a two-way feedback and a positive attitude towards change, ensures consistency while at the same time makes employees engaged. Engaged employees are motivated and will make an effort to ‘go an extra mile’ (Weal, 2014). There are different ways to communicate and advocate awareness to get the message across. It could be through postings of visuals, town hall meetings, focus group discussions, regular weekly meetings, one-on-one coaching sessions, a conference for leaders, and training for employees.

For employees to be compliant with the requirements which are not just limited to information security, a training tailored towards communicating certain information on policies and guidelines, among others are put in place. Considering the case company has no

existing training material for incoming and existing employees, a training plan needs to be drafted.

To design a training plan for existing employees specific to information security, a survey can be conducted to assess and understand their knowledge. Puhakainen and Siponen (2010) provides some sample questions as found in Appendix 4. Some of these questions can be used to assess existing knowledge of employees when it comes to email usage which is related to information security. From here the training plan can include information on how email should be used and the risks involved if misused. To provide a more adequate training, IT personnel can conduct system and application related training and discuss more practical information on information security.

Email is not the only topic that should be considered during training as there are still other factors that influenced data security. As reported by the Information Commissioner's Office (2016) covering Q3 of 2015, there are several data security incidents type as shown in Figure 11.

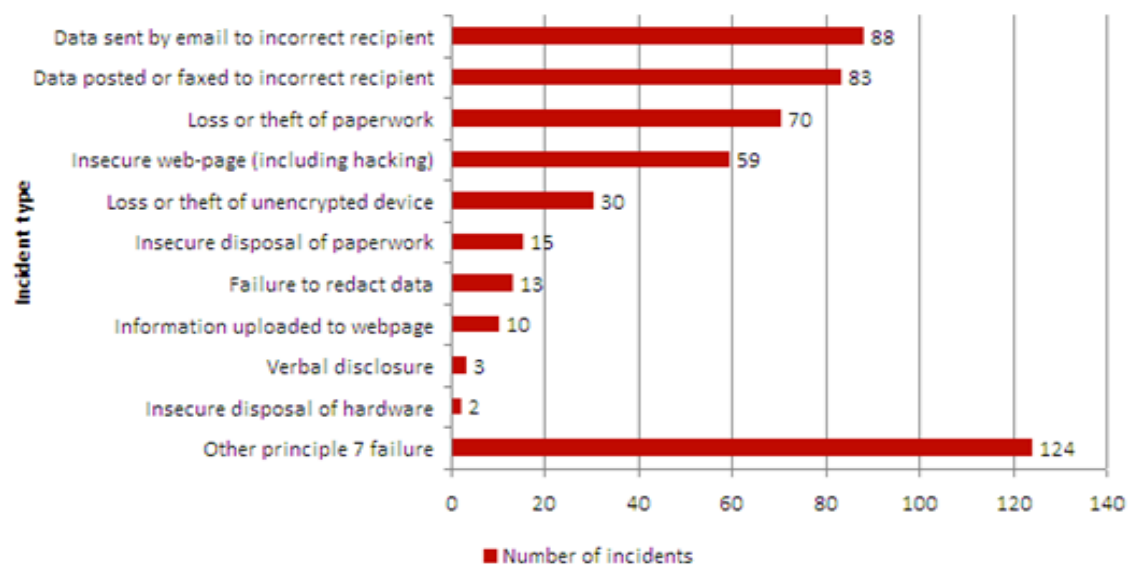


Figure 11. Types of data security incidents (Information Commissioner's Office 2016)

Various security incident types in Figure 11 happened within one-quarter from different industry segments. Topping the list is security incidents brought about by sending email to the incorrect recipient. Other incidents involve hard wares, hard copies of documents and even verbal disclosure, among others. The 'other principle 7 failure' type of incidents are those that cannot be categorized as one of the other types. This could include failure

to protect emails that contain personal information, using a password or using a non-business computer to process work-related personal data.

Thus, aside from the formal classroom training, supplementary training through one-on-one coaching sessions or team huddles can serve as venues for regular employee education. Doing so can help stress the importance of information security. After all, according to Ponemon Institute (2013: 7), human factor, as shown in Figure 12, is one of the root causes of data breach.

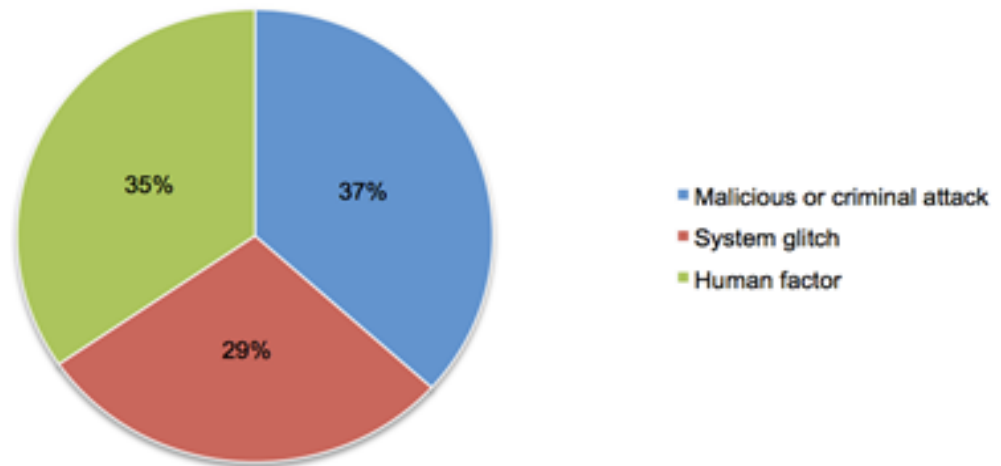


Figure 12. Distribution of root causes of data breach (Ponemon Institute 2013)

Of the 277 organizations globally that were affected by data breaches, topping the chart at 37% has experienced breach due to malicious or criminal attacks. But the fact cannot be ignored that 35% of these organizations were affected because of human factor which is attributed to carelessness and unawareness about security information.

Monitoring and Maintenance of Systems and Processes

Monitoring of the systems and their maintenance ensures that they function optimally. As for the process, monitoring sees to it that practices and activities are in compliance with the company's policy and is being adhered to by concerned individuals as well as allows process owners to make necessary changes if deemed necessary.

For the systems, continuous monitoring also allows visibility for stakeholders. Doing so provides an almost real-time snapshot and awareness of the state of risk, vulnerabilities and threats to company's information security, data, network, end points, cloud devices, and applications. Monitoring and the visibility it provides enables the company and its

management to exercise and improve governance through on-going assessment of control factors. Moreover, this also prevents a more grave situation wherein areas of risk pose an extreme danger to the company and more challenging and expensive to correct (Schultz, 2011).

According to the National Institute of Standards and Technology (2011: 17), continuous monitoring necessitates:

- maintaining situational awareness of all systems across the organization
- maintaining an understanding of threats and threats activities
- assessing all security controls
- collecting, correlating and analyzing security-related information
- providing actionable communication of security status across all tiers of the organization
- active management of risk by organizational officials

To implement a continuous monitoring program, there should be a well-designed information security continuous monitoring (ISCM) strategy. Creating this involves processes as shown in Figure 13.



Figure 13. Information Security Continuous Monitoring (ISCM) cycle (National Institute of Standards and Technology 2011)

As shown in Figure 13, the National Institute of Standards and Technology (2011: 16) explains the ISCM process as first, to **define** the strategy based on risk tolerance that provides clear visibility into assets, awareness of vulnerabilities, current threat information, and business impacts. Second, to **establish** metrics, status monitoring frequencies, control assessment frequencies, and technical architecture. Third, to **implement**

the program and collect the security-related information required for assessments, metrics, and reporting. Fourth, to **analyse** the data and to **report** findings and determine the appropriate response. Fifth, to **respond** to findings with operational, management, and technical mitigating activities or acceptance, sharing, or avoidance. And lastly, to review and update the ISCM program and adjust if necessary.

IT managers are under daily pressure to keep a fully functional system. This requires a 24by7 service. Doing so drives growth and keeps their customers and clients satisfied. Monitoring entails organizations to invest in technology. It might be costly, but early warning and detection of system issues and process failures through monitoring would prove beneficial to the organization and give more value to the business.

3.4.4 Establishing Access Controls

Access controls ensure that the person's access to information is authorized and restricted in accordance with the business and security requirements of the company (Finnish Standards Association 2010: 27). Rasmussen (2007 as cited in Bidgoli 2006: 424) also added that as a security service, it allows and denies permissions for users or programs to use the files and other programs within the system. According to Rouse (2014):

Access control systems perform authorization, identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

Rouse (2014) and INFOSEC Institute (2012) also added that there are four primary models of access controls, and they are mandatory, discretionary, role-based, and rule-based.

Rana (2011) and INFOSEC Institute (2012) differentiate the characteristics of these four models:

- mandatory access control – it is the operating system that makes the decision if the user can access a certain resource through the assigned security level
- discretionary access control - gives the user total control which is not very ideal as this could mean that the user can execute malware without being aware of it because of the privileges set could be higher than necessary

- role-based access control – this is tied to the role that the individual holds in the organization. The only drawback for this model is that the person has to find other means to have access to files that are associated with a different position
- rule-based access control - assigns access to a role based on the criteria set by the system administrator such as for instance setting time for a specified file to be accessed by the user

User Access and Authentication

User's access privileges to the system or program vary. But the most common is the ability to read, write, and execute a file or all files in a directory. Employees who need access privileges to systems and other programs are approved by a concerned manager before certain permission is provided by the system administrator.

In the event of employment or project/account termination, it is imperative that the employee's access to all systems and programs are disabled. Additionally, for the hardware like the laptop and hard drive, as well as other hardcopy information related to the project, need to have the necessary protection. Moreover, they must be returned when the project is complete or the employee is no longer connected with the company (Beaver, 2005). This is a common practice by most companies just like what one of the informants had shared,

"We have this part of the process when somebody is leaving, the HR department informs the corresponding stakeholder that all of the employee's credentials will be removed from all of the systems, and the company laptop and phone will be taken away."

(Benchmark 3, AN-CE-IT-03)

Most organizations also have a system where the concerned manager or supervisor has to send a request to IT for deactivations of all access for an employee who is transferred to another project or whose employment is terminated. A screenshot of this system as shared by one of the stakeholders, who was interviewed, is found in Appendix 7. The same system but with different fields as in Appendix 6 is also used for a request of access for a new employee. Appendix 5 also provides a sample of email coming from the corporate team of one of the international companies requiring stakeholders to verify validity of employee's access through the log-ins if one is still active or not.

According to Tipton and Krause (2007: 1813-1814), authentication is one of the processes that recognizes and verifies valid users or processes, and there are three major types. These are static, robust, and continuous authentication. They differentiate each one on the following texts.

Static authentication includes passwords and only provides protection against attacks in which an impostor cannot see, insert, and alter the information that is passed between the claimant and the verifier during an authentication exchange and subsequent session. The strength of the authentication process is highly dependent on the difficulty of guessing password values and how well they are protected.

Robust authentication relies on dynamic authentication data that changes with each authenticated session. This type of authentication protects against attacks because the authentication data recorded in the previous session is not valid for the subsequent session. To protect the user, one-time passwords and digital signatures are used since traditional fixed password will not be able to provide protection.

Continuous authentication provides protection to the user against impostors who can see, alter, and insert information passed between the claimant and the verifier even if the authentication is complete. This form of authentication is done by applying a digital signature algorithm to every bit of data.

These authentication processes are quite complex. But for employees and system administrators, awareness of the basic password management would prove to be helpful.

3.4.5 Reporting Incidents

ISO27001 defines information security incident as unwanted security event that can impair or weaken the system. No matter how strong the defences and controls are and even if the company has the best technology, information security incidents are inevitable. Just like what Benchmark 7 has shared during the interview,

“Even the best technology can be bypassed by a very skilled person.”

(Benchmark 7, JK-JL-IT-07)

Thus, awareness through training is intended to allow employees to recognize problems and incidents and at the same time respond accordingly to the situation (Lomprey 2008: 65). Additionally, the company policy should identify these incidents as well as the correct escalation path and communications plans.

In ISO27001, Brophy (2012) shares that although the section on information security incident management is reasonably short it is very vital. He added that the first of the two subsections was incident or events reporting. He thinks that this is the Holy Grail that needs to be done right. This is about getting the users, or anyone involved in the company to keep watching for events and if they find something is amiss, it has to be reported. But Brophy (2012) also believes that this requires a cultural change in most organizations as the perception is that if one reports an incident, either he is pointing to a problem that he or someone else has created, and they will be in trouble. But once the reporting process has been established and the employee is clear on how to report, who to report, and when to report, the next thing is to manage the incidents or events that were reported. This entails someone who is knowledgeable and competent to deal with these incidents when they come through. This person or somebody has to make a follow-up and act on it as it would be damaging if someone reports an incident not just once, or twice, but several times and nothing is done. When this happens, in the future employees will never report any incident.

3.4.6 Ensuring Business Continuity

Business continuity is the ability of the company to continue and provide the service for its customers and maintain its viability before, during, and after a business continuity event transpired (Lomprey 2008). The Business Continuity Institute according to Honour (2006) defines it as:

A holistic management process that identifies potential impacts that threaten an organisation, and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Brophy (2012) explains that business continuity is not a disaster recovery like when the system is down, and IT will find ways to recover and get it back up and running. Business continuity is far more encompassing, as it requires the company to look into its business

or the whole organization and understand the minimum requirements or level of service that the company has to deliver. On top of this, the company has to consider the risk assessment and consider the possibilities and frequency of risk to happen in the company and its impact on the business. Business continuity entails building a process and the system to ensure that the company can still offer the minimum level of service required regardless of any event.

3.4.7 Conducting Security Audit

Audits play an important role in ensuring that process, procedures, and policies are followed. Additionally, they ensure that the business is in compliance with relevant standards and legislations. Although audit will not guarantee the security of the network resources, it acts as a control to check whether the system or the process is working as it should be. At the same time, it provides feedback on the state of the company's security strategy (Cobb, 2011).

Some audits are either done internally or by some clients who are outsourcing their business. Others are done by the company's corporate team from the main headquarters. Not all companies conduct an internal audit. Others do it in preparation for the external audit done by the ISO certifying body. Other companies make this as part of their verification and validation initiative to the extent that some hire third party vendor to perform the audit for them. Doing so allows them to validate if process or part of the process is still in order and the company, along with its people, is in compliance with the process, guidelines or policies. As confirmed by these three stakeholders who were interviewed,

"For our production systems, we have it included in our configuration management process, it's like 3 or 4 times a year where they check our active directory in our production environment that it's updated. "

(Benchmark 3, AN-CE-IT-03)

"On a quarterly basis, we get an email from corporate to check if these logins are still valid. Every user will have a corresponding tool that they are supposed to have access to, and we have to validate that 'yes' if the employee is active. If there is no response, then all of those log-ins will be disabled."

(Benchmark 1, KC-LK-OP-01)

An internal audit typically has three phases as shown in Figure 14. These are planning, testing, and reporting. In all of these phases, the management has a major role. It is also important to note that internal auditors know what they are doing, have strong understanding of the process and the overall business, know what to ask for and have a constant training to continuously learn new guidance and standards of practice (IT Compliance Institute 2006: 7). Auditors are not the only one responsible for checking information security measures. All of the stakeholders have an important responsibility to perform in ensuring that information is secured. Although managers often try to relegate security responsibilities to an information security management function, everyone and all parts of the organization have responsibilities on security as shown in Appendix 8.



Figure 14. Audit communication flow (IT Compliance Institute 2006)

As shown in Figure 14, on the planning phase, auditors create an audit plan. This is where the management will focus and understand the audit purpose, focus, and approach. Communication is important to understand the expectations from the beginning.

The testing phase is where management facilitates auditor's access to appropriate systems and people. On this phase, the management confirms the audit results. Additionally, data and processes are verified to have that confidence on the audit result.

Reporting phase is where the management receives reports and reviews audit findings of auditors. Planning and developing of corrective actions and their implementations transpire on this phase. Appendices 9 and 10 show samples of checklists where audit report is generated from.

3.5 Information Security Management Process' Conceptual Framework

Information security management process covers a vast range of information as presented by various literature. For a small and medium enterprise (SME) like the case company, the conceptual framework is simplified to fit its needs. Moreover, by tailoring ideas based on the current need of the business, the implementation process could be faster and easier. In this case, the implementation, which is not covered by this research, will transpire depending on the decision of the case company.

The different elements of information security can happen in any part of the process as presented in Figure 15. For instance, managing assets does not necessarily come after the setting of the security policy since all throughout the process the company continues to manage its assets. In other words, this is a continuous process especially if there are new assets that need to be accounted for.

Furthermore, this framework evolved not only from ideas taken from different literature. Rather, from various interviews of stakeholders coming from different Finnish and international organizations that also shared some of their best practices in these areas.

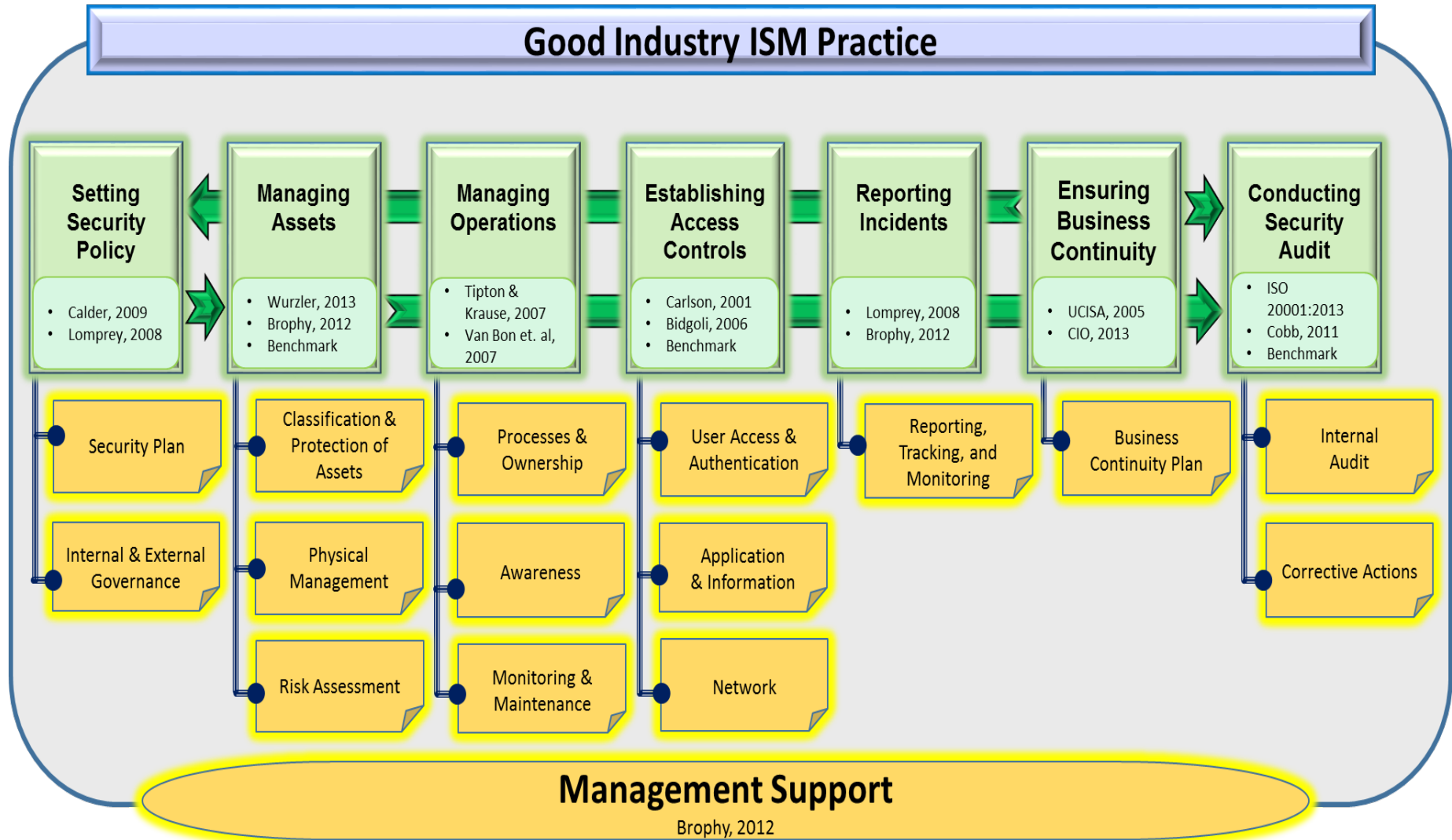


Figure 15. Information security management process' conceptual framework

The following texts discuss further the different elements of information security as illustrated in Figure 15.

Setting security policy or its revision if the document is already available commences the process. This document contains all the necessary information that cover all aspect of information security from the guidelines, roles, and responsibilities, reporting, metrics up until the various strategies and other security programs that the case company needs to have in place.

Managing assets focuses on the classification and protection of assets the company has. Along with this comes the assessment of the different risks that could happen if a specified asset is not properly protected or disposed of.

Managing operations covers all activities that involve the systems, programs, processes and employees. The hardware and software are more under the responsibility of the IT. This includes their maintenance, upgrading, and monitoring. But keeping the employees in the loop and making them understand the process and the changes, as well as their roles in the security management process, can be made possible through training and other awareness campaigns that operation leaders can come up with. Some of the topics can focus but are not limited to the following:

- company's security policy
- personally identifiable information (PII) that is associated with an individual
- knowing and understanding the risk for the company and the employee in the event of an information breach
- the value that information security brings for the company, the employee, and the customer
- guidelines that employees need to follow accordingly at work to ensure that customer information is secured and they are in compliance to the process.

Establishing access controls allows the setting of access rights to ensure that access to information is only given to authorize individuals. As there is sensitive information that is made available only to managers for instance and not to the rest of the employees, restricting the access accordingly will enable security of information to certain levels. Moreover, on this element is where log-in and password management, as well as website restrictions and deactivation of external hard drives that are not needed for the support, are put in place. Additionally, establishing access controls also incorporates granting and

terminating of employee's access rights to different systems and tools use in their support. It also iterates the responsibility of the IT and the leadership team in ensuring that logins are unique and are not shared among employees.

Reporting incidents has to be encouraged to all employees. Incidents can happen anytime. Thus, the company has to consider all the necessary measures when they indeed occur. But it is equally important that all incidents that are being reported are acted upon, closed, and feedback is provided to concerned individuals. Doing so will encourage employees to be more vigilant of its surroundings and all the associated systems and processes.

Ensuring business continuity may come towards the end, but as the business is established, the company ensures that contingency plans are present from the start, and the company can provide the service to its clients without any disruptions. This is element of information security entails thorough planning from the company as the plan is more focused towards preventive measures before a particular disaster can occur.

Conducting security audit falls towards the last stage of the process. This is a compliance check to ensure that processes are in place, followed and up to date. At the same time, this is also an opportunity to assess the readiness of the overall operation and the management in information security management. Upon completion of the audits and necessary assessments, countermeasures are planned and drafted. Countermeasures could be preventive or corrective actions the case company will implement. Preventive measures are plans to be implemented before a certain incident or risk will occur. While corrective actions are those where negative findings are found and need to be addressed. The entire process entails planning and assigning of owners responsible for the monitoring and completion of actions to be implemented. But most importantly, it is a continuous learning for all stakeholders.

In every aspect of the process, management support is vital. For all actions that need to be put in place, the management provides its support by allocating the needed resources. But this is not an easy feat as allocating resources can involve cost and in all cases cost has to be justified accordingly before a certain initiative or strategy, in this case having a structured information security management process, can be started.

4 Current State Analysis (CSA) of the Case Company's ISM Process

This section discusses the current information security process in the case company to find out whether information security has been ensured. The process under investigation for this Thesis focuses on the different best practice elements of the information security management process to assess the gaps and the status of the case company regarding the status of its information security. This section then summarizes some of the company's strengths and weaknesses which are aligned with the elements identified through best practices, as discussed in the previous section.

4.1 Overview of the CSA Stage

The CSA stage is conducted within the period 10th -21st of March 2016 through a series of six interviews with the stakeholders. All interviews were recorded except that of the IT manager as recording then was not possible due to technical difficulties and all responses were recorded in field notes. The different stakeholders are the team leaders, operations executive, assistant operations manager, IT manager, as well as the managing director. These are the people who have the understanding of the process and members of the management and operations teams who were given the authority to share some information. Considering that the case company is located in Singapore, these interviews were conducted through Skype video and phone calls and a WhatsApp phone call.

To have a complete understanding of the current process, along with the case company's strengths and weaknesses, various topics were discussed during the interview. An interview questionnaire was prepared and sent in advance to some interviewees. The questionnaire includes some topics that are focused on the different sections of the information security management process. These topics are, but not limited to, security policy, asset management, operations management, access controls, incident reporting, business continuity management, and security audit. As well as a discussion in general on the knowledge of the employees when it comes to information security management as well as the personally identifiable information that employees have access to.

On top of these interviews, some internal documents that are currently available were also reviewed. These documents include the security policy of the company, Non-disclosure agreement, access request form, employee handbook and a portion of the compa-

pany's code of conduct.

The goal of the current state analysis is to understand the current practices of the case company in ensuring that customers' information is secured and at the same time to check if employees are aware of their role in protecting and securing this information. Additionally, the CSA allows also for checking on the current process of the case company and identify some of the gaps that need to be addressed. The following subsections provides a detailed description of this process and gaps.

4.2 Description of the Case Company's Current Process in Relation to the Concepts of Information Security Management

The interviews that were conducted as well as the review of some internal documents provide helpful insights on the current state of the case company when it comes to their existing process on information security management. Since there is no documented process to review, based on the result of the interviews the researcher drafted the visual process that the case company has in relation to the framework of the information security management process. Doing so would provide a visualization of the things the case company has and does not have. This process is shown in Figure 16 along with its corresponding owner.

The ownership of each process is divided into four owners. First, the agents who are the technical support and customer service representatives of the case company. Second, the Operations Leadership that consists of the operations assistant manager, operations executive, who also happens to be the one responsible currently in documenting some operational processes, and the team leaders to whom agents are reporting to. Third, the IT team that consists of the IT manager and an external IT that was hired by the company. And lastly, the Sr. Leadership Team, that comprises of the senior manager, HR manager, and the managing director.

The process is scrutinised based on the seven sections that the researcher believes to be the simplest considerations that would cover all aspects of the information security management process and fits the need of the case company.

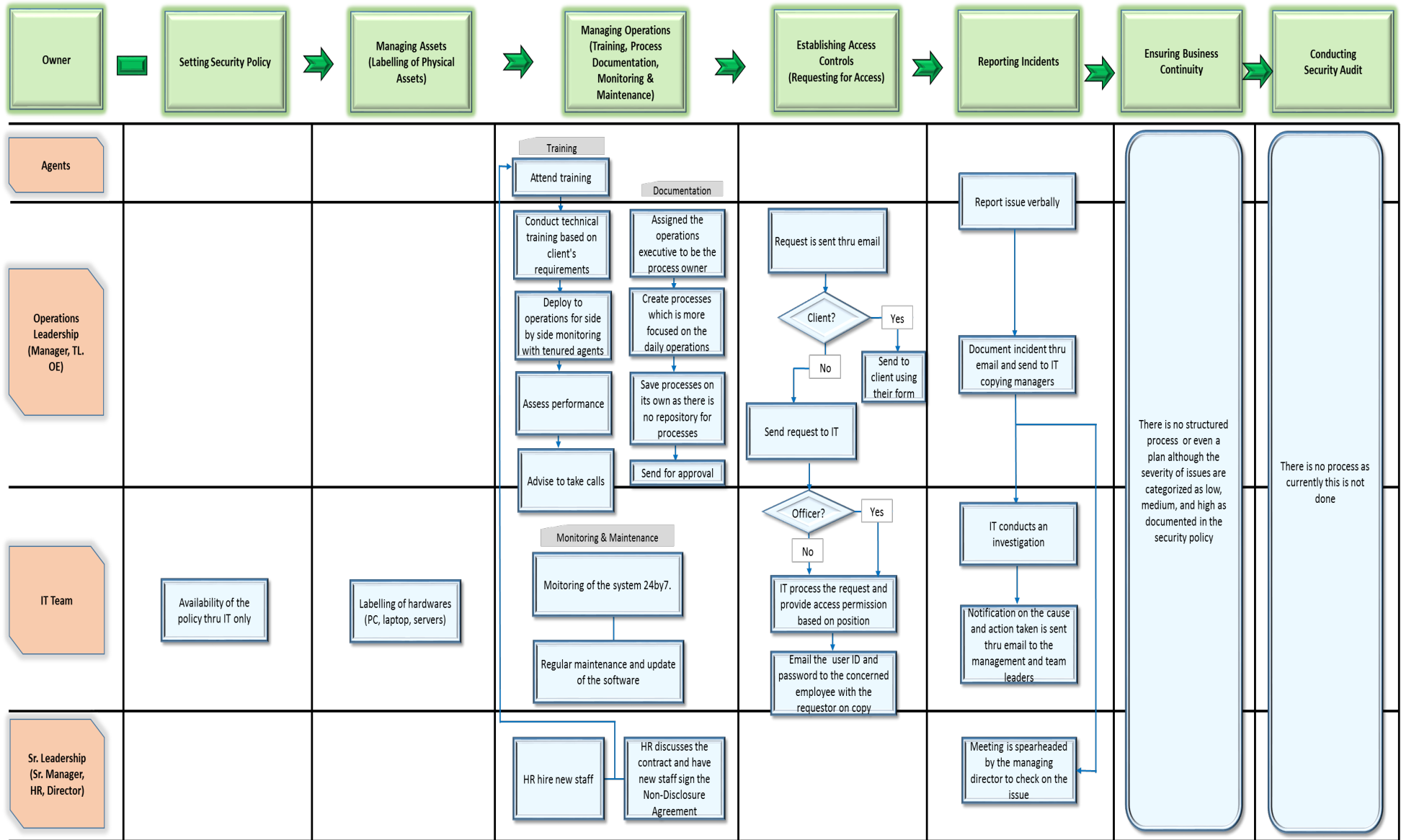


Figure 16. Case company's current process on information security management

As shown in Figure 16, most of the elements of information security are not covered based on the current activities of the case company. The following texts provide more information on each of this element.

Setting Security Policies

There is an existing security policy which is kept by the IT department. The policy was drafted on December 2011 and revised February 2015.

The policy covers information on the following:

- The responsibility of the IT team in the monitoring and maintenance of the case company's hardware and software which includes backup and restore, and the management of the data and electronic information that also involves the people who are managing the operations.
- The role of the department managers in providing training to their employees as well as in sending notification for the needed access of their team members
- Responsibility of the users in protecting and managing their passwords as well as the responsible utilization of the systems, emails and internet
- Incident reporting and escalation process

Managing Assets

Regarding asset management, the company is labelling some if not all of its asset. Figure 17 below is the label from one of its hardware.

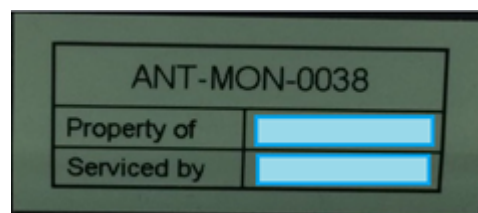


Figure 17. Label used by the case company for its PCs and laptops

This label as shown in Figure 17 is attached to the case company's assets and currently being maintained and tracked by the external IT team. The previous network administrator also confirmed that after the label is attached, the tracker is updated but this tracker is not available for verification.

When it comes to the case company's documents and processes, they contain the control number as shown in Figure 18.

Document Type	Policy Manual	Document Nº.	POI-001
Document Approver	HR Infrastructure/Director	Version Nº.	00
Security Level	Public	Effectivity Date	Jan 1, 2012



CHANGE HISTORY				
Date	Revision Nº.	Section	Details of Revision	Owner/ Modifier
December 1,2011	00		Origination	
February 5, 2015	1	6,7,8,9,10	IT Helpdesk Incident Reporting and Escalation Records Document Verification Document Approval	

Figure 18. Document labelling and recording of changes made

As shown in Figure 18, modifications and other revisions are tracked through the change history portion of the document. It also includes the name of the person who made the changes as well as the date when it was modified.

Managing Operations

This area is mostly the responsibility of the IT but on the operations side, management entails instilling awareness to every member of the team. This is done either through formal coaching sessions, team huddles, town hall meetings, training and re-training, and even casual chats on a relevant topic. One of the ways to keep employees and members informed is through the training.

Currently, the only training the case company has is focused on the technical support or customer service requirement of each account. The training is usually done when there is a new employee wherein the responsible team leader conducts the training for that new member of the team. During the hiring process, once the employment of the applicant is confirmed, the HR personnel discussed the contract. The contract includes information related to non-disclosure of information where employee signs a document referred to as non-disclosure agreement (NDA) as shown in Figure 19.

The training is specific to the processes and information related to the support of a particular client. Part of the training requires the employee to listen to calls with tenured agents through side by side monitoring. The training period varies depending on the set training plan of the client. For some clients, they do the assessment through the calls the

new hire has taken. Clients conduct a mock call where they assess the performance of the employee. If they are satisfied, then the employee is advised to 'go live' or ready to take calls. Else, additional training is done, or client requests the case company to replace the employee.

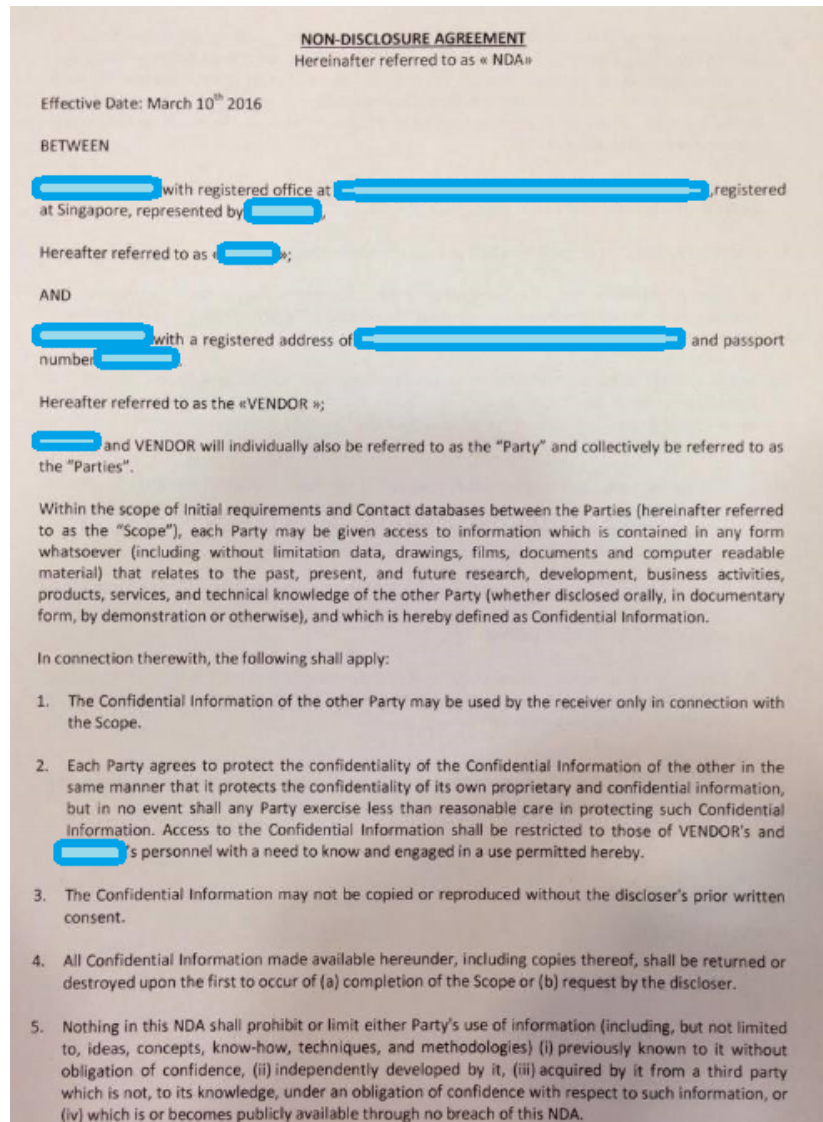


Figure 19. Non-disclosure agreement signed by the case company's employees

As shown in Figure 19, this is the NDA that new employee signs along with the contract. The document contains information that the employee must bear in mind while employed in the company. One of which is never to disclose confidential information to a third party.

Another way to manage operations is by having processes in place and having them documented. There is a newly assigned process owner who is the operations executive

handling also some accounts within the company. Currently, the processes that were created are more related to the daily operations and invoicing of the company. These processes are saved and kept by the process owner as there is no process repository yet.

As operations is running 24by7, monitoring of the processes, activities of the employees and the performance of the system is imperative. The IT team runs a system that monitors the entire operations 24by7. Regular maintenance is also done for that software in which update is needed. According to Respondent 6,

“Preventive maintenance is done on a daily, weekly, and monthly basis. Back-up is monitored since I joined a year ago.”

(Respondent 6, SN-AS-IT-06)

Establishing Access Controls

Access for every employee is managed by the IT team. Permissions are provided in accordance with the role of the employee. If the request is for agents, the level of access is intended for that role alone, else officers. As confirmed by Respondent 6,

“Top management has access to everything. Team leaders have access to their respective campaigns and other certain things like shared folder and printers. Agents only have access to their own campaign’s folders and cannot install or delete anything”

(Respondent 6, SN-AS-IT-06)

Access for agents is requested through email. If the access is for those systems owned by the company like for instance the customer relationship management (CRM) tool that is referred to as ‘Callfront’ and the phone which is known as ‘Eyebeam’, internal IT process the request. Once completed, user ID and password are sent to the concerned agent with the requestor on copy.

The access that will be provided by IT will allow the agent to view all campaigns that he handles as shown in Figure 20.

Callfront CRM Dashboard Campaigns Notes

SHORTCUT

- New Case
- Cases
- Search Cases
- Reports

New Case

Caller Information

Company Customer Name Contact No -select Country-

Problem Description

Details

Engineer Information

Escalated To Phone Service Hour?

Email Contact -select status-

Remarks

Cases Save

Different campaigns that correspond to the different clients

Figure 20. Screenshot of the case company's CRM system

As shown in Figure 20, the access provided by IT to the agent gives the agent access to those campaigns that he is hired and trained to support. In other words, the one user ID can access multiple campaigns depending on how many projects, referred to as campaigns, the agent is trained on. This set-up allows the agent to toggle between campaigns and handle multiple support in one shift without switching to a different system and changing log-ins and password. This might prove to be convenient for the agent, but the possibility of documenting information to the wrong campaign is high. Thus, the agent has to pay close attention to the documentation of notes and verification of the caller's information that they are intended to the right campaign.

On the other hand, if the access is needed for those systems that are owned by the client, some requests are made through email. Although there are also other clients, who would require for their official request form as shown in Figure 21 for one of those clients.

[REDACTED] - IT APPLICATION SYSTEM ACCESS FORM

(A) REQUESTED BY (Head of Dept):		
Name:		
Designation:		Department:
Date:	Signature: _____	

(B) STAFF(User) Particulars:			
Name:			NRIC/FIN:
Designation:		Department:	Access Type: <input type="checkbox"/> Permanent <input type="checkbox"/> Temporary / Contract
Commencement Date:		End Date :	
By signing I agree that, I will ensure proper logoff from the above application & I will be solely responsible for the confidentiality of information & of the User ID and Password that may be issue to me based on this request.			
Date:	Signature: _____		

(C) IT APPLICATION SYSTEM DETAILS:						
Application Name:	<input type="checkbox"/> CLS	<input type="checkbox"/> HIVE	<input type="checkbox"/> EADMIN	<input type="checkbox"/> Plus	<input type="checkbox"/> T1	<input type="checkbox"/> Voucher system
	<input type="checkbox"/> CMS	<input type="checkbox"/> ARC	<input type="checkbox"/> CALTEX		<input type="checkbox"/> Padma	<input type="checkbox"/> Target One
	<input type="checkbox"/> SAGE	<input type="checkbox"/> RFTS	<input type="checkbox"/> BHG		<input type="checkbox"/> Spark	
Database Access:	<input type="checkbox"/> DB Name _____					
	Note: Only read access is provided for Databases. If any other access required, need to get prior approval from HOD and attach the approval with the form					

SAGE User Group:			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(Front/ Backend)	Call Centre	Call Centre
SAGE User Rights:			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Call Agent	Call Supervisor	CSO	IT Admin Manager
Note: This section is <i>only</i> applicable for SAGE application			

Figure 21. IT Application System Access Form as provided by one of the clients

The above form is a client requirement every time access is requested. This form needs to be filled-out by the team leader before the agent can be given access that would enable the latter to take calls for that particular campaign.

Reporting Incidents

When an incident or event happened, the person who discovered the incident informs the team leader. The latter then informs IT verbally. Email documentation to IT copying all officers follows to document the incident officially. The team leader then notifies the client. While IT checks and conducts an investigation, the managing director, most of the time, calls a meeting to discuss the issue. This is just one of the several meetings that usually follows. In most cases, if the issue involves inability of the agent to take calls

because of the non-functionality of the phone system which usually lasts for an hour or so, there are follow-up meetings to discuss the result of the investigation and the countermeasure that was done.

Not all clients will require an incident report. But if there is one who would require it, the manager will come up with one to let them know what transpired and why such incident happened. In the report, action plans are included along with target dates and owners of every action. The actions plans included serve as assurance for the client that the case company will have to perform to ensure non-recurrence of the issue.

Ensuring Business Continuity

There is no process in ensuring business continuity. According to Respondent 6,

"BCP document is available. It was not used before as we do not have the luxury to do the long drill."

(Respondent 6, SN-AS-IT-06)

Conducting Security Audit

No audit is happening within the case company. When Respondent 5 was asked if there is any audit being done, he confirmed that there is none. As a matter of fact, when the researcher mentioned that the company is very focused on operational services and financials aspect and at some point processes are swept under the rug the said respondent confirmed this statement to be true.

Some clients are doing their audit. During the interview with the managing director, he mentioned that one of the client's representatives just left the company's premises after spending a couple of hours doing an audit with the team leader handling their campaign.

4.3 Case Company's Strengths and Weaknesses

Although there are some strengths observed on different areas of information management within the case company's operations, the number of weaknesses still outweigh its strengths. To get a clear picture as to which element of the information security management framework the case company is adequate or lacking, questions that are focused on these elements were considered during the interview.

4.3.1 Strengths in Information Security Management

Despite over a decade of operation in the service business, observed strengths for the case company is just a handful. Especially in the area of information security management, this is particularly vague, but it is good also to note that at some point, some things are still visible.

Security Policy. The case company has a security policy which is good to have as this policy is like a foundation of any information security management system. With the policy in place, the company has a basis of how to manage its assets to protect the information that it has for its clients and its client's customers.

Managing Assets. The case company has a new IT team which is outsourced. With this new team, there are some new developments in place like for instance on February 2016, the case company launched the new payroll software with this IT partner. With this new system in place, manual calculation of employee's salary specific to overtime will be automated and would eliminate error on the pay of the employees. Employees will also be able to print out their payslips which was not done before.

The case company has also purchased ten new high-availability servers. Having these systems will mitigate issues on downtime that could result in data loss, client dissatisfaction, and business problems. With these servers and other hardware, the IT manages these assets by labelling and tracking.

Managing Operations. Currently, there is already an assigned owner to draft processes that the operations need.

Establishing Access Controls. Active directory containing a list of all employees with their corresponding access is regularly updated. During hiring or termination, team leaders automatically request for activation or deactivation of employee's access. As shared Respondent 6,

"Active Directory is updated, and every campaign has it which includes the access each employee will have when it comes to the folder and services. We have complete control on this.

(Respondent 6, SN-AS-IT-06)

Access permission is established based on the role of the employee. When it comes to network and database access including authentication,

“Most of the malicious sites have been restricted, but there are some loopholes. Restriction is through the firewall. As for the password, it’s only changed for the first time the user will access a certain system. Database is also protected, and nobody can access the PC level.”

(Respondent 6, SN-AS-IT-06)

Reporting Incidents. These are some reports generated by the operations manager. This incident report is submitted to the clients to provide some assurance that the issue is being or has been addressed, and some countermeasures are put in place to avoid recurrence.

Ensuring Business Continuity. For possible major breakdown that will not allow the current site to perform its operations, there is another location that could cover and provide the support.

Conducting Security Audit. Although the audit is not done by the case company, the latter is open to clients conducting their own audit based on the need of their campaign. In most cases when negative findings are reported, which seldom happens, by the client to the case company’s management, the latter addresses them accordingly.

4.3.2 Weaknesses in Information Security Management

The result of the interviews conducted with different stakeholders was proof enough that information security management is not the priority of the case company but instead the financial aspect of the business.

Setting Security Policy. While it is nice to know that the security policy is available, the issue is that this policy is not known to the employees. The document as checked was not approved by the managing director who is the signatory of the document even if it has been revised last February 2015, four years after its origination. It was also verified during the interviews with the assistance manager, operations executive, team leaders, and even the managing director if they have a security policy, and everyone confirmed that they do not have one. As mentioned by Respondent 5,

“Well, unfortunately, we don’t have a security policy. Everybody is so busy it’s crazy.”
(Respondent 5, EN-AS-OP-05)

During the interview with the IT manager on the 21st of March, he mentioned that there is a policy, but it is not used. He shared this document on the 2nd of April in which the researcher has also shared to the other stakeholders. The IT manager mentioned in his email that this policy can be used as a base guideline for the company.

Managing Assets. Though it is true that assets are labelled, there are still other assets like the headset that is not labelled as shown in Figure 22.



Figure 22. Unlabelled asset (headset)

As seen in Figure 22, and as confirmed by one of the team leaders, some of the headsets have not been labelled. This is contrary to what the previous system administrator had shared when he was asked during one of the chat conversations that all of the case company’s assets are labelled and tracked. But with the new IT partner, although it has not been completed yet, the team has started to standardize the labelling of assets as shown in the previous Figure 17.

Another issue that the case company has to address is the handling of proprietary documents. As confirmed by Respondent 4,

“We have to shred in a real-time basis but there still lapses so in my team of around 80% of the time we are shredding documents as one of our clients called our attention regarding exposing documents in our station.”
(Respondent 4, RC-AS-OP-04)

He also confirmed that it is possible that other campaigns are not practicing shredding because their clients are not as stringent as the others.

Managing Operations. This element of information security management lies on the IT team. During the data 1 collection, the IT Manager is working offsite and was in the process of completing his handover to the new IT partner that is outsourced as he is leaving the company. Some of the information shared during the interview cannot be verified with the existing team. During his stint, there was no other IT staff, and it was just a one-man IT team. Except for the software and application-related information, the IT manager cannot provide further information related to operations management of the system and other assets. According to him,

"I am more on the application side; the hardware is not managed. Other engineers who left were more in-charge of the hardware. I take control of the application side."

(Respondent 6, SN-AS-IT-06)

Operations management involves checking for awareness of agents when it comes to information security and the risks involved if control is not in place and system is not protected. For one, this is absent in the training and daily operations of the case company. All employees are just focused on providing the support based on clients' requirement. There is no initiative available that exhibits awareness campaign. The first time the employee will know that information should not be disclosed is during the signing of the contract. Other than that, any communication on information security is missing in the daily operations.

On top of the awareness campaign that needs to be implemented, it is important that information security processes are documented, tracked, and modified as needed based on the needs of the company and in accordance with the requirement of the client and the company policy.

Establishing Access Controls. When it comes to websites access, restrictions are done through the firewall. Although Respondent 6 has previously stated that most of the malicious sites have been restricted, he also recognized the loopholes,

"If the agents will use HTTPS the firewall cannot detect it."

(Respondent 6, SN-AS-IT-06)

Respondent 4, also confirmed that,

“Some of our agents’ computer can still access other websites that may be unsafe for some of the systems we have right now. Because if we can access any public websites you can easily disclose or spread information.”

(Respondent 6, SN-AS-IT-06)

Incidents related to sharing of log-ins are also happening in some cases when the agent is not able to use the log-in for some reason, and this happens at a late shift where IT is not present on site. When this happens either the Team lead logs in in the system, in behalf of the agent, or use another agent’s log-in. This is quite critical as there are instances of client escalations, and sharing of log-in poses a challenge to identify ‘real’ owner of the case documentation unless the team lead listens to the call recording. Nevertheless, the agent can abuse the use tool log-in and might result in not reporting any issue with own log-in knowing that somebody else’s log-in is always available for use.

Reporting Incidents. Though it is true that the reporting happens. This process is not consistently done. Reports are usually generated when clients demand one. And if it is done, it lacks some follow through on the closure of the issue and completion of the actions. There is no proper tracking and reporting as confirmed by Respondent 3,

“If I want to backtrack history, there is none. I cannot say if this has happened before. No template and no form.”

(Respondent 3, SN-AS-IT-06)

Ensuring Business Continuity. This element of information security is considered to be no easy feat as it involves planning and strategy building on the side of the case company to ensure that the minimum level of service required is still met regardless of the incident. But how can this be performed when even the little processes that need to be in placed are missing or lacking? It is clear that the company has no process at all related to business continuity management.

Conducting Security Audit. Audit in any form, may it be internal or external is not part of the case company’s process. Even with the current manpower, there is an issue on establishing owners to perform certain tasks the company considers to be more important. Business development for instance or acquiring more clients which involves drafting of proposals have no current owner as the previous owner finds it difficult with the current

tasks assigned to her. Thus, it cannot be expected that the company can assign someone to perform the audit especially if this is not a priority of the company. As shared by Respondents 5 and 6,

“We don’t have a compliance department. We don’t have an IT department. Currently my IT is outsourced.”

(Respondent 5, EN-AS-OP-05)

“No one audits you ‘coz nobody audits as long as client is happy.”

(Respondent 6, SN-AS-IT-06)

4.4 Summary of Key Findings

Gathering information from the various stakeholders of the case company proved to be challenging. Finding areas where its strengths is almost non-existent. Though documents were reviewed, there are very limited documents that are available related to information security management process.

The result of the interviews points to several weaknesses of the case company. It is evident that the management does not support any initiative related to information security management, nor they are equipped to even with the right amount of knowledge required to understand the value of information security and the risks involve when systems and processes are breached. But there seems to be a light at the end of the tunnel with the current IT team the case company has partnered with. Although time and opportunity did not permit an interview and verification with this team, feedback from some stakeholders bespoke improvement on some of the processes.

Some high points and several negative findings are gathered during those interviews and they are summarized as shown in Figure 23.



Figure 23. Summary of case company's strengths and weaknesses

There are several areas in the process where the case company is found to be lacking. On the researcher's point of view, this is because the company is not well aware of the various elements and set of actions that need to be considered to fulfil the initial requirement of an information security management process. In essence, the case company is missing a framework in a form of a process that would guide and provide the support that it needs to start implementing some actions.

5 Building the Information Security Management Process

This section merges the results of the summary of the current state analysis and the conceptual framework but at the same time, this section also includes information gathered during the discussion with stakeholders during the collection of data 2. Additionally, some feedbacks from the gathering of good practices from stakeholders of other companies are considered to be valuable in some of the process areas. All of this information gathered were used towards the building of the proposal. The contents of this chapter are the overview of the process of how the proposal was developed and the initial proposal that was submitted to the case company's stakeholders for their feedback. The proposal is drafted in such a way that the proposed activities for the case company to perform were taken into account in each of the seven elements.

5.1 Overview of the Proposal Building Stage

It has been concluded that the case company has no structured process of information security management process based on the interviews that were conducted. From the CSA stage, the weaknesses were gathered and summarized. Additionally, during the course of the interview on this stage some information were initially collected for the building of the proposal. Researcher posed a question to the stakeholders,

"If there is one thing like a process that you want to have or want to know for the company when it comes to information security management, what is it or what are those?"

Some of the interviewees expressed the things they would like to have in place like for instance the availability of the training material that would cover some of the topics related to information security. But other than this, most of them are not entirely aware of what they need for the company that the researcher could help on. One of the interviewees expressed that,

"You see the challenge for me nowadays if you would like to know. It is very operational to me; it's very technical to me so there are many things that unfortunately based on my monkey brain I cannot be aware honestly speaking I must confess. So this is my challenge, this is my gap."

(Respondent 5, EN-AS-OP-05)

Another interview was conducted on 13th of April with the operations assistant manager as the rest of the previous stakeholders were not available for discussion to officially build the proposal. During this session, the concept of the information security management processed was discussed along with some sample forms and guidelines that the case company can make use of.

At the onset of the interview, it was quite challenging to get some ideas from the interviewee to build the proposal. Thus, with the information that was gathered from previous discussions along with some feedback received during the gathering of best practices with other companies, and with the concept of information security management, a summary of the proposal as shown in Appendix 12 was drafted. This was further improved and included the corresponding owner of each item as shown Figure 24. This improved proposal summary was sent to the different stakeholders for their feedback. However, the color-coded boxes and the codes L, C, and D2 were not included. The codes stand for the sources of these action items either as suggested by literature, result of the current state analysis stage, or those information gathered during the data 2 collection when the proposal was developed with the stakeholders, respectively.

Most of the action items drafted for the case company to perform were the result of the CSA stage. These needed actions are evident under the elements of managing operations, establishing access controls, and reporting incidents where even the basic form and flow are missing. But to also address these weaknesses, best practices from literature and other companies are taken into account.

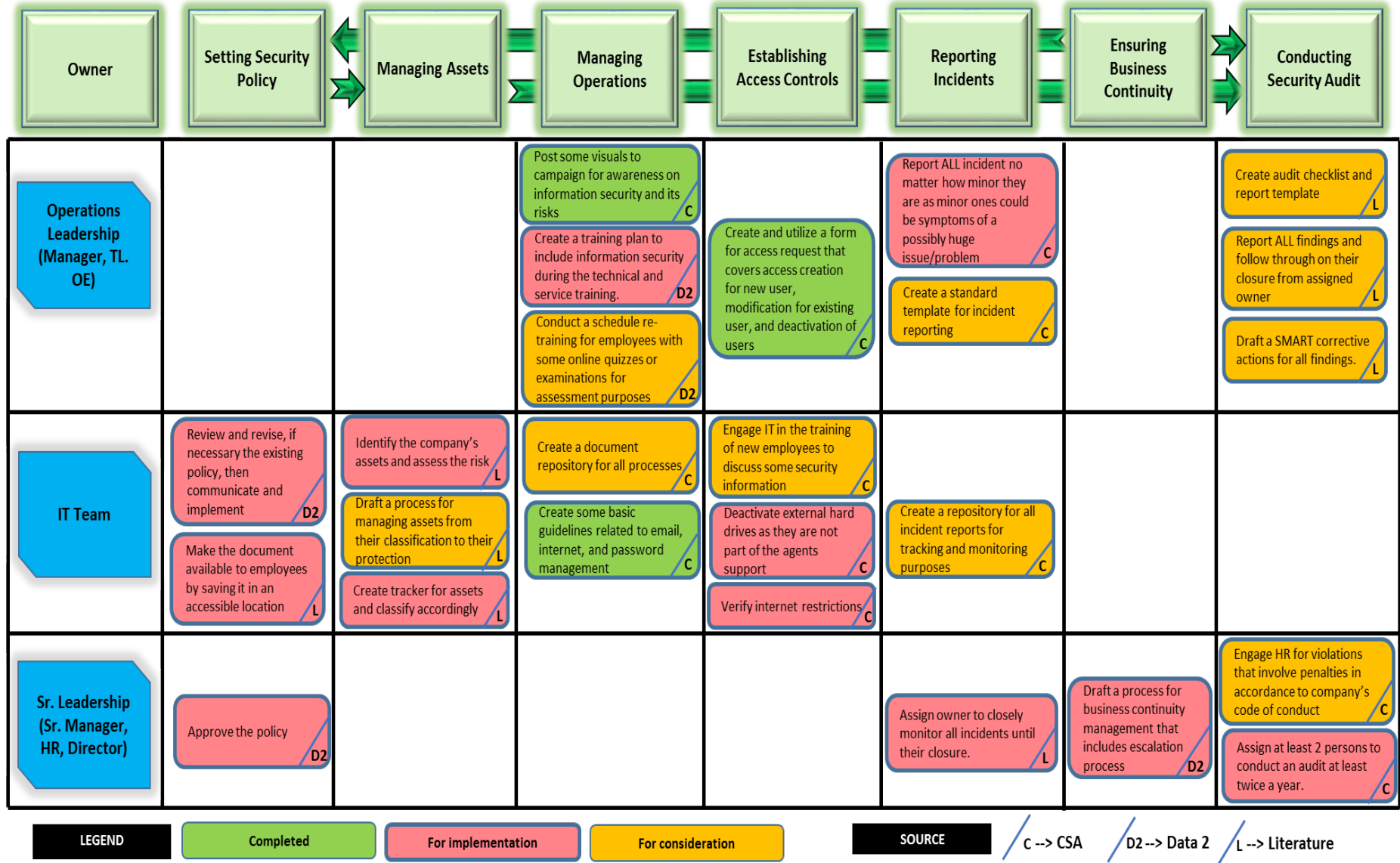


Figure 24. Summary of the initial proposal on information security management

As shown in Figure 24, there are some actions the case company has to prioritize 'for implementation', and the basis for coding such is because these are crucial items regarding information security and need to be in place for the process to be started. There are also those that they could consider at a later time as this could mean further discussion and consideration on their end. There are also some items that were highlighted in green that were done and provided by the researcher to the case company. These are considered to be small wins that if the case company can utilize and start to implement will be helpful to commence the process at some point.

5.2 Setting Security Policies

During the discussion with the principal informant, we talked about the security policy of the company which is already available. Since it is not known to everyone except the previous IT, it was discussed that the document has to be reviewed by the different stakeholders of the operations and IT team, but the latter will own this action item. Considering that the document has not been approved yet, following the review will be the approval of the document. Official approval of the document has to be done by the senior leadership and in this case by the managing director.

As the policy involves all entities within the case company, especially the agents, it has to be made available to them by saving it in an accessible location. Team leaders and managers have to ensure that employees understand the content of the policy and questions are asked if necessary. These three action items will cover the element of setting security policy.

5.3 Managing Assets

This section of the process is the responsibility of the IT team. And currently, the case company does not have an IT team of its own but rather an outsourced one. Thus, the managing assets element of the process is not verified.

Nevertheless, it is important to include still the action items that need to be in place to ensure that all of the company's assets are accounted for, and possible risks are identified in case these assets are not updated, protected, maintained, and disposed of accordingly.

The ideas come from literature as the key informant cannot speak more about this stage of the process as their assets are managed and controlled by the external IT.

With this, the IT team has to identify all of the case company's assets and ensure their tracking. A documented process known to concerned individuals would be helpful in the event there will be new employees who will handle these assets. This process will provide some guidelines for natural transition and proper handling of assets and to guarantee that all areas are covered when it comes to asset management.

5.4 Managing Operations

Just like in managing assets, managing operations is mainly the domain of IT as this involves monitoring and maintenance of the system and the process. But in another aspect of managing operations what was discussed was within the scope of the operations team which means those that can be done by the team leaders and managers. Since managers and team leaders have their set of responsibilities to ensure that some processes and initiatives are in place related to information security management, this is the focus of the proposal. Thus, the discussion is geared towards training and awareness campaigns in which a proposed process flow is shown Figure 25.

In any change or a new process to be implemented and information to be relayed, it is just right to have a well-informed employee to avoid resistance and embrace acceptance. Training always provides an excellent venue to ensure that everyone is on the same page in understanding new information. But it is not enough to just do the training without any knowledge check afterward. Thus, in every training, an assessment that can either be done online or through the traditional way of providing paper tests/quizzes would prove to be helpful if trainees understand the topic and has retained the information that has been shared. Employee education is not a one-time activity; rather it would be beneficial if there is a periodic training or even a huddle session that will be initiated by the team leader. Doing so will build a habit and consciousness on the end of the employee on the importance of information security.

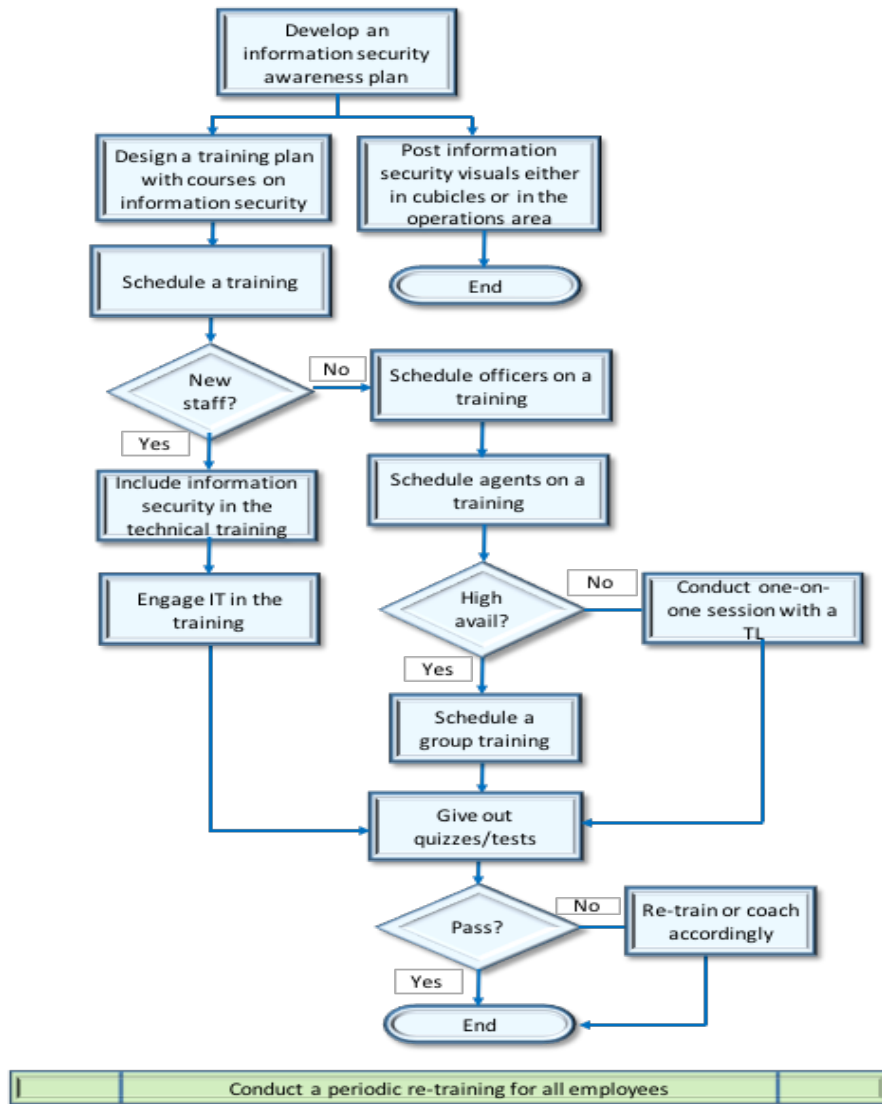


Figure 25. Information security awareness process flow

The process flow as illustrated in Figure 25 is drafted to provide a guide on how the case company could start to campaign to its employees the awareness on information security.

As shared by an informant from one of the Finnish IT companies who was interviewed,

“I personally believe that the most important risk to consider is the internal risk, the internal employees. Not malicious practice but things like mistakes people can make if they are not aware. So the best practice is to make people aware. To continuously teach them about the simple things that they need to take care and they need to understand in handling security risks.”

(Benchmark 7, JK-JL-IT-07)

Therefore, campaigns through training and other means to advocate awareness would be helpful for employees and the whole organization.

It would also be useful to consider some guidelines for employees especially agents to utilize and follow. Some of these guidelines, as inspired by Bidgoli (2006: 425-426) are shown in Figures 26 and 27.

EMAIL AND INTERNET GUIDELINES

SCOPE:

This guideline covers email, internet, and intranet access. Included also are messages, files, records, data, and all electronic communications that are stored, copied, or transmitted by or on Company-owned or leased equipment, system, or asset.

- Email and Internet are intended for Business Use ONLY.
- All files, data, and any electronic communications remain as company property even if it is transferred or copied to an equipment/application that is not owned by the company (e.g. USB, personal emails, mobile phones, external hard drives, social media accounts, etc.)
- All information communicated using company owned property/systems, may it be thru email or the internet, remains as company property and should not be considered as private even if it is personal in nature.
- Employees must avoid sending spam emails especially if they are not related to their work.
- Employees may not use company-provided-email and internet for viewing, storing, or distributing pornography, sexually offensive materials, and harassing or discriminatory communications related to sex, gender, race, religion, national origin, age, or disability.
- Employees must be more vigilant in opening email attachments especially if they come from unknown sources.
- Confidential and proprietary information must not be disclosed on any form of communication.
- Personal log-ins must be used by the employee themselves and not to be shared to anyone or borrow somebody else's.
- Before employees leave their respective workstations, PCs must be locked in order for unauthorized individual not to use them.

Figure 26. Email and Internet Guidelines (Bidgoli 2006)

PASSWORD GUIDELINES

SCOPE:

This guideline covers password management that system administrators do as well as education and awareness to be instilled to users.

- Employees should be educated about the importance of keeping their user IDs and passwords confidential.
- Employees should be encouraged not to write down their passwords. If they do, the company should advocate storing them in a secure place.
- Default password should be assigned when the account or access is created and users must be prompted to change this password upon initial log-on.
- Passwords length should be a minimum of eight characters and configured with combinations of upper and lower case alphabetic characters, numeric, and special characters.
- Communications regarding account creation or user IDs and password initialization should be done separately.
- Passwords should be set to expire with the system-wide parameter within a minimum of ___ days.
- Screensavers must be utilized to enforce automatic log-off for periods of inactivity greater than ___ minutes.
- Accounts should be automatically locked out following ___ to ___ password attempts guesses. System administrator should be the one to re-enable them.
- Password history should be configured to ensure that users do not reuse old passwords over a period of time.
- Passwords should not be displayed on screen but should always be masked with special dummy characters like asterisk.

Figure 27. Password Guidelines (Bidgoli 2006)

As seen in Figures 26 and 27, these guidelines are related to the responsible use of internet and email as well as that for creating a password to ensure that access to systems and tools are secured and have a strong authentication. Having these guidelines visible and known to employees will keep the latter aware of the responsibility in utilizing the company-owned system.

Another important initiative to consider is the posting of visuals. These posters as shown in Appendix 11 and Figure 28 can serve as a constant reminder of how valuable information security is and that every employee is responsible for making things happen.

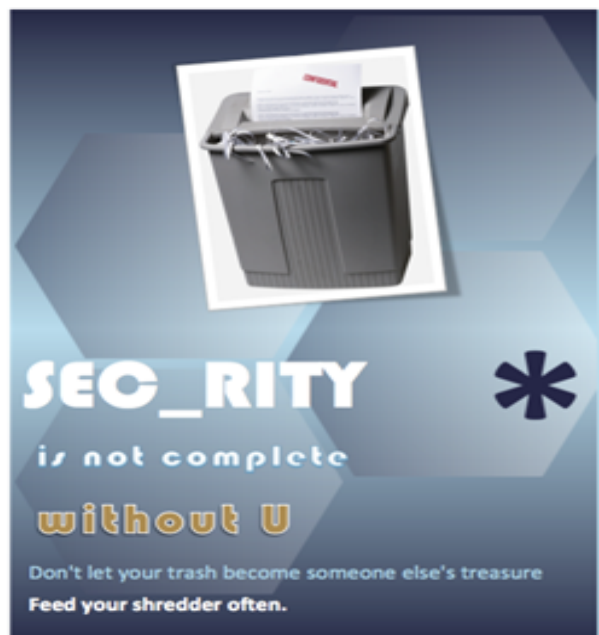


Figure 28. Poster on security awareness

The poster can be used by the case company to campaign for awareness on information security. It can be hanged in strategic areas of operations to serve as reminders that important and confidential documents have to be kept and shredded if not anymore in use. But of course, the case company needs to have a training and constant reminder about the risk if security is not ensured. The poster will not serve its purpose if the management will not give out its support and instill in the minds of its employees the importance of information security.

Awareness campaign covers only one part of the best practice element in managing operations. Process documentation another important aspect of operations management. This is not necessarily a best practice but rather a necessity for an organization to have.

It is not enough that process will be documented and be saved anywhere. One best practice and which is recommended for the case company to have is a centralised filing system to store not only processes but at the same time files containing confidential information. Since processes and confidential or proprietary information are considered as critical company assets, a decentralised system could jeopardise the security of these assets and could also pose a potential issue on data breach. Moreover, this system allows an efficient business operation as it will eliminate time wasted in file retrieval. Additionally, this increases security as it offers only one point of access that can easily be monitored and restricted especially that most companies (Secure Data Management, 2014).

5.5 Establishing Access Controls

When it comes to providing access permission to employees, the IT team has their process. They also follow certain guidelines in restricting network access. The process flow shown in Figure 29, is more applicable to the operations or the team leaders and managers in cases when an access request is needed.

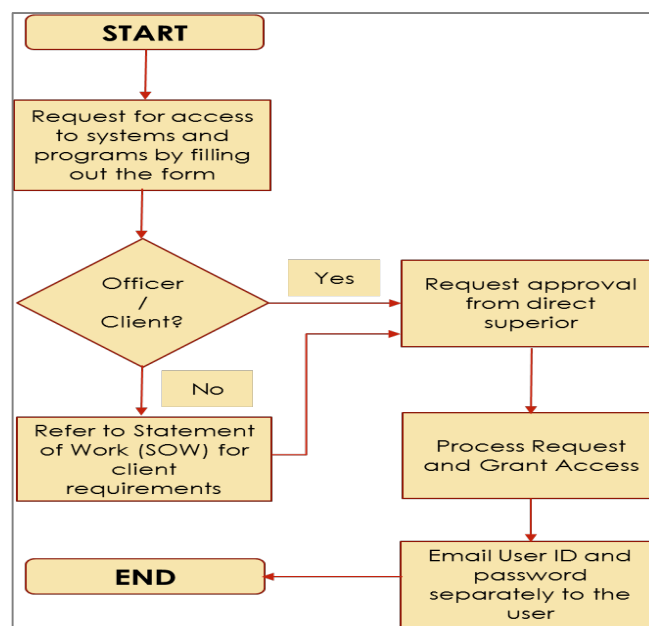


Figure 29. Access request flow

Since the assistant manager has confirmed that there is no guideline or standard that the team can follow, this simple flow can serve as a guide on how access request should be done. It was also mentioned that the case company has no ticketing system nor form to use. Thus, a user access request form is drafted ready for use by the case company.

Company Logo	<h1 style="margin: 0;">USER ACCESS REQUEST FORM</h1>		
Request Purpose			
<input type="checkbox"/> Add New User <input type="checkbox"/> Modify User Access <input type="checkbox"/> Deactivate Access			
Requestor Details			
Date			
Name			
Designation			
Department			
User Information			
Name			
Email			
Designation	<input type="checkbox"/> Temp. Staff <input type="checkbox"/> Agent <input type="checkbox"/> Team Lead <input type="checkbox"/> Manager <input type="checkbox"/> Client*		
Department	<input type="checkbox"/> Operations <input type="checkbox"/> Management <input type="checkbox"/> HR <input type="checkbox"/> IT <input type="checkbox"/> Client*		
Shift			
Effectivity Date			
System and Program Access			
<input type="checkbox"/> Email <input type="checkbox"/> Callfront <i>(Specify the Accounts: _____)</i>			
<input type="checkbox"/> Internet <input type="checkbox"/> Remote			
<input type="checkbox"/> Intranet <input type="checkbox"/> Hard drive <input type="checkbox"/> Payroll System			
<input type="checkbox"/> Sharepoint <input type="checkbox"/> Folder/Directory <input type="checkbox"/> Finance System			
Callfront	Eyebeam	Internet	
<input type="checkbox"/> Level 1 (Agent) <input type="checkbox"/> Reports <input type="checkbox"/> Administrator <input type="checkbox"/> Clients	<input type="checkbox"/> Level 1 (Agent) <input type="checkbox"/> Reports <input type="checkbox"/> Administrator <input type="checkbox"/> Clients	<input type="checkbox"/> Full Access <input type="checkbox"/> Selected Sites <i>(based on the client's list or company requirement)</i> <input type="checkbox"/> Intranet Only	
Distribution List <i>(please list)</i>			
Additional Remarks			
Approval Information <i>(attach email approval)</i>		System Administration <i>(to be completed by IT)</i>	
Approved by		Processed by	
Signature**		Completed on	
Date		Remarks	

* Duration of the access has to be specified under 'Additional Remarks' for client-related requests. Email request coming from the client has to be attached to this form.

** Signature has to be affixed if this form is printed and signature is sought, else, email approval from supervisor / manager will suffice

Form and Revision Number

Figure 30. User access request form sample

The user access request form as shown in Figure 30, contains all the necessary information that is specific to the case company. This would serve as a checklist in requesting for employee's access may it be for a new user, access deactivation, or access modification. This form is drafted in response to the feedback of one of the respondents on the concern that the team does not know what needs to be requested if there are new employees.

5.6 Reporting Incidents

First and foremost, all employees must be encouraged to report all incidents no matter how minor such incident. An incident report needs to be created. As discussed with the key informant, it would be helpful to have a standard template as well as a repository for all incidents so track history of issues and review previous actions.

With this, IT needs to create this repository and a standard template has to be created where reporting will not only be done by the manager whenever a client requests for it but rather, for all officers to use and for all events to happen.

Since it is not enough to just report incidents, the senior manager has to assign an owner to review and close all reported incidents. Employees must see that the incidents that were reported are acted upon so they will continue to be vigilant of other issues.

5.7 Ensuring Business Continuity

This element of information security is quite complex as this entails planning from the management. Thus, the senior leadership team needs to draft a plan and involve all departments to gather inputs. The plan should include the analysis of the event's impact on the business like for instance if the telephone line is disrupted and no calls would come in. When this happens, the company will incur a loss, but this cost impact needs to be analysed and provide measures to at least mitigate the issue.

Since the case company already has another site in the event of a breakdown, this should be part of the plan that needs to be worked out. Once the plan is complete, it needs to be tested. Simulation exercises that involve employees will be beneficial to campaign for awareness in case these unwanted events will take place.

5.8 Conducting Security Audit

An audit has never been conducted by the case company. Thus, the key informant is not aware as to who will do the audit. With this, it is proposed that the senior leadership team specifically the senior manager assigns at least two persons to spearhead the process. It would be ideal that each depart has to have a representative but considering the manpower of the case company, this is not possible. The audit can happen once or twice a year depending on the frequency that the case company will decide. As this process is not present, checklists and all pertinent information related to security audit are not available. To start this off, a checklist needs to be drafted.

At the end of the audit, findings need to be reported to all stakeholders. The respective process owner who will be assigned by the internal auditors from operations will draft a SMART action plan. This means that the actions are specific, measurable, achievable, relevant to the issue that needs to be addressed and time bound which means that it is expected to be completed at a particular time or extend if deemed necessary.

5.9 Summary of the Proposal

The initial draft of the proposal is designed to address the gaps, and those weaknesses found as evidenced in the current state analysis. The content of the proposal which are the elements of the information security management is inspired by best practiced from literature and information gathered during the interview with various stakeholders from other companies. Table 7 compares the current process of the case company and the proposed process.

As shown in Table 7, several elements of information security are not evident in the current process of the case company. Although some actions or processes under each element are in place, there are still gaps that need to be filled in. For instance, the security policy is available but it is not known to all especially to the leadership team as it was just drafted, but no review and approval were conducted. Furthermore, in reporting incidents, events are not tracked. Thus, there is no history to check in case these events recur.

Table 7. Case company's current process vs. the proposed process

#	ELEMENTS OF ISM	CASE COMPANY'S CURRENT PROCESS	PROPOSED PROCESS
1	Setting Security Policy	No available process except that the security policy is available	<ul style="list-style-type: none"> • Operations review the policy and revise if necessary • Managing director approves the policy • IT creates an accessible location for employees
2	Managing Assets	<ul style="list-style-type: none"> • IT labels some hardware like PC 	<ul style="list-style-type: none"> • IT identifies the company's asset and assess the risk • IT creates a tracker for these assets • IT drafts a documented process for asset management
3	Managing Operations	<ul style="list-style-type: none"> • IT monitors the systems 24by7 • IT updates the software regularly • HR hires new staff, discusses the contract and lets new employee sign an NDA • Team leaders train new employees on the support without the inclusion of information security • Process owner documents processes but not on processes related to security but more on the support and daily operations 	<ul style="list-style-type: none"> • Operations post visuals on information security • Operations creates a training plan that include information security • Operations conduct a training that include information security • IT creates a repository for all processes • Creates guidelines for email, internet, and passwords as a reference for employees (<i>this was provided by the researcher</i>)
4	Establishing Access Controls	<ul style="list-style-type: none"> • Team leaders sends email to IT to request for access of internal systems • Team leader send request to client if access is needed for client's systems • IT process the request and email the information to the concerned employee and to the requestor 	<ul style="list-style-type: none"> • Create a form for access request (<i>this was provided by the researcher</i>) • Utilize the form for every access request • IT engages in training to discuss information related to security • IT verifies internet restrictions • IT deactivates external hard drives
5	Reporting Incidents	<ul style="list-style-type: none"> • Manager creates the report is requested • IT resolves the issue • Management team conducts meeting to discuss 	<ul style="list-style-type: none"> • Operations encourages employees to report all incidents • Operations creates a template for standard reporting • IT creates a repository for all incident reports for tracking and monitoring • Senior manager to assign owner to track, follow-up and close all incidents
6	Ensuring Business Continuity	No available process.	<ul style="list-style-type: none"> • IT to conduct a simulation • Senior manager drafts a process for business continuity management that includes escalation process
7	Conducting Security Audit	No available process.	<ul style="list-style-type: none"> • Senior manager assigns persons to conduct the audit • Operations creates audit checklist • Auditors (coming from operations and IT) reports all findings • Auditors solicit for corrective actions from concerned departments • HR engages in doing corrective actions for violations related to the company's code of conduct

There are several areas to fix as evident in the comparison between the current and proposed process as summarized in Table 7. But the proposed process is designed in such a way that the action items for the case company address each area. These are practical steps that can be fulfilled for the commencement of a structured process in information security management.

The following section discusses the feedback received from some of the case company's stakeholders regarding the draft of the proposal.

6 Validation of the Proposed Process

Following the stage of the proposal building for the initial draft of the information security management process is the finalization of the proposal based on the feedback that is solicited from the case company. This section discusses the process on how the proposal was validated based on the feedback provided by the stakeholders of the case company. These feedbacks are helpful either revising the initial proposal or considering it as a final proposal as the proposal which is the process along with its contents already fit the need of the case company and acceptable to the stakeholders.

6.1 Overview of the Validation Stage

The validation of the process was initially planned to be a discussion with the stakeholders who were interviewed during the CSA stage. The discussion flow should have been done in a way wherein the process will be discussed, along with the sub-processes under each element of the information security management process and the respective owners. After which, stakeholders will be encouraged to ask questions on items that are not clear to them or solicit for their feedback on the whole process and those individual deliverables. The purpose of the feedback solicitation is to validate if the entire process and its different components fit their current need, or if there are other items that they want to add, exclude, modify, or enhance the process.

But when the draft of the initial proposal was sent to the stakeholders, getting the feedback through a discussion is not possible as the case company is in the middle of their preparation for an IT migration. With the unavailability of the stakeholders to go through the proposal, their feedbacks were only sent through email.

6.2 Stakeholders' Opinions on the Prototype Process

It would have been ideal to get the feedback from all concerned stakeholders who were interviewed. But of the six respondents, only two validated the proposal, and these came from respondents MS-AS-OP-03 and EN-AS-OP-05.

The email as shown in Figure 31 shows a positive response, if not for the whole process, at least on some of those items that were provided by the researcher for the case company to use.

Hello Hidden

Sorry for the late reply. I needed some time to go through the file.

You have done a great job!!

I agree with your Summary of Current State of Analysis. It is very accurate.

Your proposed guidelines below came in a the right time.

INTERNET AND EMAIL GUIDELINES, PASSWORD GUIDELINES & ACCESS REQUEST – after the completion of migration to the high availability server (to happen on April 30), the next phase is to set restrictions on all these 3 areas. We will surely use your guidelines as reference, to ensure that all important items are covered.

All the best!!

Figure 31. Email feedback of MS-AS-OP-03 on the initial proposal

Respondent MS-AS-OP-03 has already confirmed the possibility of implementing some of the things that the researcher has proposed. As mentioned in the email, the guidelines that were provided will be used as a reference when the case company will set some necessary restrictions after the migration. There was no other feedback regarding changes that need to be made in the process.

Respondent EN-AS-OP-05 also thinks that the process is a simple but a comprehensive guide for small organizations like the case company. Moreover, the respondent believes that the management team will find the file relevant and consider what is most appropriate. Additional feedbacks are shown in the following texts.

- The communication plan should be considered as part of the process.
- The respondent also commented on the accountability and ownership that should be in the process.

In the end, the respondent thinks that implementing the process would require a certain amount of resources and time for the company to consider that at this point cannot be afforded.

6.3 Final Proposal

Based on the feedbacks that were sent by the two stakeholders of the case company, the implementation of the entire process as proposed is not feasible any time soon. And since

the feedback provided does not merit changes to be made on the proposal, the submitted process, as shown in in Figure 24, is considered to be the final process.

In response to the feedback of respondent EN-AS-OP-05, it was clarified through an email correspondence that the respective owners are indicated in the process on a per team basis, and it is up to the case company to decide the particular person who will own the identified deliverables to fulfil each element of the information security management process.

As for the other feedback on the inclusion of the communication plan, the researcher believes that this is included as part of the element of managing operations which will fall under the scope of the operations team. But this was not clarified to the respondent.

6.4 Recommendation / Next Steps

Information security plays an integral part in the overall operations of the business. Having a structured, reliable, and tight process to secure confidential information, entrusted by clients and customers, is vital in retaining customers' trust and having integrity as a business entity.

The implementation of the process is ideal but with the feedbacks that were received, the possibility of doing so is not evident anytime soon. The researcher understands the current situation of the case company and would like to recommend the following actions as a next step for the case company to consider instead.

- Start with the awareness campaign especially for agents. This can be started by utilizing some of the tools like the forms, guidelines, and posters that were provided by the researcher. These tools are free and ready for use. The guidelines and posters do not entail cost or additional manpower as they only need to be discussed which could be included as part of the coaching team leaders do with their agents. After which they can post in visible areas like the agents' workstations. As for the form, which is more on the access control request, this is only needed when there is a new employee and request is necessary to be made to IT. Having the form available will be more convenient for the team leaders and will only take a few minutes to complete as compared to sending their requests through email.

- Review the security policy. This is one document that a company must have. Since this is already available, the review, approval, and implementation of the document are the only missing items.
- Implement the inclusion of the training on information security on the next run of hiring. Training is already part of the process every time there are new hires. Spending an hour or less to discuss some pertinent information related to information security will be the beginning of the awareness campaign for employees. This does not entail extended training time but even if it does, the benefit of making the employee aware is worth more than the cost incurred for that extra hour of training.
- It is also advisable to revisit the proposal after the IT migration and verify those processes that have been done by the current IT team. Although it was not verified previously with the external IT, there is a big probability that the process on asset management, for instance, is part of their portfolio.

The above recommendations are practical. But the last item regarding revisiting the proposal would be helpful. The process could have been perceived by the stakeholders initially as complicated and difficult to implement, but if reviewed again especially by the managers, it could be viewed with a new perspective. Of course, if the input of the researcher is necessary, the latter can discuss this with the case company.

The following section concludes this Thesis.

7 Discussion and Conclusions

This section discusses the outcome and finalises this Thesis. Included are managerial implications and the evaluation of the entire process, as well as the assessment of the Thesis' validity and reliability. Moreover, this section also presents some of the limitations and challenges the researcher has encountered in the course of the study and the completion of this thesis.

7.1 Summary

The issues on information breaches and measures companies deploy to protect the business shaped the interest of the researcher on information security management. This is further fuelled by the researcher's experience and observation of the process of the case company. With those observations, come the idea of helping the case company put structure to its current process to properly manage and protect clients' and the clients' customers' information.

Thus, the objective to propose a practical internal information security management process for a case company. With the knowledge of the absence of the process, a conceptual framework was designed using valuable information from various literature, and those practices gathered from interviews with stakeholders of other companies. Elements of information security were identified which were used as the baseline in gathering evidence of the case company's current process and practices.

There were rounds of data collection that commence with the analysis of the case company's current state. This was done through series of interviews with the case company's stakeholders who are familiar with the process and given the authority to share confidential information. The interview was semi-structured where questions are focused on the current practice that surrounds the different elements of information security management. The results of all interviews and information from the literature were merged to draft the initial proposal.

The proposal, which is a process with assigned owners and actions items for the case company to perform, was sent to case company for validation, but a discussion is not possible as the case company was in the middle of preparation for an IT migration and all stakeholders are not available to discuss the process. Positive feedback was received from one of the stakeholders although overall, the result of the validation in the opinion of

the researcher lacks depth. As there are no changes that would prompt the researcher to make necessary modifications to the proposal, the initial draft that was submitted as shown in Figure 24 is considered as the final proposal on information security management process.

7.2 Practical/ Managerial Implications

The Thesis highlights the importance of information security management. The findings on the CSA stage clearly shows some areas where the company is lacking regarding taking measures to protect its clients' and clients' customers' information. Thus, having a structured process will be able to address these findings.

The process is also beneficial for potential clients who are particular about having structured and documented processes in place. Additionally, risks are present everywhere. People not properly using the system or not aware of the process poses a risk to the security. Systems that are not regularly monitored, maintained, and updated, or assets that are not tracked, labelled, and protected present risks on possible data loss. In other words, there are several situations that could constitute a threat to the business. The proposed process is a practical process designed for the case company to have that only entails a commencement. It does not even have to be done at once.

Unfortunately, despite the risks brought about by the absence of the process, the unawareness of employees on information security, the need for audit to verify and correct nonconforming practices, among other things, the head of the company himself admitted and confirmed that implementing such process entails cost, thus, the company would bear the risks of security breach. The case company has recognized the huge price to pay when such event will happen. Nevertheless, having this process in place is not a priority at the moment.

7.3 Evaluation of the Thesis

The journey in completing the Thesis proved to be strenuous but at the same time fulfilling. There is a vast source of information that covers the topic on information security so the whole process is a learning experience and a number of key take-away was recognised.

Overall, the objective was achieved based on the outcome of the thesis which is a process for the case company to implement. The case company's stakeholders provided honest feedback on their weaknesses/gaps. Although at the beginning it was observed that the respondents were trying to be very vigilant with their responses but in the end, after it was explained that the intention of the researcher is to help the case company, the information flowed freely without hesitations.

The interview with the stakeholders of other companies are insightful, and the information that the respondents shared were valuable in understanding the process and building the proposal. Although the proposal was not reviewed and validated as it should be and the process was not accepted for implementation, the feedback from a key informant that some of the tools like email, internet, and password guidelines that were provided by the researcher will be implemented after their IT migration, is a good start.

Completing the Thesis is not a walk in the park. It is worth pointing out some of the challenges that were experienced by the researcher, and the following sub-section discusses some of these limitations.

7.3.1 Limitations of the Thesis

Working on the Thesis has presented some limitations. With the limited knowledge presented by the stakeholders on information related to information security management, inputs during the building of the proposal were limited. As a result, the proposal was drafted by the researcher with ideas coming mostly from literature and information from other companies with the intention to address the weaknesses and gaps on the CSA stage for each element of the information security management process.

Due to distance and the difference in the time zone, as well as the current status of the company when it comes to its turnover rate especially on its IT, the stakeholders are always not available for discussion. Responses to requests are at times delayed, and input from the IT side is insufficient, as well as verification and review of the process and documents are not possible. As pointed out in the previous sections, there was also insufficient validation from all stakeholders involved in the case company. Thus, the validation was not as profound the researcher wants it to be.

With the limited time allotted to complete the Thesis, the researcher believes that initiating a pilot test and validating the proposed process with stakeholders of other companies could have been useful.

Despite all of these limitations, the outcome of the Thesis is achieved, and several things were learned along the way.

7.3.2 Outcome vs. Objective

The objective of the thesis as discussed in Section 1.4 was to propose a practical internal information security management process for a case company that offers outsourcing services.

The outcome of this thesis is a practical process of information security management that was provided for the case company. The process as shown in Figure 24 consists of practical steps that the researcher believes to be feasible for implementation should the case company wish to do so.

In conclusion, the objective of the Thesis was fulfilled based and outcome. A process was drafted with respective owners who are responsible for each of the deliverables and provided to the case company. This process will enable the latter to put a structure in the way they manage clients' and customers' information.

7.3.3 Reliability and Validity

The assessments on the reliability and validity of the Thesis were discussed in Section 2.4.

Validity is assessed and achieved based on the honest responses provided by the stakeholders to questions that are focused on the different elements of information security management that were asked during semi-structured interviews. The respondents were those individuals who are most familiar with the process and the responses to the questions shed light on the absence of a security process which supports the business challenge. The questionnaire was sent to the stakeholders and the result of current state analysis was also provided. The stakeholders had verified and agreed on the findings. It

would have been helpful if these external companies were able to validate the process after it has been finalised.

Aside from the internal validity that was done with the stakeholders of the case company, the wide range of sources from various literature as well as the best practices gathered from other companies are proven to be useful in the assessment of the external validity of the proposed process and those elements that were covered within the process.

Reliability is assessed through the interviews with stakeholders from operations, IT, and the management. The interviews were done in separate occasions and with different informants from team leaders, operations executive, managers, and director. Standard questions were asked and responses to the questionnaires were recorded and transcribed. The responses of the informants are consistent when it comes to the current state of the business and the absence of the process on information security management.

To further verify the reliability of the responses, some documents were reviewed. As there are limited documents available, reliability cannot be cross verified with any documented process as there was none. The only document that is relevant for verification is the security policy. Unfortunately, only the IT Manager is aware of the existence of the document. It is known to the rest of the respondents, but even the IT is not following the content of the said document. Moreover, the document was not also approved by the assigned approver, so its content is not reliable if compared with the current practices of the case company.

Furthermore, at the time of the interview, one of the respondents who is the IT manager was in the process of transitioning his duties to an outsourced IT that was commissioned by the case company. With this, some of the information related to IT processes and practices as provided by the respondent may not hold true as the new IT team has already taken almost all of the responsibilities and as shared by other respondents made some improvements to the current process.

This transition of the internal IT processes to an outsourced IT is one factor that could affect reliability of the Thesis.

7.4 Closing Words

Integrity and trust are paramount in any business. This is more so if a confidential and proprietary information is shared with the company that provides services to clients and the clients' customers. The expectation is set that this information, which connects to the identity of the individual, is safeguarded.

The issue concerning information breach keeps anyone anxious. Thus, it is only right that every company has to consider information security management as part of their daily operations. Safeguarding the information entails processes and structures. Moreover, it necessitates knowledge on the end of the company and all of its employees who provide the service and support these clients and customers. Keeping employees informed of the risks brought about by these breaches, and their responsibilities to avoid these risks could help the company save money and grow the business.

To build that structure, this Thesis sheds light on some of the elements every company needs to have in place to start the process in information security management. For the case company, its implementation, though challenging at the beginning as several areas are found to be lacking, would, in the long run, help to add value to the service. With the comprehension of the process and the support of the management, this structure will aid the company in providing a more effective and efficient service.

8 REFERENCES

Aberdeen, T. (2013). REVIEW ESSAY on Yin, R. K. (2009). Case study research: Design and methods (4th Ed.). Available at: <http://journals.nipissingu.ca/index.php/cjar/article/view/73/49>. [Accessed: 25 February 2016].

Axelrod, W. (2004). *Outsourcing Information Security*. Massachusetts: Artech House, Inc.

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. Available at: <http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf>. [Accessed: 26 February 2016].

Bayuk, J. L. (1996). Security Through Process Management. Available at: <http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper015/bayuk.pdf>. [Accessed: 22 April 2016].

BBC. (2015). AT&T pays record \$25m fine over customer data thefts. Available at: <http://www.bbc.com/news/technology-32232604>. [Accessed: 16 February 2016].

Beaver, K. (2005, April). Six essential security policies for outsourcing. Available at: <http://searchsecurity.techtarget.com/tip/Six-essential-security-policies-for-outsourcing>. [Accessed 11 March 2016].

Bidgoli, H. (2006). *Handbook of Information Security. Threats, Vulnerabilities, Prevention, Detection, and Management Volume 3*. California: John Wiley & Sons, Inc.

Blaxter, L., Hughes, C., & Tight, M. (2006). *How to Research, 3rd Edition*. England: Open University Press.

Brink, H. (1993). Validity and Reliability in Qualitative Research. Available at: <http://www.curationis.org.za/index.php/curationis/article/download/1396/1350>. [Accessed: 10 February 2016].

Brophy, M. (2012). ISO 27001 Information Security Incident Management. Available at: <https://www.youtube.com/watch?v=BcP3c-Vd7n0>. [Accessed: 20 March 2016].

Brophy, M., Loughran, S., & Geary, J. (n.d.). ISO 27001 Communications And Operations. Available at: <https://www.youtube.com/watch?v=J0A20nwEWrQ>. [Accessed: 20 April 2016].

Carlson, T. (2001). Information Security Management: Understanding ISO 17799. Available at: http://www.gta.ufrj.br/ensino/cpe728/03_ins_info_security_iso_17799_1101.pdf. [Accessed: 01 March 2016].

Carmines, E. G., & Zeller, R. A. (1979). Reliability and Validity Assessment. SAGE University Papers. Available at: http://www.uky.edu/~clthyn2/PS671/carmines_zeller_671.pdf. [Accessed: 19 February 2016].

Carter, M., & Hinson, G. (2010). ISMS implementation and certification process overview. Available at: <http://www.iso27001security.com/html/toolkit.html>. [Accessed: 10 March 2016].

Cobb, M. (2011). Internal security audit: The importance of security system assessment. Available at: <http://www.computerweekly.com/tip/Internal-security-audit-The-importance-of-security-system-assessment>. [Accessed: 10 March 2016].

Ernst & Young. (2011). Data Loss Prevention. Keeping your sensitive data out of the public domain. Available at: [http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/\\$FILE/EY_Data_Loss_Prevention.pdf](http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf). [Accessed: 17 March 2016].

FFIEC. (n.d.). IT Examination Handbook InfoBase. Risk Assessment. Available at: <http://ithandbook.ffiec.gov/it-booklets/operations/risk-assessment.aspx>. [Accessed: 21 April 2016].

Finnish Standards Association. (2010). *SFS-ISO/IEC 27000, Information Technology -- Security Techniques -- Information Security Management Systems -- Overview and vocabulary*. Helsinki: Finnish Standards Association.

Gibbs, G. R. (2012). Reliability, validity, generalizability and credibility. Pt .1 of 3: Research Quality. Available at: <https://www.youtube.com/watch?v=4NQHl8GD54>. [Accessed: 10 February 2016].

Holtzhausen, S. (2001). Triangulation as a powerful tool to strengthen the qualitative research design: The Resource-based Learning Career Preparation Programme (RBLCPP) as a case study. Available at: <http://www.leeds.ac.uk/educol/documents/00001759.htm>. [Accessed: 19 February 2016].

Honour, D. (2006). Defining Business Continuity. Available at: <http://www.continuitycentral.com/feature0398.htm>. [Accessed: 21 April 2014].

Information Commissioner's Office (ico.). (2016). Data security incident trends. Available at: <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>. [Accessed: 28 February 2016].

INFOSEC Institute. (2012). Access Control: Models and Methods. Available at: <http://resources.infosecinstitute.com/access-control-models-and-methods/>. [Accessed: 27 March 2016].

ISO. (2013). ISO/IEC 27001 - Information security management. Available at: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>. [Accessed: 15 April 2016].

IT Compliance Institute. (2006). Information Security. Practical guidance on how to prepare for successful audits. Available at: http://download.101com.com/pub/itci/Files/ITCi_ITACL-InfoSec_0612_finalweb.pdf. [Accessed: 22 March 2016].

KPMG International. (2006). Asian Outsourcing: The Next Wave. Available at: <http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/asian-outsourcing-O-0611.pdf>. [Accessed: 10 March 2016].

Krantz, D. (2015). Communication Strategies: 5 Ways to Effectively Communicate With Employees. [Online]. Available at: <http://www.entrepreneur.com/article/248757>. [Accessed: 22 March 2016].

Lomphey, G. R. (2008). Critical Elements of an Information Security Management Strategy. Available at: <https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/7613/2008-lomphey.pdf?sequence=1>. [Accessed: 20 April 2016].

Myers, C. (2015). Asset Management. Available at: <https://spaces.internet2.edu/display/2014infosecurityguide/Asset+Management>. [Accessed: 21 April 2016].

National Institute of Standards and Technology. (2011). Information Security. Available at: <http://www.slideshare.net/dgsweigert/nist-sp-800137>. [Accessed: 27 March 2016].

Ponemon Institute. (2013). 2013 Cost of Data Breach Study: Global Analysis. Available at: [http://www.ponemon.org/local/upload/file/2013%20Report%20 GLOBAL% 20CODB %20FINAL%205-2.pdf](http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf). [Accessed: 20 April 2016].

Prunty, M., Pritchard, A., & Heffernan, R. (2006). The Customer Focused Contact Center. A Companion Paper to IBM's Advocacy in the Customer Focused Enterprise Paper. Available at: <http://www-935.ibm.com/services/us/gbs/bus/pdf/the-customer-focused-contact-center.pdf>. [Accessed: 10 March 2016].

Puhakainen, P., & Siponen, M. (2010, December). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 757-778.

Rana, M. (2011). Types of Access Control Mechanisms. Available at: http://www.techmahindra.com/sites/blogs/types_of_access_control_mechanisms.aspx. [Accessed: 05 May 2016].

Ritchie, J., & Lewis, J. (2003). Qualitative Research Practice. A Guide for Social Science Students and Researchers. Available at: https://mthoyibi.files.wordpress.com/2011/10/qualitative-research-practice_a-guide-for-social-science-students-and-researchers_jane-ritchie-and-jane-lewis-eds_20031.pdf. [Accessed: 29 February 2016].

Rouse, M. (2014). Access Control. Available at: <http://searchsecurity.techtarget.com/definition/access-control>. Accessed: 29 March 2016].

Schramm, W. (1971). Notes on Case Studies of Instructional Media. Available at: <http://files.eric.ed.gov/fulltext/ED092145.pdf>. [Accessed: 26 February 2016].

Schultz, E. (2011). Continuous Monitoring: What It Is, Why It Is Needed, and How to Use It. Available at: <https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030>. [Accessed: 28 March 2016].

Secure Data Management. (2014). 3 Advantages of a Centralised Filing System. Available at: <http://www.securedatamgt.com/blog/centralised-filing-system-advantages/>. [Accessed: 21 April 2016].

Stahl, S., & Pease, K. A. (2011). Seven Requirements for Successfully Implementing Information Security Policies and Standards. Available at: <https://citadel-information.com/wp-content/uploads/2010/12/seven-requirements-for-successfully-implementing-information-security-policies-2012.pdf>. [Accessed: 05 February 2016].

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22 (4), 441-469.

Theriault, M. (2013). 7 Simple Tips For Documenting Your Important Business Procedures. Available at: Forbes: <http://www.forbes.com/sites/allbusiness/2013/09/17/7-simple-tips-for-documenting-your-important-business-procedures/#bf3a32c470ce>. [Accessed: 22 April 2014].

Tipton, H. F., & Krause, M. (2007). Information Security Management Handbook, Sixth Edition. Available at: <https://books.google.fi/books?id=KV3vBQAAQBAJ&pg=PA834&lpg=PA834&dq=process+on+advocating+awareness+on+information+security&source#v=onepage&q=authentication&f=false>. [Accessed: 12 February 2016].

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., et al. (2007). *Foundations of ITIL V3*. Zaltbommel: Van Haren Publishing.

Violino, B. (2012). The in-depth guide to data destruction. Available at: <http://www.csoon-line.com/article/2130822/it-audit/the-in-depth-guide-to-data-destruction.html>. [Accessed: 28 March 2016].

Weal, R. (2014). Importance of Good Employee Communication. Available at: <https://www.linkedin.com/pulse/20140313231422-50813842-importance-of-good-employee-communication>. [Accessed: 25 March 2016].

World Economic Forum. (2015). The Global Risks Report 2015 10th Edition. Available at: <http://www.weforum.org/reports/global-risks-report-2015>. [Accessed: 26 February 2016].

Wurzler, J. (2013). Information Risks & Risk Management. Available at: <https://www.sans.org/reading-room/whitepapers/bestprac/information-risks-risk-management-34210>. [Accessed: 21 April 2016].

Yin, R. (2014). *Case Study Research: Design and Methods - 5th Edition*. California: SAGE Publications.

Yin, R. K. (2004). Case Study Methods. Available at: <http://www.cosmoscorp.com/Docs/AERAdraft.pdf>. [Accessed: 26 February 2016].

Yin, R. K. (2009). Case Study Research. Design and Methods, 4th Edition. Available at: http://www.hampp-ejournals.de/hampp-verlag-services/get?file=/frei/ZfP_1_2012_93. [Accessed: 10 February 2016].

Questionnaire used in CSA Stage

This questionnaire is used to understand the current state of the case company. The set of questions are in accordance to some of the elements of information security management process.

NO.	TOPIC(s) OF THE INTERVIEW	QUESTIONS
1	Involvement of the interviewee and experience in relation to the topic	What do you do to protect your customer's information?
		What is your involvement in the information security management process of the company?
		What is the important decision Operations has to make regarding security management?
2	Strengths / Weaknesses	What are the current strengths of Operations in security management?
		What are the common issues Operations' team encounters in security management?
		What are some of the areas that were challenging/weak?
3	Access Rights	How do you provide or request permission or access rights to employees? Do you follow any hierarchy?
		What is the process related to security management in cases of resignation/ termination employees?
4	Audit	Does Operations perform any audit related to information security? What is the frequency of this audit?
		Do you have available reports?
		How are findings reported to the management?
		How are negative findings addressed?
		What is the timeline set to close the findings?
		Do you do follow-up audit? When?
5	Training	How are employees educated regarding information security?
		Are there documents employees have to sign? (<i>Indicate the name</i>)
6	Confidential Data	What are some of the customer's information employees have access on?
		How are important documents disposed?
7	Hardware / Applications	Are USB drives accessible to employees? If no, are there exceptions?
		If yes, how does Operations ensure that the information that is copied is authorized and not brought outside?
		What are some of the limitations on access employees have, if any (e.g. email, websites, etc.)?
8	Business Continuity Plan	How do you ensure business continuity in the event of system failure?
		Do you have any contingency plan?
9	Best practice / Initiatives	What are some of the best practices Operations have regarding security management?
		What are the current initiatives or strategies Operations has to address issues on information security management?
		In your opinion, what could be done better to avoid or mitigate issues in future endeavors related to data breach or communication?

Questionnaire used during the gathering of best practices with stakeholders from other companies

This questionnaire is used to gather best practices from other companies. The set of questions are in accordance to some of the elements of information security management process.

NO.	TOPIC(S) OF THE INTERVIEW	QUESTIONS
1	Involvement of the interviewee and experience in relation information security	What do you do to protect your customer's information?
		What is your involvement in the information security management process of the company?
		What is the important decision IT has to make regarding security management?
2	Access Rights	How do you provide permission or access rights to employees? Do you follow any hierarchy?
		Does this need to be requested or IT has to initiate the process?
3	Operations Management	Do you have list of systems to be maintained?
		How often does IT conduct system maintenance?
		Is there any specific time when you do the maintenance?
4	Asset Management	How do you dispose of information of old clients, or those of ex-employees?
		Do you have any back-up systems?
		Are USB drives of the system accessible to employees?
		How does IT ensure that the information that is copied is authorized and not brought outside?
		What is your process in blocking unauthorized websites or programs or applications?
5	Incident Reporting	What is your process when you find the system is having an issue?
6	Business Continuity Plan	How do you ensure business continuity in the event of system failure?
		Do you have any contingency plan?
7	Security Audit	Do you conduct system audit? What are the areas covered by the audit?
		What is the frequency of this audit?
		Do you have available reports?
		How are findings reported to the management?
		How are negative findings addressed?
		What is the timeline set to close the findings?
		Do you do follow-up audit? When?
8	Best practice / Initiatives	What are some of the best practices IT have regarding security management?
		What are the current initiatives or strategies IT has to address issues on information security management?
		In your opinion, what could be done better to avoid or mitigate issues in future endeavours related to data breach or communication?

Overview of Important Incidents (*Data Loss Prevention, Ernst & Young 2011: 5*)

The table below summarizes a list of some affected agencies that experienced data loss and have incurred huge monetary losses and extreme media exposure.

AGENCY	DESCRIPTION OF THE INCIDENT
Web technology firm	On its official weblog, a web technology firm published a message that it had uncovered a ploy to collect user passwords, likely through phishing. This ploy affected the personal accounts of hundreds of users, including among others, senior US Government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists.
Public health corporation	A public health corporation had to notify 1.7 million patients, staff, contractors, vendors and others about a reported theft of electronic record files that contained their personal information, protected health information or personally identifiable employee medical information. The information included Social Security numbers, names, addresses and medical histories.
International oil and gas company	An international oil and gas company lost a laptop which contained personal information for 13,000 individuals including names, Social Security numbers and addresses. The laptop was not encrypted, and the information lost was for claimants against the company.
US public agency	Personal details for 3.5 million teachers and other employees of a US public agency were accidentally published on the Internet. Information released included names, Social Security numbers and birthdates. This data had been posted on the internet for more than a year without the organization realizing it.
National retail bank	Two thousand customer records from a national retail bank were stolen by employees prior to leaving and joining a competitor firm. Records included customer bank account numbers, Social Security numbers and other highly sensitive personal data such as tax returns and pay statements.
Online storage provider	According to a blog post, an online storage provider explained that due to an authentication bug, all accounts were at risk of a data breach. As soon as the bug was discovered, as a precaution all logged in sessions were disconnected. The bug was active for almost four hours and took five minutes to fix.

Training Questionnaire Sample for Email Usage (*Appendix 1 on Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, Puhakainen & Siponen 2010*)

These questions are used to understand the email usage of employees. At the same time to assess their awareness and understanding to possible threats on security brought about by improper use of email and everything that goes with it.

NO.	QUESTIONS
1	In your opinion, what are the most common ways malicious software (viruses etc.) gets into our company's network?
2	Where can you find our company's official information security instructions?
3	Have you applied the instructions concerning the company's e-mail use to your work? If yes, give some examples of what instructions and for what purposes they were used.
4	Did you find the instructions useful for your purposes? Were they easy to understand and use in practice? Why or why not?
5	Explain briefly the purpose of our company's information classification rules.
6	How have you applied the information classification rules in your work (i.e., in practice)?
7	How much time do you spend processing e-mail (company's e-mail account) on a weekly basis? (Your best estimate)
8	For what purposes do you use e-mail in your work?
9	What do you consider as acceptable use of our company's e-mail system?
10	Give examples of what you consider unacceptable use of our company's e-mail system?
11	Have you ever encountered malicious software in e-mail attachments? Did this happen at the company or somewhere else? Explain what happened.
12	Have you ever followed (clicked and opened a page) a specially crafted, malicious link in an e-mail message? Did this happen at the company or somewhere else? What happened?
13	How many spam messages do you receive at our company's e-mail account (e.g., on a weekly basis)? Also give an estimate of how many received messages (e.g., percentage) are spam. Have you ever tried to answer any of the spam messages?
14	In your opinion, by what means is it possible to distinguish relevant e-mail messages from spam or other possibly dangerous messages?
15	By what means would you ensure it is safe to open an e-mail attachment?
16	Are there any other security issues that you consider important for your work?

Sample Email Validation for Employees' Access

The screenshot below is a sample email from one of the international companies. This is being sent out by the corporate team to all concerned stakeholders of the local team on a quarterly basis. The purpose is to ensure that database of employees' user ids is updated and those who are not part of the company have been deactivated from the system. The concerned stakeholder has to respond on or before the given date. Else, user ids will be deactivated and might include those of active employees who could be part of the list.

The user revalidation process review is an important part of [REDACTED]. Evidence should exist to support that the review is effective in identifying and removing inappropriate access. It is critical that you be able to discuss the process you used to gain comfort that your employees access is appropriate. Last year, our external auditing firm found weaknesses in our managers general response as to why their employees had access. Some considerations as you perform this review are noted below.

Ensure those who have left the company, or left your department, have had their access appropriately removed. If they have not, mark them REVOKE.

For those who have left the company, you should also execute a TERMINATE transaction in Peoplesoft. Normally this should be done immediately when an employee leaves [REDACTED] or at the end of the assignment of a contingent worker.

For current employees, you should review and be able to speak to the functionality provided by all authorizations assigned to your employees. You must understand whether these access assignments are required by the employee to perform their current job responsibilities and be able to discuss with an auditor if requested. If you determine that an employee has access rights that are no longer required, those authorizations should be marked as REVOKE.

Follow the link below to review the user ID information, and submit the form to validate the business need for each application ID. For some applications, you may find additional information about the user ID by moving your cursor over a cell in the revalidation form. When you have taken all your decisions, scroll to the bottom of the list of users and click the "Make Changes" button at the bottom to save changes.

Any user IDs that are not confirmed by 11/07/2014 will be deactivated. Please do not reply to this e-mail. If you have questions, please address them to [REDACTED]

You may log-in to the revalidation website to proceed.

[https://www.\[REDACTED\]](https://www.[REDACTED])

For more information about Siebel Job Roles please click on the link below for a more complete description of the roles.

[https://docs.google.com/document/d/1IbkiHN2Jza2c\[REDACTED\]](https://docs.google.com/document/d/1IbkiHN2Jza2c[REDACTED])

[REDACTED] T Security Standard 670.1.10 mandates periodic revalidation of user accounts. For more details on the requirement, see IT Security Policies

New Hire IT Checklist

Screenshot of the tool as provided by one of the stakeholders during the gathering of best practices. This checklist is used for the request of log-ins to different systems for new hires.

New Hire IT Checklist
 Employee Transfer and Off-boarding IT Checklist

Request Number : 021816-231955

EMPLOYEE INFORMATION

Name	<input type="text"/>	Start Date	<input type="text"/>
Manager	<input type="text"/>	Location(Bldg/Floor/Area)	<input type="text"/>
Department/Code	<input type="text"/>		

Systems/Services	Comments (for Dept Manager)	Status (IT only)
<input type="checkbox"/> Desktop/Hardware <input type="checkbox"/> Business <input type="checkbox"/> CAD <input type="checkbox"/> MLS	Provide specific or additional instructions for this request.	
<input type="checkbox"/> Account <input type="checkbox"/> CDEV Account <input type="checkbox"/> LPDEV Account ⓘ		
<input type="checkbox"/> Telephone <input type="checkbox"/> New Phone ⓘ <input type="checkbox"/> Re-Use Phone ⓘ	Provide specific or additional instructions for this request.	

Submit Request

Employee Transfer and Off-boarding IT Checklist

Screenshot of the tool as provided by one of the stakeholders during the gathering of best practices. This checklist is used to request for deactivation of employee's access to different systems during transfer or termination of employment.

New Hire IT Checklist
 Employee Transfer and Off-boarding IT Checklist
 Request Number : 021816-231955

EMPLOYEE INFORMATION		
Name <input type="text"/>		Reason: <input type="checkbox"/> Voluntary Separation <input type="checkbox"/> Termination <input type="checkbox"/> Transfer of Job Role/Dept. <input type="text"/> only Effective Date <input type="text"/>
Manager <input type="text"/>	Location(Bldg/Floor/Area) <input type="text"/>	
Department/Code: <input type="text"/>		
Systems	Comments (for Dept Manager)	Status (IT only)
<input type="checkbox"/> Accounts (Removal/Disable) <input type="checkbox"/> CDEV Account <input type="checkbox"/> LPDEV Account	Provide list of all the accounts used to be disabled.	
<input type="checkbox"/> E-mail (Distribution list/Group Mail):	Provide list of all the mail group/s used for removal from the distribution list.	
<input type="checkbox"/> Data on shared drives (Remove access to the shared directory)	List all the shared drives and directories for disable and removal	
Telephone <input type="checkbox"/> Disable of assigned IDD & NDD PIN Code <input type="checkbox"/> Return of assigned Mobile Phone (Kindly engage to exec asst)	Please provide the numbers both extension and mobile.	
<input type="button" value="Submit Request"/>		

Information Security Responsibilities (*Information Security. Practical guidance on how to prepare for successful audits, IT Compliance Institute 2006: 6*)

These are some of the roles of each stakeholder in ensuring that information is secured, security measures are in place, issues are addressed, and that the company always aims for continuous improvements.



Security audit checklist sample on areas of awareness and training, and maintenance (*Information Security. Practical guidance on how to prepare for successful audits, IT Compliance Institute 2006: 17, 20*)

Auditing in general covers management, operational, and technical controls. Auditors may review the controls within this section and potentially others depending on the audit's purpose and focus.

Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Number	Description
<input type="checkbox"/> AT-1	Security Awareness and Training Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
<input type="checkbox"/> AT-2	Security Awareness: The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and [organization-defined frequency, at least annually] thereafter.
<input type="checkbox"/> AT-3	Security Training: The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and [organization-defined frequency] thereafter.
<input type="checkbox"/> AT-4	Security Training Records: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Number	Description
<input type="checkbox"/> MA-1	System Maintenance Policy and Procedures: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
<input type="checkbox"/> MA-2	Periodic Maintenance: The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
<input type="checkbox"/> MA-3	Maintenance Tools: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.
<input type="checkbox"/> MA-4	Remote Maintenance: The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
<input type="checkbox"/> MA-5	Maintenance Personnel: The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.
<input type="checkbox"/> MA-6	Timely Maintenance: The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.

Security audit checklist sample on the area of access controls (*Information Security. Practical guidance on how to prepare for successful audits, IT Compliance Institute 2006: 25*)

The following items included in this checklist is a helpful tool that can be used as basis for audit in checking for controls on access provided to employees.

Access Control (AC)

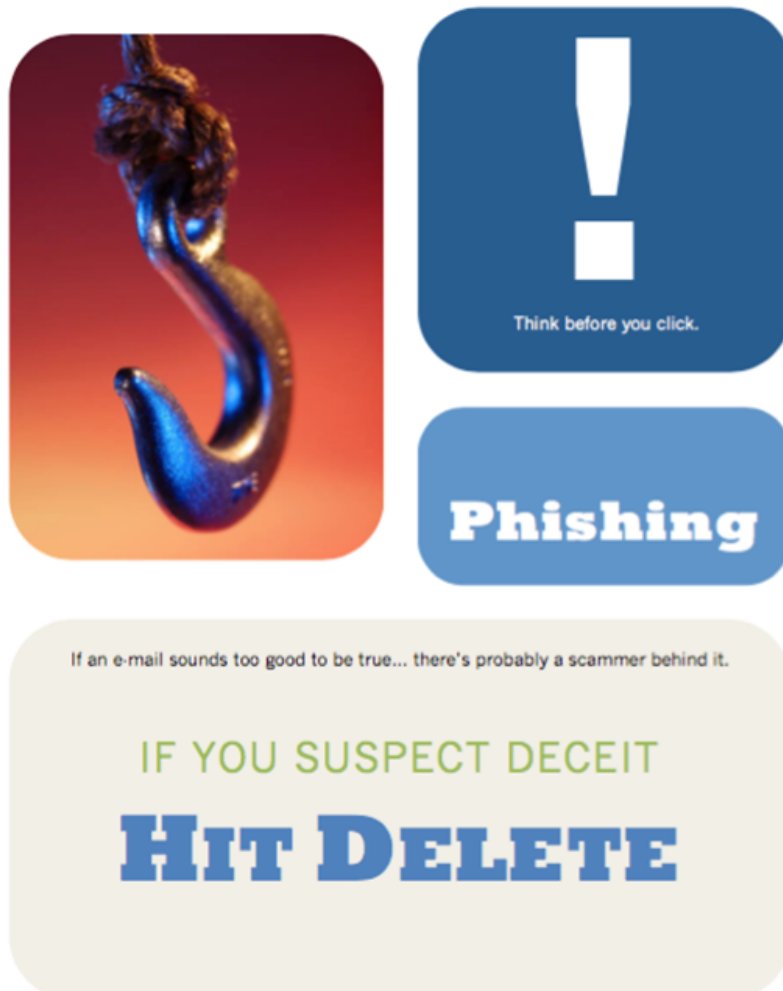
Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Number Description

- | Number | Description |
|-------------------------------|---|
| <input type="checkbox"/> AC-1 | Access Control Policy and Procedures: The organization develops, disseminates, and periodically reviews/ updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. |
| <input type="checkbox"/> AC-2 | Account Management: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts. |
| <input type="checkbox"/> AC-3 | Access Enforcement: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. |
| <input type="checkbox"/> AC-4 | Information Flow Enforcement: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. |
| <input type="checkbox"/> AC-5 | Separation of Duties: The information system enforces separation of duties through assigned access authorizations. |
| <input type="checkbox"/> AC-6 | Least Privilege: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. |
| <input type="checkbox"/> AC-7 | Unsuccessful Login Attempts—Control: The information system enforces a limit of [organization-defined number] consecutive invalid access attempts by a user during a [organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [organization-defined time period], delays next login prompt according to [organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded. |
| <input type="checkbox"/> AC-8 | System Use Notification: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes |

Poster for Awareness Campaign

This sample poster was made for the case company to utilize and post in strategic places to serve as a reminder for employees to be cautious when using their emails.



Summary of the Initial Proposal (*first draft*)

Based on the interview result and the feedback from some of the interviewees, as well as the summary of weaknesses that was gathered, the content of the proposal was drafted.

