KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES

Formulating Secure Information Communication Guidelines

A Case of Orange Gate Private Limited Company (OGPLC)

Ibrahim, Abduletife Abdulwhab

Bachelor's Thesis of the Degree Programme in Business Information Technology

Bachelor of Business Administration

TORNIO 2012

ABSTRACT

Ibrahim, Abduletife Abdulwhab 2012. Formulating Secure Information Communication Guidelines A Case of Orange Gate Private Limited Company. Bachelor's Thesis. Kemi-Tornio University of Applied Sciences. Business and Culture. Pages 54. Appendices 2.

The case company in this Thesis work is OGPLC. The general aim of this Thesis was to discover the weakness in information security and make them visible to the company. To meet these targets problems were sorted out and investigated. The process of investigation primarily starts by exposing the research question in detail. Secondly narrow down the research questions into one. Lastly, recommendations are proposed directly related to the research questions chosen for investigation and technologies that have indirect influence.

The objective is to present significant recommendations. These recommendations include recommendations directly relate to the research questions, recommendation for applying existing technologies and recommendation of procedures in the form of guidelines. Therefore, exploratory research method was considered and utilized. The methodology is considered suitable for this work because it facilitates the process uncovering the incident. Moreover, it enables to find out what happened and look at it from different point of view.

The outcome of this thesis work can be used by organizations that use computer based information sharing systems. The output contains recommendation to solve the problem and recommendation to stay safe and run the business efficiently.

Keywords: information security, information disclosure, information system, communication guidelines.

CONTENTS

ABSTRACT

FIGURES

PICTURES

TABLES

FIGURES

PICTURE

TABLES

1 INTRODUCTION

Information is among the mandatory asset of any business whether the business is operating in computer based information system or in a manual system the fact remains the same. The disclosure of information to those who does not authorize to use or make a change on the state of information is more than an unfavorable condition, and it is extremely costly. Information disclosure is among the serious attacks that can happen against the company. The result of it can be loss of loyal customers and end of the long lasting relationship, loss of business opportunities, and downgrade of company image in the competition at the market.

Information Security means protecting information from unauthorized access, use, disclosure, modification, or destruction of information. "Information security means the quality of being secure - to be free from danger". (Whitman & Mattord 2005, 8.) Information security is "The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. See also communications security; computer security; information security; information system" (Sharp 2006, 9).

The case company has confidential information. Some are procedural such as the complete requirement of their business procedure. The others are a record of information for instance a list of customers' information. Some of the information has significant value in the company for instance their business strategies others are less valuable. In general, for many reason the company needs to safeguard their information.

From the definitions suggested by established authors in Information Security, information security can be understood as involving action which is taken for the safeguarding of information assets against indiscreet uses. This taken into account, but is not restricted to this only, security of information can further be understood as involving measures taken against wrong release of information intentionally or unintentionally, accessing information without the authorization of the information

owner and dishonest or wrong use of information by persons who have legitimate access to organizational information resources.

1.1 Motivation

My Thesis work deals with confidential facts about information security and information security strategies. Therefore, the secrecy of the company was highly required. For the secrecy purpose, the company name has been given a pseudonym name called Orange Gate Private Limited Company (henceforth OGPLC). OGPLC wanted to examine and increase their understanding of their information security practice than it was before. OGPLC demands to be provided with a sound recommendation of existing technology that increases security for their company or recommendation for improving their technology utilization. Recommendations are related to their current problem in information security field. Moreover, the case company needs to be handed with information communication guidelines for the purpose of acquiring secure business transaction and information flow.

The motivation to conduct this research primarily comes from my genuine interest in the area of information security. In addition, the intention inside it is the potential to offer something on information security. Secondly, the information disclosure that has happened to OGPLC gives me an opportunity to work on formulating secure information communication guidelines. Based on the previous experience and professional skill, I acquired during my study time.

Information security is applied when information are created, sent out, received, stored and communicated electronically to share information with others by the medium of networks and computer devices. (McCumber 2008, 99-106.) Security is hard to trace security threats, and information security is the hardest sub-part of security to trace. “Security is about protection of asset” (Gollmannn 2006, 18). Information security is not limited or specified in a certain way. Therefore, Information security is hard to obtain before breaking it into different sub parts such as, administrative, personal, and office. Information security is not something that we can see as compared to other sub parts of the security. (Iivari 2008, 98-110.)

Miettinen (1999, 44-47) emphasizes that information security to be a burden of management. The whole staff must be engaged to the implementation of company's information security program and practice to share the burden and increase efficiency. (Miettinen 1999, 44-47 cited in Iivari 2008. 98-110.)

This Thesis work focus on formulating secure information communication guidelines to secure confidential business information. It includes answers to the research question posed and recommendations to improve the security practice in the company and create awareness. However, it does not include creating policy by which the company must have to follow. Instead, it offers recommendation and guidelines to secure confidential business information. Confidential business information has some valuable that the information is kept in secret. Colantoni (2009, 11) listed out the list of confidential business information as follows, confidential customer database, contact list, prospect list, mailing list, list of supplier, product development, acquisition plan, cost and profit margin information, and business strategies. These lists expedite the identification of which information are considered as confidential. The identification of information considered confidential information is essential to give suitable recommendations.

Confidential information is essential information kept confidential. Confidential information could also take a form of intellectual property. In general confidential information is information which is a means of gaining profit for the company (Colantoni 2009, 8). Colantoni (2009, 9) urges that companies' information must pass tests to be a trade secret (1) Value the information need to possess actual or potential monetary value. (2) Protection the information should be protected and necessary prevention method has to be applied to keep the secrecy of information. (3) Unavailable the information does not have to be open or available for others who do not entitle to access it.

1.2 Objectives of the Thesis

The objective of my Thesis work is to bring a sound and applicable recommendation to enhance OGPLC's Information Security. Moreover, to determine the factors that will enable OGPLC to function safely.

1. To determine the factors for information disclosure outside the company premises.

2. To identify action or procedure need to be followed to secure information in the company premises and while communicating with other company for doing business.

3. To establish smooth flow means with less interruptions of information in a relatively secure manner compared to the situation that case company is in right now.

Securing confidential business information of OGPLC requires analyzing the connection between the characteristics of computer system with the Confidentiality Integrity Availability (henceforth CIA) of information. Confidentiality keeps authorized restriction on information access and disclosure. Integrity protects information from modification from an individual who do not have a legitimate right to make changes in confidential information. Availability ensures timely and reliable access and use of information to certain individual authorized to process the information further. The Objective is to ensure the protection of information by providing a recommendation and indicate the right security measures to keep the CIA reliable and contribute safe business operations to OGPLC. (Vaidyanathan & Mautone 2009.)

Figure 1 illustrates a corporate defense cycle. The process involves anticipating a threat or vulnerability, taking measures against the anticipated threat and vulnerability, detecting a breach in the corporate defense, and taking a reaction to mitigating the detected threat and vulnerability. Moreover, the corporate defense cycle shows how to tackle information security breach and it helps to make security modification and improvement to an organization. The cycle is endless which needs to be recognized and fully understood to strengthen security. (Lyons 2008.)

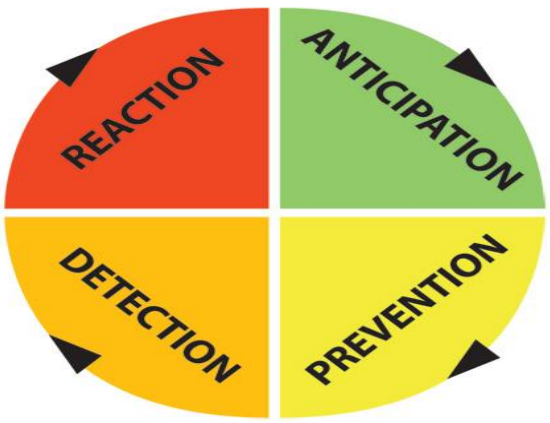

Figure 1. Corporate Defense Cycle (Lyons 2008)

1.3 Methodology

The objective of this Thesis work is to provide recommendation to OGPLC and in the process to learn from the research process and acquire a better understanding of the phenomena under OGPLC is my personal goal. Therefore, the objective of this thesis work and my goal can be fulfilled by applying the appropriate method which is more suitable to this thesis work was extremely beneficial to collect data and present the data as well as to make a better analysis of the data collected.

According to Silverman (2005, 112) it is difficult to say a methodology itself is wrong. However, Silverman (2005) urges the researcher has to make informed choice of the methodology. The selection of methodology in this thesis was on the basis of suitability for the research question and title. As Silverman (2005, 112) points out methodology itself cannot be wrong. However, it can be less appropriate to the research work depending on the research question proposed by the researcher for the purpose of the study.

Case Study research strategy is utilized in this thesis work. Yin (1994, 13) Case Study is based on practical question that investigates a current incident inside its tangible context, in particular when the restrictions between the incident and circumstance are noticeably evident. (Yin 1994, 13 cited in Woodside 2010, 2). Woodside (2010, 2) questions Yin's (1994) suggestions by emphasizing that case study research is not restricted to a current incident or its tangible contexts, especially when the restrictions between circumstance and context are not noticeably evident. Therefore, Woodside (2010) defines case study research as a particularly crucial strategy specially, if the output of the research needs to be presented in describing understanding of the case.

My case study thesis work followed the exploratory approach to investigate the information security method applied in OGPLC. The exploratory research approaches utilized because the main research questions proposed deal with "what" and "how" the case happened (Yin 2003, 9 original emphases). Therefore, Yin (2003, 9) suggests that exploratory approach is suitable when the nature of the research question is "what" happen and "how" something happened. Moreover, the objective is to give a significant recommendation which directly relates to the research questions and proposition for further improvement. Exploratory research is a valuable means of finding out what is happening and assessing phenomena through different means (Robson 2002).

Throughout the data collection for this thesis work, structured observation was utilized because structured observation provides a complete list of expected behavior. Observation requires the observer to check what occurred (Sunders & Lewis & Thornill 2007, 284-93). The result from the structured observation indicated clearly in the results table. In other words, the results indicate what is applicable and what is not applicable as well as what was utilized properly and what need improvement based on the observation check list. The data collected from the interviewee, observation and books analyzed at the analysis phase. One information source for data collection was an interview with the OGPLC Information Security Officer and Server Administer. Structured observation was made by a delegated person from the company. Secondary source was used to have a comprehensive understanding of the subject and make objective analysis of the case. The interview, observation and secondary sources have contributed to meet my research objective.

1.3.1 Research Topic and Questions

The title of my thesis work is formulating secure information communication guidelines A case of OGPLC private limited company. This thesis work will investigate the causes of information disclosure, with the objectives of finding suitable solutions and offers recommendations to enhance the security practice and create awareness. Moreover, existing technologies that can contribute for the security of the case company assessed and recommend for the case company. The case company is currently losing market share due to information disclosure outside the company premises. They would like to conduct this research to be recommended to improve the organization information security and the process of information flow.

The objective of my thesis work is to determine the factors that enable the company to promote and ensure secure information flow. Moreover, to recommend the options available to secure information sharing process. Therefore, the research questions focus on the process of information security flow and strategy implementation of the information security. Moreover, I will examine the infrastructural preparedness and usage of technology in OGPLC. The research questions are listed below as follows:

Q1.what does OGPLC need to do to protect the confidential information?

To answer this question, the factors that affect information security from information security basic point of view in relation to OGPLC were investigated. Calder (2005, 34-36) has listed out the basic information security points of view as follows: having a policy, insist on accountability and responsibility, identify asset ownership and classification, physical security of information systems, have up-to-date anti-malware software, implement and enforce user access controls, implement and enforce system access controls, manage vulnerabilities, have an incident response process, business continuity and disaster recovery plans, Monitor compliance, Users training and awareness of their responsibilities. These were used to investigate the utilizations of these basics of information securities by the case company.

2. How does employees (insider) behavior leads to information disclosure?

To answer this question, insider behavior and the motive of attack were investigated. In addition, the approaches the insiders follow to cause attack were investigated. Suitable investigation method recommended which enhance the investigation process. Moreover, information security guidelines procedure recommended, that enables the case company to be aware about the security measures. The procedure explains what need to be done before starting job, in the middle of job, after completion of job.

3. What are the essential components that are affecting the information security flow in OGPLC PLC?

To answer this question, existing literature about components of information security and information system were explored. The research supported by the response gathered from the interview and structured observation about the use of Information system components. Existing technology which are not utilized by the case company are recommended.

1.3.2 Research Steps

Figure 2 illustrates the six steps of the research I took. Each step requires comprehensive understanding of research techniques. The first step was taken to acquire knowledge before approaching the research. Therefore, the second step shaped the case based on the background information obtained from the first step. The third step was conducted by investigating the research questions. The investigation step from the third

step supported by the evidences collected on forth step. The evidences collected were compared with the results obtained to form the analysis on the fifth step. Finally, based on the result obtained from the investigation, the evidences and analysis during the last step propose recommendations for enhancement. The 3-D block diagram outline was used to demonstrate the sequence of research steps taken to conduct this thesis work.

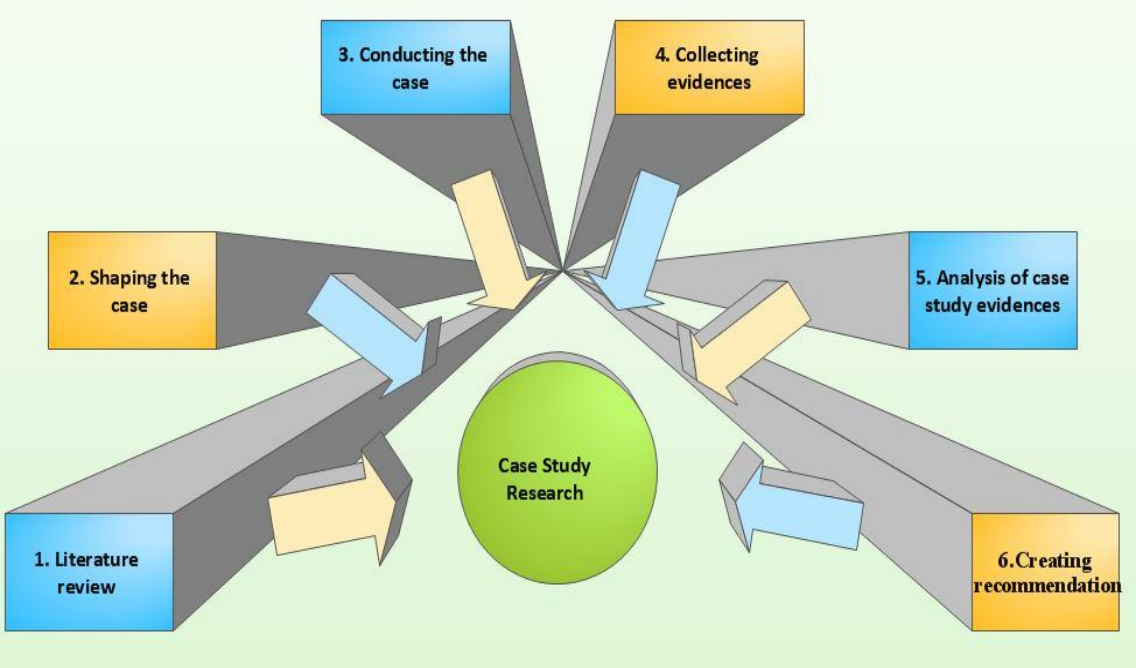

Figure 2. Research Steps Taken

Interview

The interviews were utilized to collect information directly related to the case study research questions. The interview provides an in depth explanation of the case study problem which enhances the process of defining the research problem objectively. The nature of the interview was open ended. The interviewees for this thesis work were with the Information Security Officers and Server Administrator Mr.MKfrom OGPLC. The interviews with the interviewee were made three times within the time span of this thesis work, to ensure that correct information gathered. Interviews were made through Skype. Furthermore, when conducting the interview the interviewee was motivated enough to explain unclear statements and further clarified and summarized by the interviewee. More significantly, I was objective and did not have bias, during the

process of the interview, to influence the interviewee's statements. I did not show acceptance and assumption to stay away from influencing the respondent. In addition, the responses to the questions forwarded to the interviewees written clearly for the analysis stage of this thesis work.

I avoided unclear and confusing questions, or those questions made up of two or more questions. Robson (2002, 313-325) points out by raising long-questions the opportunity to obtain a response for each aspect of the question would not be achieved. I avoided posing many theoretical concepts to eliminate the misunderstanding which arise from the difference of opinion. Finally, the researcher ensured that the interviews did not last extremely long.

Observation

Gill and Johnson (2002, 144) define Observation "observing what is happening but also feeling it." (Gill & Johnson 2002, 144 cited in Sunders & Lewis & Thornill 2007, 284). Observation used to address the root of what is going (Robson 2002). Observations made in order to determine the implementation of information security measures in the case company. Observation was done by a delegated person who works for the company in order to gather information on the use of security. Moreover, Observations are essential instruments in order to verify the responses of the respondents on the interview. Therefore, the research was not entirely depending on secondhand research sources of investigating the incident. (Saunders & Lewis & Thornhill 2007, 286-293.)

During the observation, the observer keep record all that is going on. Rather than asking a question about it. The observer focuses on only on what is highly relevant. The observer takes note and comment on the comment box. (Robson 2002, 325-328.) Therefore, the results table which shows the comment of the observer is utilized during the analysis phase of this thesis work.

1.4 Expected Research Outcome

My research outcome firstly, shows the factors that cause the information disclosure. Secondly, it identifies actions and procedure to secure confidential Information. In addition, this thesis work recommends guidelines to ensure less interruptive flow of information in a highly secure manner. The significance of this Thesis work is that it

can be used as a reference for future study undertake in the OGPLC. Moreover, it will improve the level of understanding towards information security for the company employee. Furthermore, the information communication security guideline will make it easier by illustrating what to do, when to do it and at which stage. It also offers recommendation on the distribution of information that who will have the right to information and in what manner.

1.5 Structure of the Thesis

This Thesis work is divided into seven chapters in order to address the research questions and come up with a clear and appropriate solution and discuss them coherently. Chapter 1 covered above. Chapter 2 addresses the introduction and background information about the case company and the current challenge of the company plus a detailed description of the case. Chapter 3 discusses existing literature about information security, information system and components of information system to indicate what the research covering area is. Chapter 4 presents the impact of Insider behavior on the case company. The chapter focus on the motive of attack and the main reason that direct them to engage in causing attack on the company they are working. Chapter 5 discusses the risk of information disclosure and the different states of information. The consequences of disclosure are explained in detail. Chapter 6 presents the findings from the structured observation, analysis and interpretation of the findings of the Thesis work. Concurrently, this chapter highlights the answer whether OGPLC information security practice is effective or needs more improvements. Moreover, the chapter includes the proposed recommendations which are categorized in the following structure, recommendations that answer the research questions, recommendations for utilizing existing technologies and recommendation for guidelines to be followed. Chapter 7 presents conclusions, discusses the analysis of the Thesis work, and calls for further research.

2 BACKGROUND INFORMATION OF OGPLC P.L.C

The background information of the case company is not presented because this thesis work includes the weakness of the company in securing information and deals with confidential facts about information security and information security strategies. Therefore, the secrecy of the company was highly required. For the secrecy purpose, the company background information is removed.

2.1 Current Challenge of OGPLC

According to the Information Security Officer and Server Administrate Mr.MK(2012) OGPLC has encountered an information disclosure from the premises of OGPLC to outside the premises of OGPLC. Security breach has brought considerable challenge to OGPLC. Primarily it affects the trust of the company image in the sight of their customer. Secondly it affects the profit which could be obtained, if this information does not disclose to unauthorized people. Gardner (2000) points out the five actual business risks that a company can encounter from the case similar to the above are theft, fraud, legal liability, Company image and lost revenue. The existence of these five in broader category can cause challenge in terms of economic and reputation. (Gardner 2000 cited on Boyce & Jennings 2002, 38).

2.1.1 Trust Implication

Trust on this context is the provided confidence from the company to the customer that the information collected by the company be protected in a promised manner. Trust is about the quality of clear and understandable effort made by a company and expressed through the physical, operational and technical information system components used for processing information. (Axelrod & Bayuk & Schutzer, 2009, 23-27).

It is acceptable for a customer to think that the company is not reliable to do business with them after having information disclosure occurred. The following practical example shows what has happened related to the case, OGPLC offer discount for a customer who registered to be a member as a customer of their company. When the customer would like to apply for a membership, OGPLC requests them to provide personal detail to have their customer detail on their customer database. The purpose of gathering the information of their customer is to contact them, when there is an offer and to have them as a potential customer for other business conducted by OGPLC. Therefore, a customer who gives all his personal detail when he realizes that the company has a breach in their customer database list. It is obvious that the customer will lose trust to some extent. Depending on the information disclosure occurred it can be become a danger to OGPLC.

2.1.2 Economical Implication

When OGPLC prepare a statement of the scenario of the information breach faced recently, it is more likely that the customer who is the victim of the information breach will require a recovery of the damage. Therefore, OGPLC has to pay them in monetary terms, and it is a cost for OGPLC. The other cost associated with the case is that cost of investigation. The Company has to discover who, when, how the cause happened and the necessary precaution and lesson from the incident. Furthermore, they incur a cost of lawyer who can defend the case on the court as well, OGPLC did not only lose profit but OGPLC has incurred loss due to the information breach that occurred. The fishbone outline was used to compile the tangible costs for the purposes of this thesis work.

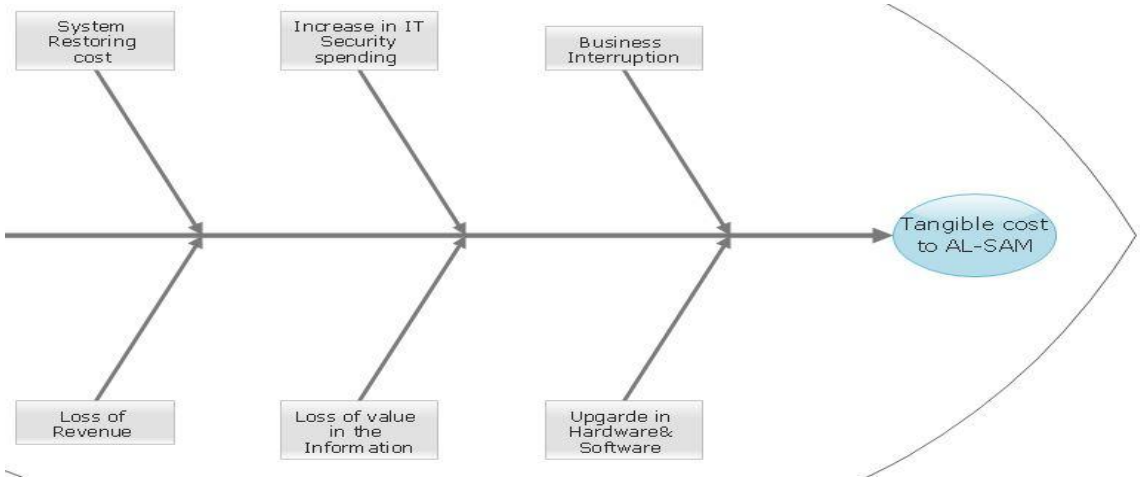

Figure 3. Fishbone-Tangible Cost

Intangible costs

Signal to the attacker: the announcement of information security breach also regarded as an invitation for other hacker that company defense mechanism have shortcoming and security have a weakness issues. The alert even attracts more of such incident because those hackers will keep trying to seek for available weakness and have access to the company confidential information.

Bad reputation: the security incident that caused information breach affect the company in a way such as leading the customer to step back and look for some other company. The impact can be highly dangerous because it opens the door for competitors to take away the case company's customer. (Cashell & Jackson & Jickling & Webel 2004.) The fishbone outline was used to compile the intangible costs for the purposes of this thesis work.

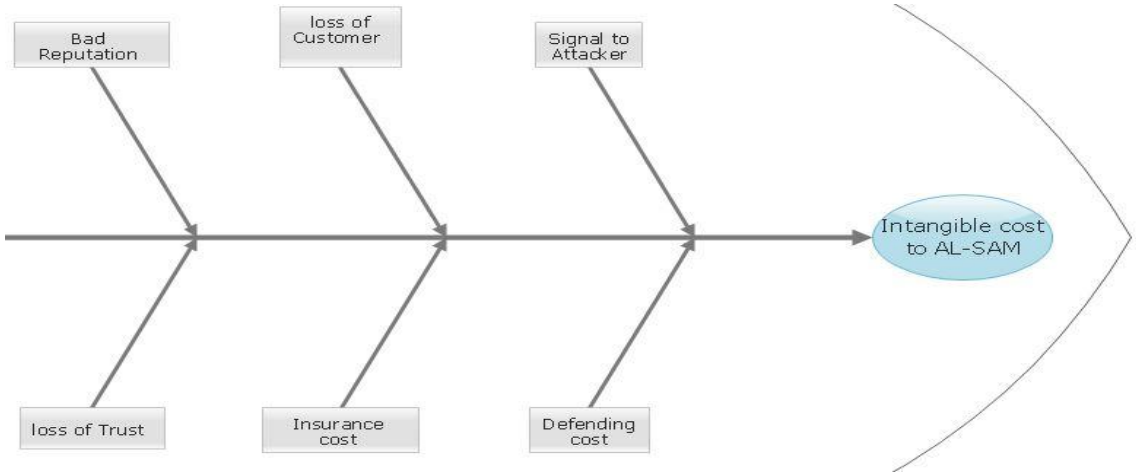

Figure 4. Fishbone-Intangible Cost

2.2 Description of the Case

The case will be present in detail on this paragraph for better understanding of the case in hand. According to Mr.MK(2012) the case company has made a research on importing new product for a domestic consumption purpose. The research conducted indicates that there is a demand, if the products might have made available for the local market. OGPLC made the list of a potential customer of the product to be imported for start up. Moreover, they have made a deal with their distributors and reach an agreement. Profit expected to rise up to about five percent. However, when they begin to process to import the products they found out that these products already imported. OGPLC begins to study what exactly is happening with their study, and they realized that one of the research study document is shared from the office with other outsiders since the document made in five copies on different systems the situation was difficult to identify who did it.

The case in hand clearly indicates that there is a breach in the vital business strategy to gain new market niche information it is a breach in information. Information breach considered as undesired event by which some confidential information compromised, accessed, stolen and utilized by an individual who do not have legitimate permission to view the protected information. Breach can also be considered as any incident which causes a dangerous one to the confidentiality, availability, and integrity of any given confidential information. (Michael Krausz 2010, 50-60).

The research alone is considerable loss for the OGPLC in financial terms. Similarly, the prospect list also is a dangerous one because it contains customer personal detail which could lead to identity theft. This means OGPLC is putting the prospect customer in an enormous risk called identity theft. The case is just a little more than just information loss it contains broader complicated cases inside it.

Personal identity theft relates to using one person's individual detail without his or her awareness and transferring their information to others without their knowledge. Identity theft is pretending to be anyone who you are not that person for the main objective of obtaining access for different services, services that requires legal access verification. Pretending someone primary purpose of gaining money or commit crime. (Hoffman & McGinley 2010, 1-3).

Hoffman & McGinley (2010) points out that personal identity includes a person's information such as, a person’s name, address, telephone number, birth date, Social Security number (henceforth SSN), driver’s license number, passport number, health insurance policy number, employee identification number, employment history, student identification number, financial account numbers, account passwords, biometric data, e-mail address, and instant messaging screen name. If this personal information obtained, there would be multiple ways they can be used against that the individual whose personal detail has been under the thief. The relation to this thesis work is that all information collected by the company has to be given serious attention and apply all kind of security measures.

3 BACKGROUND INFORMATION OF THE STUDY

3.1 Data, Information, System and Security Issues

Information is a vital component in doing business today. As Gollmann (2006, 26) points out, information is the subjective interpretation of data. Information is the interpretation of data in a way which gives meaning and relevant to a person who hold the information (Laudon & Laudon 2004, 8).

On the other hand, data are raw fact illustrating event as they are happening in the company. Before data are organized and arranged into a form that people can understand and use them. (Laudon & Laudon 2004, 8.) Therefore, information security is about protection of information asset from different kinds of threats. Information security can be accomplished by ensuring the CIA of any given information. (Bishop 2005, 1-4).

The above paragraphs discuss about data, information and information security. In the section to follow, the emphasis is on Information Systems, which is a collection of components which are connected to retrieve, process, and distribute information. Information systems have information about significant people, place, and the environment in the company. This helps the decision making and control process in a company. (Whitman & Mattord 2005, 14-17.)

The objective in this Thesis work is securing information, which is processed in a computer based information system (henceforth CBIS), CBIS is an information system which highly depends on computer hardware devices and computer software applications with the intention of utilizing and processing information. (Laudon & Laudon, 2004, 9-21).

Figure 5 below illustrates that information system goes beyond a computer using information for the purpose of doing business. However, Information system, demands the recognition of the company, management, and information Technologies, (henceforth IT), in shaping the system (ISACA, 2009).

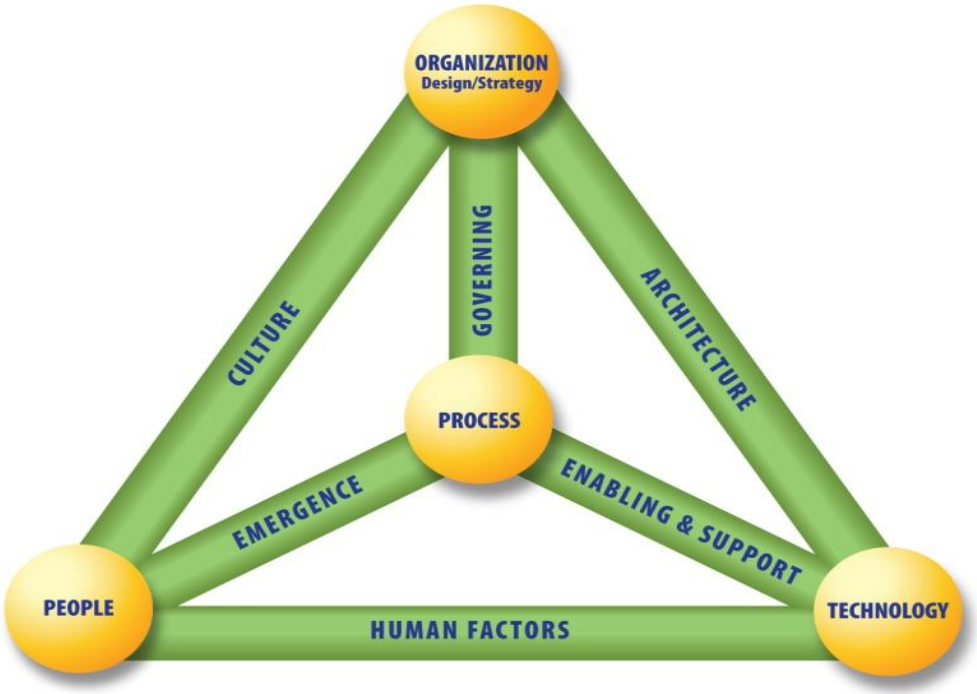

Figure 5. The Business Model for Information Security (ISACA 2009)

The Business Model for Information Security contains four main components i.e. Organization Design and Strategy, People, Process and Technology. Further, the model contains six links which are Culture, Architecture, Governance, Emergency, Enabling, Support, and Human Factor, and they connect the four main components to determine the casual relationship between them. Figure 6 illustrates that all the main components and links between them are interconnected to one other. The relationship has to be recognized and addressed properly.

Giving the recognition to information system leads us to consider the components of information system. As Whiteman and Mattord (2005), points out the components of information system are the entire set of software, hardware, data(database), people, and networks (telecommunication) are necessary to use information as a resource in company. Figure 6 shows the components of an information system.

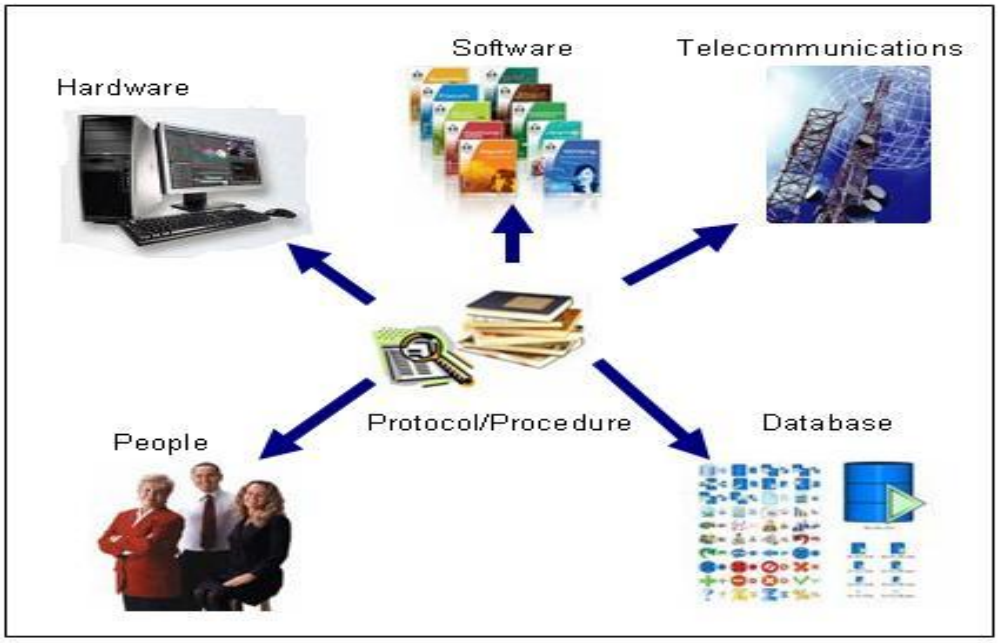

Figure 6. Components of an Information System (Whitman & Mattord 2005)

3.2 Components of Information security

Software this component includes the application, operating system, command utilities, procedures and programs running on the device.

Hardware this component includes the physical device that surrounds and executes documents used in information processing, software and data. The hardware serves as a medium for entry and dismissal of information from the system and to the system.

Data is a component which is mandatory and highly valuable asset owned by the company. Data is the target of different kinds of attack.

People are components necessary for the execution of all the information stored in CBIS. Information system is created by people and meant to serve a required service to people. It is reasonable to say that people are the components that can have more influence for Information system to succeed or not succeed than other components.

Procedure this component is contains manuals and instructions on how to perform a certain task. Therefore, if an unauthorized person gets access to this manual or instructions they can cause a serious threat to the integrity of the information.

Network this component is a means of communication medium and it includes the Internet, Intranet, and Extranet, which are extremely beneficial for a company and CBIS. (Whitman & Mattord 2005, 14-17.)

Information disclosure can happen any time through the means of information system components. However, those components can be protected from being a tool for disclosure by applying right security based on their attributes.

I will illustrate in Figure 7 below the distribution of information disclosure and attributes they inherit. Information system is classified based on their attributes such as disclosure, cause, sensitivity and their security reflection.

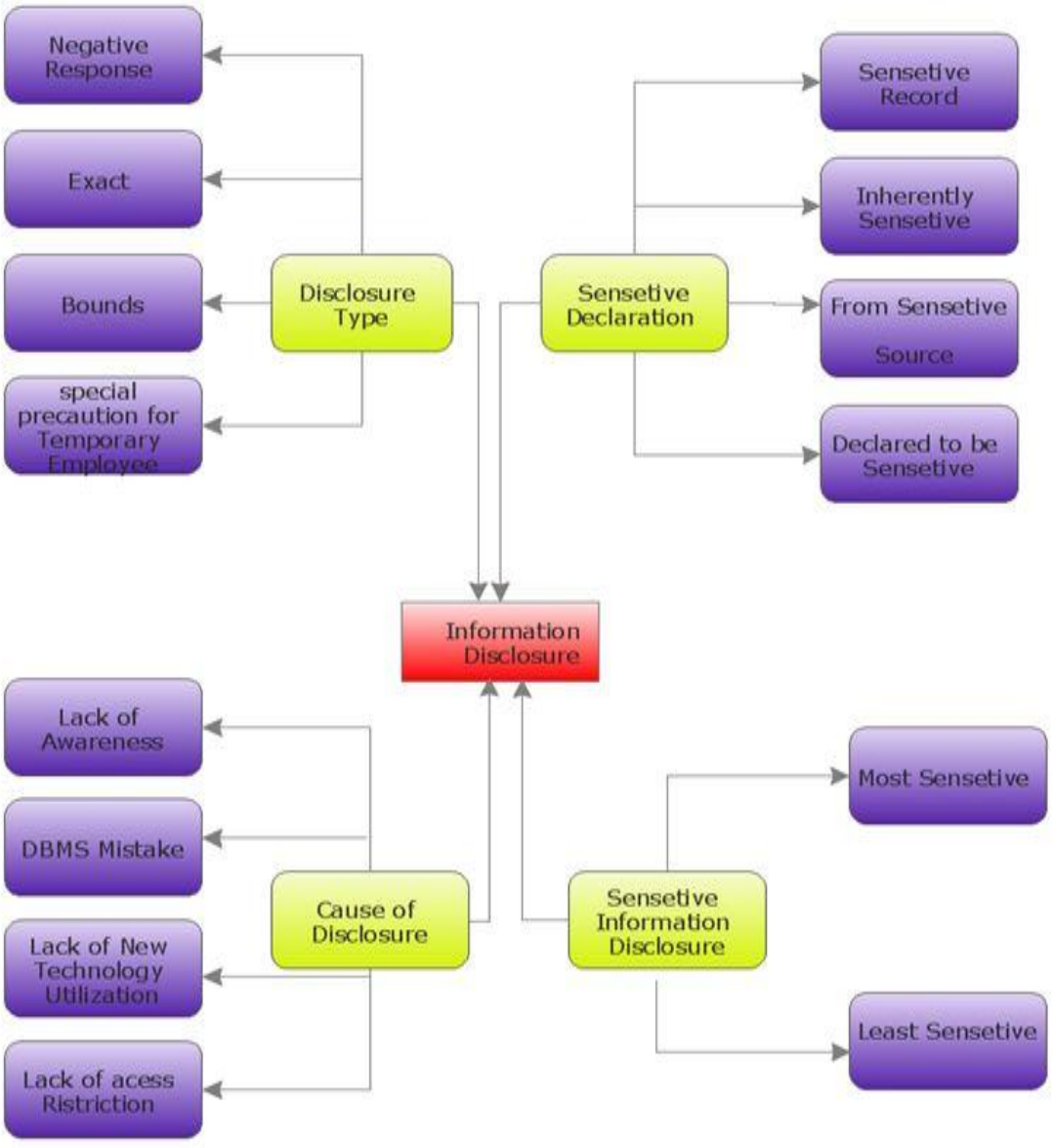

Figure 7. Information Disclosure Map

4 MAJOR IMPACTS OF INSIDER

4.1 Introduction

Insider on the Thesis work reefers to the employee who works in the company. Insider is a broad subject which contains many elements in it. Insiders are employee of the company who are offered a legitimate access to the company information, systems, and network connections to perform their daily assigned job duties. Therefore, the risk that is caused by the insider is refereed as an insider attack. (Stolfo & Bellovin & Hershkop & Kerontyis & Sinchair & Smith 2008, 19.)

McCumber (2005 180-186) emphasizes human behavior in relation to technologies and discusses how they can impact on the company if they are not carefully studied. Humans who have been offered a legitimate right to use the company's system to perform their daily jobs could also have possibilities to cause serious attacks to the company.

Stolfo et al (2008 20-25) argue that insider is not only this individuals who have a legitimate access to the company but also the business partners, suppliers, guests who have a formal or informal connection with the company for doing business. Moreover, anyone who gets authorized, properly defined, and authenticated to do certain business activities using the company's system is considered as an Insider.

Figure 8 illustrates the three stages of data theft. The stages require obtaining legitimate access. Having legitimate access copying or downloading documents not allowed be copying or downloading. When copy is ready they took it out. (Stolfo et al 2008, 53-61).

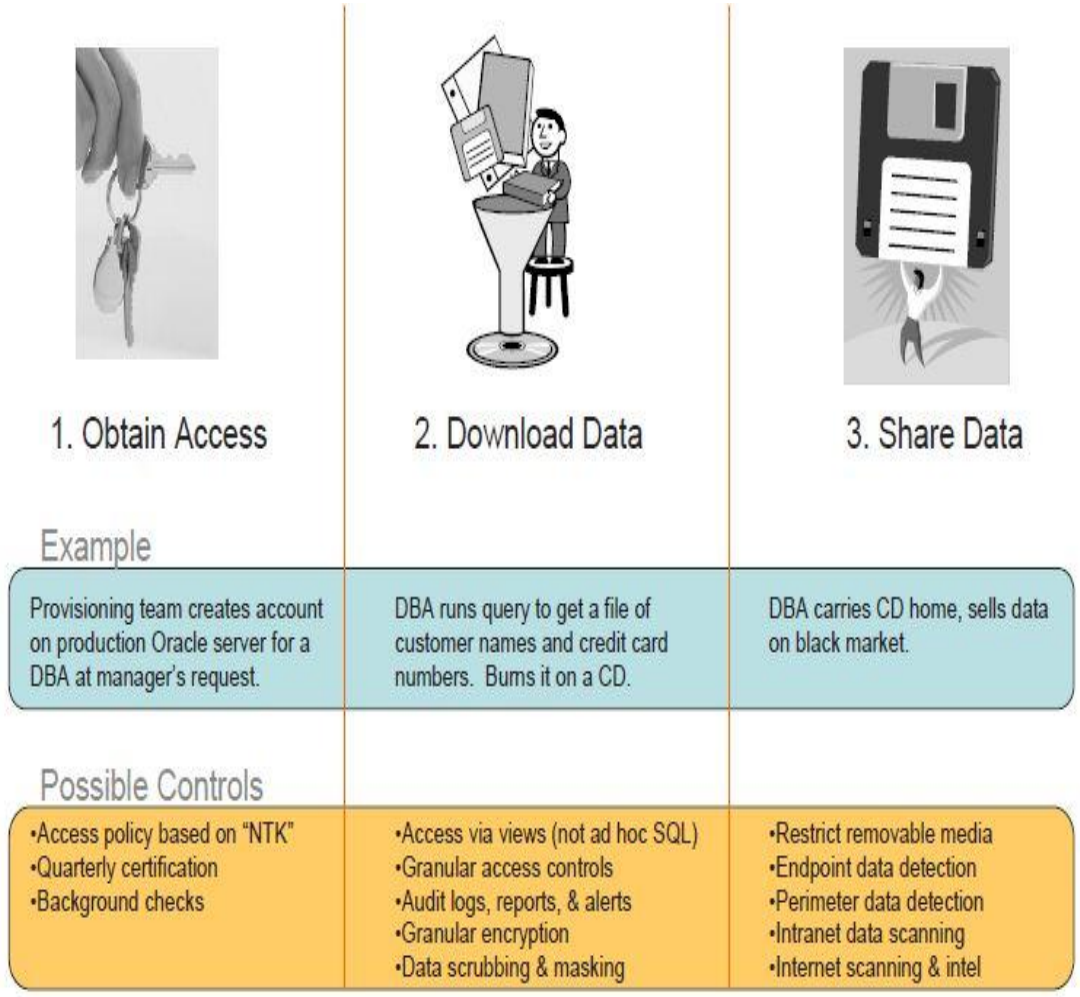

Figure 8. Stages of Data Theft (Stolfo et al 2008)

4.2 Attacks That Emerge From Insiders

The attacks emerging from the insider can follow a different approach. The first reason is that the attack can be categorized as Intentional and Unintentional. The second point depends on the motive behind the attack.

Stolfo et al (2008 1-4) emphasizes that there are three main Insiders attack Approach. Misuse of Access this attack approach is difficult to detect it. The main reason is the attack emerges from the people we trusted and give them legitimate access to perform a certain task. However, those we trusted use their legitimate access unaccountably to cause a problem. Defense Bypass this approach is trying to intentional gain access to information the insider has no right to view. Insiders are already inside the company, and they have passed the different levels of the company security check point somehow. Therefore, if they work on breaking through and gain access, the likelihood of success is

much higher than the other hacker outside the company. Access Control Failure lastly, these types of approach indicate that insiders are more likely to gain access when certain failures occur in the company access control mechanism. There is no other way to control who accessed what in case failure occurred. During the investigation of research question it has been clear that the case company put more effort to detect attacks from outsider than insider. The above discussion made to question the case company about their effort on protecting their information from the insider.

4.3 The Driving Compass of Insider Attacks

The desire of insider attack remains unclear. The reason is that insider attack contain both intentional and unintentional context in it. Unintentional attacks are attack which does not occur for the primary motive of causing a problem, but it could result in disclosing information to unauthorized users. Unintentional attacks include making unintentional error, insider might try to fulfill his duty and seek more information and go beyond the access granted to him. Additionally, for the purpose of getting his work has done remarkably well. Insider checks the company system to bring creative way of using the system and make the work more efficient. In some situation insiders pass their limit without them knowing it that their action is beyond the circle of limit given to them. Lastly, insiders check the existence any vulnerability that could pose harm to the system with the main objective of informing to the concerned authority in the company for the sake of enhancement. Stolfo et al (2008 1-4.)

However, the main focus on this thesis work remains with this attack which meant to be intentional insider's attack such as searching for possible weakness and vulnerability. Obtain access to information and spending more time than necessary in searching and viewing information, demonstrating a challenge and outsmart other fellows by causing harm and showing what they are capable of doing to seek respect of intelligence, lastly to show their detachment and dissatisfaction on the company.

It is highly agreeable what Krauzs (2010, 101 original emphases) emphasized, breaches are not just simply “happening” from nowhere rather breaches are “committed” by individuals. This breach emerging from inside get supported by insufficient security

measures and lack of effective security policy, managing the human resource of the company, indefinite use Technology and function of business activities in the company.

Among the many intentions of insider for disclosing information to outsiders, some are chosen for discussion to let the case company be aware of them. “Greed” individuals decide to take information out from the company with the primary objective of personal benefit and getting enough money and live life in prospers. They do not consider the consequence of their action could cause serious damage to the company they are working. Clearly their motive here is Money and Money. “Despair” comes from individual incapability, to run life smoothly due to lack of money to cover up the bills he is due such as mortgage, automobile, phone bills. Therefore, the pressure comes from paying everything off. However, they choose to engage in passing information out and exchange for money. “Revenge” Individual engage in revenge when the company does not threat them well, or they feel unhappy they way they approached. For one of the reasons, they can be involved in revenge. “Business Advantage” the individual task here is to spy on the company. Steal some information and sell it that company who engaged relatively in the same category of business. Individual seek advantage from the business through the means of finding out some relevant information which kept in confidential. (Krauzs 2010, 101-104 original emphases.)

4.4 Insider Security Breach Investigation

Insider security breach investigation describes the security breach situation come across in general. It shows where the breach happened and who has caused the breach. It brings detail information and supportive evidence for the situation in hand. The method used to identify the suspect and gather supportive evidences to claim compensation for the damage caused. (Bayuk 2010, 3.)

Additionally sorting the main components and their relationships considered to be essential for better understanding of the figure 9. The ultimate goal of the whole investigation process is to bring law enforcement. Therefore, the process begins with a case seeking law enforcement. The investigation process contains core components such as Investigation, identification of harm caused to the system and collecting evidence.

Firstly investigation, the framework starts with the investigator in the field and gives an idea about how investigation techniques understood in the circumstance of a complete investigative approach. It also demonstrates links to technical specialization that required performing investigations in certain categories. Secondly, identification of harm caused to the system: the importance of sorting where the cause takes place helps to understand where the breach comes from be it from an insider or other outsides. Lastly, collecting evidence putting the evidence together with the analysis made, it enables the investigator to put the case forward with a strong investigation results and understandable to bring the desired law enforcement. (Bayuk 2010, 1-5.)

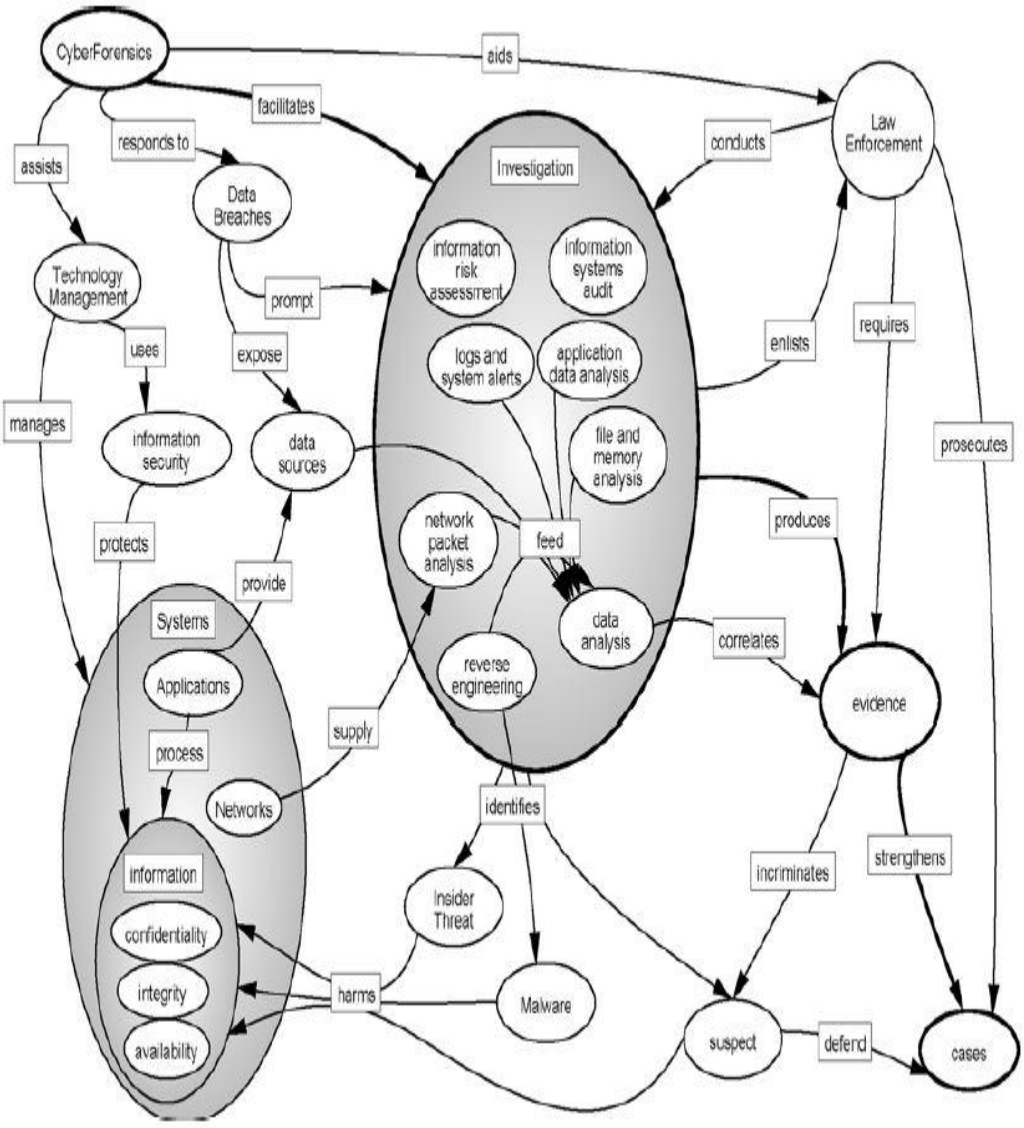

Figure 9. Cyberforensics framework (Bayuk 2010)

Figure 9 illustrates a cognitive framework. The framework indicates that all the different specialization in the organization has to work in collaboration, to discover the one who cause the information breach. It starts with investigator chosen for the case in the middle. The investigator makes analysis of the components under it to seek law enforcement on the criminal. The court requires evidence to judge. The investigator provides evidence and the potential suspect of the case. The cyberforercise provide the data source and the network analysis result and feed it to the investigator. Therefore, the analysis result altogether with evidence enables the investigation outputs support the case and brings justices.

4.5 Business Processes of OGPLC

The business process of OGPLC and the application in use described below. The description is a highlight for the next chapter. The following chapter addresses the issue related to information disclosure and their consequences. Therefore, information disclosure that is discussed in the next chapter falls under one of the items of the category below.

- Conducting research necessary to make a decision whether or not to import certain product or not.
- Create import and export document on the company system.
- Execute sales and distribution documents.
- Process wholesalers and sub-distributor request.
- Manage wholesale and sub-distributor load record and send reminder.
- Produce report monthly about the sales and distribution performance of the company.
- Process membership request from customer.

4.6 Business Software Application in Use at OGPLC

The business software applications and their utilization purpose are described in the following table.

Table 1. Business Software Application in use at OGPLC

Application Type	Application Name	Application purpose
Antivirus Software	Norton Antivirus	To protect the computer from getting a virus
Word Software	Microsoft Word 2007	To write, edit, and format a document
Payroll Software	Payroll mate 2007	To calculate net pay and local taxes payroll
Inventory Software	Inventory Tracker Plus	For Managing the inventory
Contact Management Software	Sage ACT	To keep record everyone dealing business with

Table 1 illustrates the list of major application used in OGPLC to run the business smoothly and effectively. There are additional applications used in parallel to those which are listed on the table. However the focus remains on the above listed application because of their relation in storing and manipulating information other than the Antivirus software. Unauthorized access to this application is the one that put the company in danger.

5 RISKS OF INFORMATION DISCLOSURE

5.1 Introduction

Information is re defined in this chapter again in relation to information disclosure and security. Discussing about information disclosure first it is important to begin by determining information itself clearly. Information is a highly difficult word to define since it is suggested several definitions since it is hard to define because of the characteristics it possesses. There are different states of information namely, information being transmitted, information being stored, and information being processed. These states show that when the concept of information is discussed, three different states of information are discussed. Figure 10 illustrates the Cube Model of information (McCumber 2008, 99-106).

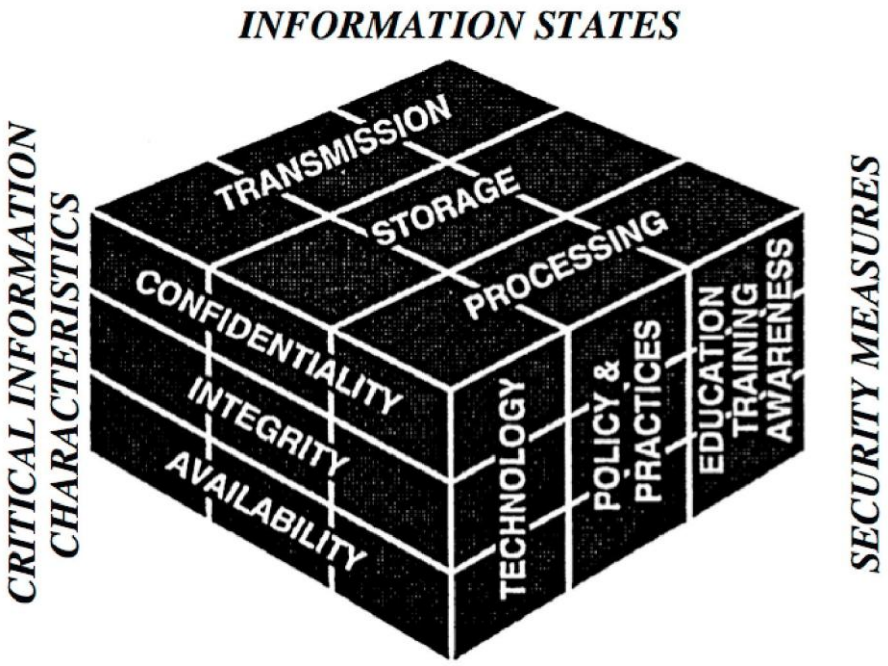

Figure 10. McCumber Cube Model (McCumber 2005)

Figure 13 illustrates that security measure has to be applied keep the critical information characteristics in a confidential state. The three main concepts are the state of the information, the characteristics of the information and the security measures, each main

concept contain three different layers. These different layers of information systems security can be observed on the structure of the model. For instance, technology such as authorization, authentication, and passwords and physical security and locks on server rooms, can be applied at the storage state of information. Furthermore, "cryptography" can be used as technology which safeguards information at the transmission state. "Education, training and awareness" can be used to secure information in its processing state. (McCumber 2008, 99-106 original emphases.)

5.2 Types of Information Disclosure

Exact Information Disclosure happens when the exact confidential information itself is disclosed. Unauthorized user might request confidential information and obtain it due to lack of proper authentication check. It could also happen when an unauthorized user requests general information and get obtain the exact confidential information included in it. Therefore, in both cases it can be concluded that confidentiality of the information is breached. (Pfleeger & Pfleeger 2003 326-332.)

Bounds Disclosure happens when the boundaries of the confidential information disclosed. For instance, the company keeps a record of employee detail such as last, first, and middle names, social security number, address, salary, marital status, nationality, race, health condition, drug use, and background. Therefore, boundary here could be to disclose first name last name and address, and the rest can be declared to be confidential. However, if information among those declared to be confidential information disclosed to an unauthorized user then, we can conclude that the boundary of information disclosure breached. (Pfleeger & Pfleeger 2003.)

Existence Disclosure indicates that certain information exists in the company database or file cabinets which does not disclose for everybody. Therefore, the existence the information in the database or file cabinet becomes the center of attraction. For example, a company does not want to revel that the use downloads using the company system are monitored. Therefore, discovering download records filled in a file cabinet or database would disclose the information that the company wanted to keep it confidential. (Pfleeger & Pfleeger 2003.)

Partial Disclosure does not disclose the exact confidential information. However, the user can get the probability of the information he has requested for. For instance, there is a very important people's henceforth (VIP) meeting held on the company, and four line mangers were invited to attend the meeting from each department. The user wanted to know if Mr. Ibrahim will be attending the VIP meeting. The user may know how many people were invited from sales departments. The answer would be that four person invited from sales department. Therefore, if the user knows how many people from sales department registered as attending for VIP meeting. The answer would be for instance three, and then the user can conclude that the probability of Mr. Ibrahim attending the VIP meeting is 75 percent. (Pfleeger & Pfleeger 2003).

5.3 Consequence of Information Disclosure

McCumber (2008) has categorized the consequences of failing to protect information properly. McCmber (2008) call the category the four Ds.

- Destruction
- Delay
- Disclosure
- Distortion

Firstly, Destruction deals with the actual destruction of data media for instance, breaking CD, memory stick, hard-drives, and deleting items from the database to cause a denial of information when the information required for use. Secondly, Delay deals with denial of access to certain information for a limited time span. Thirdly, Disclosure deals with exporting internal, confidential information to other for the purpose of keeping it, with the intention to use it sometime in the future or simply sale it and gain money in return. Lastly, Distortion deals with detection of information from the unauthorized modification made on the information for the purpose causing wrong decision to be made. Distortion is the alteration of information to mislead or interrupt decision making. The consequence making a decision on the basis of inaccurate information is disastrous. (McCumber 2008, 40-47.)

6 RESULTS

6.1 OGPLC Information Sharing System

OGPLC has six sites to run that company business activity day to day. OGPLC shares and distributes information to facilitate business transaction and process of their company. Communications between the sites are enabled by the medium of Internet connection. OGPLC uses four servers to distribute, share, and keep a record of information. OGPLC has one centralized server plus two access server named as access server A and access server B both contain different information. OGPLC grant permission to these servers on the basis of the department the individual belongs. Therefore, the individual who belong to a certain department can view information indefinitely without any restriction.

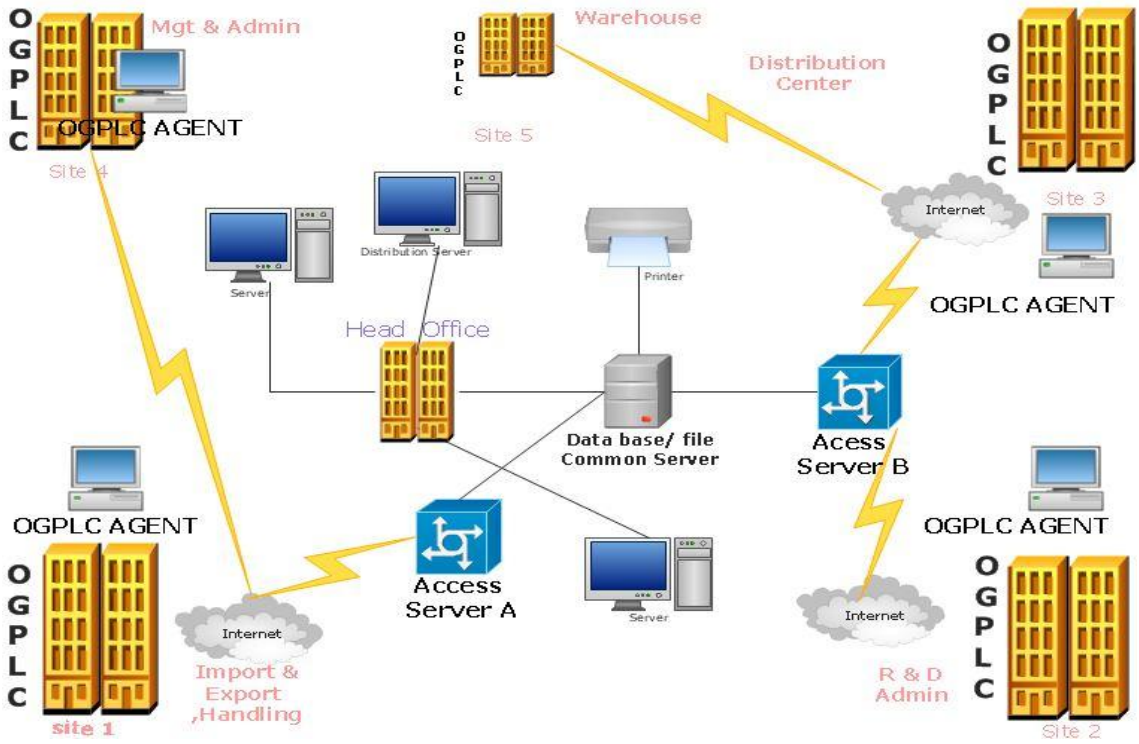

Figure 11. OGPLC Network and Information Sharing System

6.2 Observation Result

The observation result table describes in brief the expected security measures need to be applied by referring to the result table. The result table below serves as a reference point. The table allows checking what already has been used and what has not been used

or what is less effectively used. Therefore, it is indicated on the table below if certain security measures were utilized and if they were utilized unsatisfactorily or if they were not utilized at all.

The information stated on the results table shows that the company takes real effort to protect information from external attackers. Protection from external factors are expressed by making use of firewall, antivirus tools, restriction on remote use, encryptions, strong password system and system control measures. It is clearly evident that OGPLC gives more emphasis to protect the information from external attacker than insider. However, attacks from insiders have been given less priority than the attacks that come from outside OGPLC. The result presents the loopholes which need to be reconsidered such as securely shared resource utilization, download restriction, access control, choice of proper desktop location, securing the trash are among the get way for attack from Insider. These results will be discussed in detail later on the same chapter.

Table 2. Observation result

Information Security of workstation	Comments
Update operating system regularly	Utilized
Keeping virus protection up to date	Utilized
Using firewall	Utilized
Secure shared resource	Utilized but not satisfactory
Prevention of remote use	Utilized
Check application security properties	Utilized
Using proper password	Utilized
Managing user account	Utilized
Back up handling	Utilized
Security awareness	Utilized but not satisfactory
Download restriction	Not Utilized
Email use	Utilized
Encryptions	Utilized
System access restriction	Utilized
Incident handling team	Not Utilized
Security policy	Utilized
Proper directory and file permission	Utilized but not satisfactory
Workstation lock	Utilized but not satisfactory
Device positioning	Utilized
Securing trash	Utilized
Use lockable file cabinet	Utilized but not satisfactory
Virus protection	Utilized
Checking browser cookie	Not Utilized

6.3 Result Analysis and Interpretations

The results collected from the observation are analyzed in table 3. The analysis table is made to show the strengths and weaknesses of the security aspects in OGPLC. The table contains two main aspects to evaluate the security experience of the company. The horizontal list is meant to represent the company information security principles. The vertically listed contents are meant to represent the core principles of security. Therefore, by comparing and contrasting the results table with the analysis table, the area which requires improvement was sorted out. The shaded part with dark orange color shows what the company has to pay attention to.

Nevertheless, the results obtained and evidences collected facilitated the process of analyzing the work objectively. The analysis was made from the light of two most important perspectives with many rays. These two perspectives are information security principle of the company and the main principle of information security. Therefore, they have to match up since otherwise problem are to be expected. The importance of using the table to analyze this thesis work is that it illustrates the dissimilarity between information security principle of the company and the main principle of information security.

Table 3. Mapping Enterprise security principles to security principles (SIFT Pty.Ltd 2007)

Information security is integral to enterprise strategy	Information security impacts on the entire organization	Enterprise risk management defines information security requirement	Information security accountability should be defined and acknowledged	Information security must consider internal and external stakeholders	Information security requires understanding and commitment	Information security requires continual improvement	The shaded part indicates Deficiency seeking for an improvement The boxes which are left not shaded represent the principles practiced and the company managed to practice them to some extent
			■				Accountability
				■	■	■	Awareness
■			■		■		Compliance
	■						Effectiveness
			■				Ethics
			■			■	Inclusion
	■	■					Transparency
						■	Measurement & reporting
		■	■		■		Scope
■						■	Response
		■				■	Risk management

6.4 Recommendation

6.4.1 Problem Driven Recommendation

After conducting structured observation, interview and literature review in the field, I have managed to come up with a series of recommendations of existing technology and crucial guidelines for enhancing the security of the company confidential information. Firstly, Figure 7 on the previous chapter depicts that if individual belongs to certain department he can have indefinite access to the information provided to that department. Therefore, sharing resources is among the serious challenge considered as the cause of information disclosure for OGPLC. Secondly, the information security policy document does not practice ought to be due to insufficient awareness and carelessness. Thirdly, securing disposed paper and Device positioning is the easy to figure out security measures. However, it has neglected and neglecting the obvious never recommended. Fourthly, granting free permission to download is among those serious challenges to the company. Unsupervised download permission can result in inviting undesired threat to the company. Downloads have to be monitored. Lastly, incident handling team and security breach investigation team has to be formed. The seven listed items below proposed for successfully and resourcefully making use of the technology in hand.

1. Securing shared resources
2. Device positioning
3. Download restriction
4. Incident handling team
5. Policy in action
6. Security breach investigation team
7. Securing disposed paper handling

Securing shared resources, download restriction can be monitored my making use of the system resources effectively. For instance secure shared resources and download restriction can be managed by applying the right setting in the active directory.

Device Positioning should be considered as a loophole and rearrangement has to be done. The simplest ignored security measure could turn in serious disaster. Therefore, making sure the entire devices used to process information are placed in a protected

manner recommended highly. Similarly security policy is something the company already has. Therefore, to make it utilized effectively the company has to create awareness. I recommend the company should add a section on the website that tells about the policy and security issues of the company. Moreover, organize training once in a short time and give recognition for good performance. These increases the motivation to learn more about the policy and the more they learn and know increases the likelihood of practicing the policy they know. Again, I recommend the utilization of secure trashcan at least to a chosen department. For instance, research and development, the papers thrown out from this department contain relevant information. Therefore the papers have to be destroyed not thrown away. Finally, Security handling team and Security investigation team are something the company does not have yet. However, both are necessary to mitigate the risk and identify the how, who question of the incident. Therefore, the formations of those teams are recommended.

6.4.2 Solution Based Recommendation of Technologies

Security Event Correlation Tools

Security event correlation tools organize the log files from different sources and bring them together. Logs gathered from systems program and applications that run on the system. Logs are collected from different sources that have different formats. Therefore, security event correlation tool convert them into a standard format such as Extensible Markup Language (XML) and Report the analysis of logs to demonstrate the entire image of the current system activities. The report can serve to confirm whether the system is operating with respect to the company's policies. (GAO 2004.) A security event correlation tool first combine the log files from different sources, as illustrated on the figure12 and makes the analysis and displays the output of the analysis made.

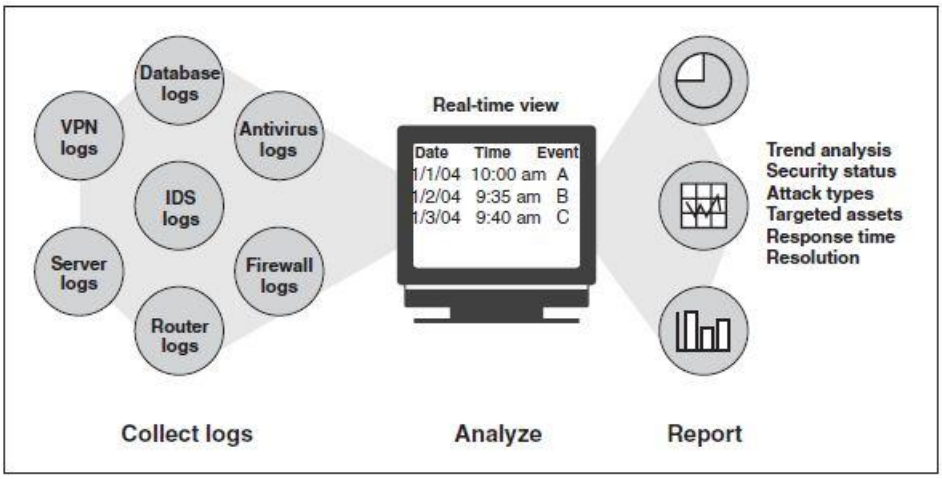

Figure 12. Security Event Correlation Tools (GAO 2004)

Content Filters Application

Content filtering applications can Control Web and messaging applications on the basis of their content. Content filters detect restricted file types, circulation of information which is against the company security policies, spam. Besides, web filters restrict unwanted document and web page out of the company's systems. Moreover, it detects different types of attacks. Most of all, web filters make supervision remain considerably easier by providing users and their browsing history with additional detail such as the web they browse, when, where, and for how long. (GAO 2004.)

Figure 13 shows the main classifications of content filters such as web filters, messaging filters, and web integrity filters. Web filters examine certain web pages to the parameter sited. Accessibility or availability web pages removed, if web pages appear to be offensive or non-business related. Messaging filters, examine suspicious message that comes through messaging applications such as e-mail, instant messaging, for spam or other offensive content. Web integrity filters, examine the integrity of whether the web pages are reliable to proceed with or not.

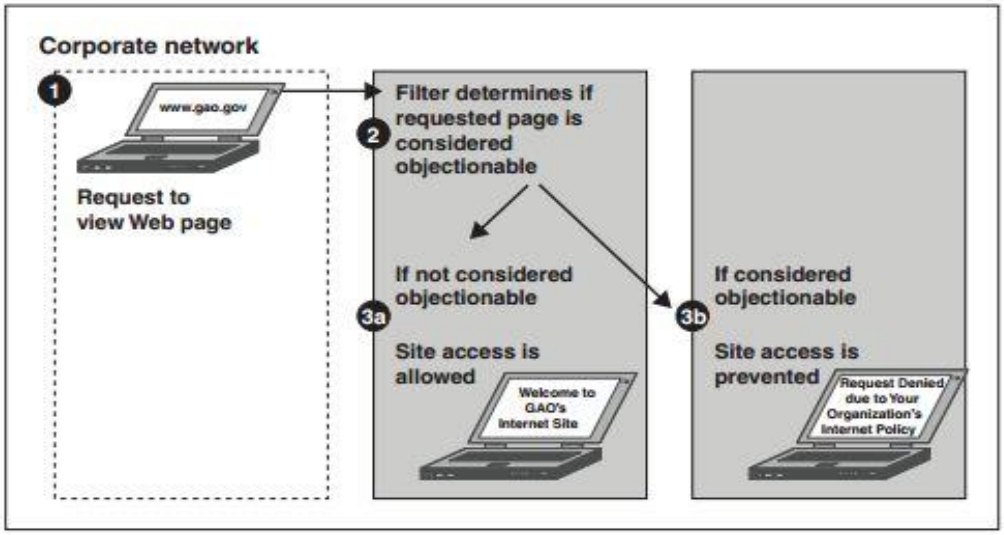

Figure 13. Web and Content Filtering (GAO 2004)

Outbound Email Filtering Application

Outbound Email Filtering is a tool which filters internal email before sent out from the company network. It minimizes the risk of inappropriate message routing and misuse of company resources. In addition, attachments are scanned from viruses and other undesired contents, and checked with the security policy of the company. (Symantec 2012.)

The figure 14 illustrates the process of filtering email. Filtration begins from user inside when they want to send information by making use of the company network to a third party who is outside the company network coverage. The filtrations are done by filtering the information contained in the email to be sent or received. In addition, the receiver, sender, topic and addresses are used during the email filtration. Finally, scanning applied automatically when messages are sent and received through the antivirus and anti spam during the transmission of the message. (Symantec 2012.)

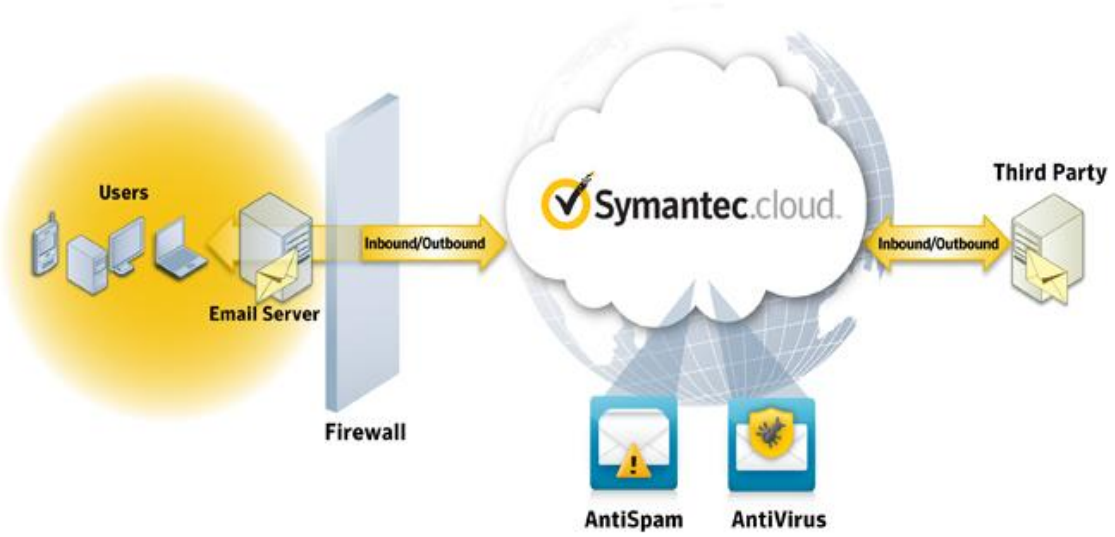

Figure 14. Symantec Email Security (Symantec 2012)

Biometrics

Biometric identification technologies recommended uncovering the identity of a person by computing and cross checking human characteristics. Biometric technologies can be used to authenticate by checking certain part of the human body which is well thought-out, to be different from person to person. For instance fingertips or eye irises identifies users on the basis of their registered biometric data to grant access to the systems. (Bishop 2005, 190.)

According to GAO (2004) Conventional identification methods in most cases use identification methods such as smart cards and Passwords. Smart cards are something the users have such as, chip cards and identity cards. However, password can be number, alphabet, symbol which someone possesses. Password considered as something that someone has to memorize than something that the person is. Biometrics is more reliable than conventional methods, for reasons such as they should not be remembered and extremely unlikely to loss them.

Therefore, OGPLC security can be enhanced more by making use of biometric scanner. The scanners recommended for utilization by the database administrator, information security officer and system administrator. The scanner can be assembled into the workstation, mouse, keyboard attached to the computer. Verification of authorized

individual can be more reliable and secured. The scanners can be a hardware device used only for the purpose of taking fingerprints. Fingerprint recognition technology pulls out features from imitations made by the unique characteristics on the fingertips. Primarily the picture of the fingerprint captured through a scanner and stored into a template. Different techniques of fingerprint scanners commercially presented.

Picture 2 and 3 below shows the biometric technology assembled in the mouse and a keyboard to enhance the process of authentication. The figure illustrates the fingertip scanner placed in both cases.

Picture 1. Fingerprint Recognition Technology Built into a Mouse (Siemens PSE TechLab cited in GAO 2004)

Picture 2. Fingerprint Recognition Technology Built into a Keyboard (KeyTronicEMS 2011)

File Integrity Monitoring

File integrity monitor grant permission to preserve digital signatures of essential system files and then once in a while monitor the integrity of those essential system files, detect unofficial changes, reports and make e-mail notifications. Moreover, file monitoring identifies any change that occurred to a monitored directory. If a new file added to a monitored directory, removed from a monitored directory, increases its size, and decreases its size. The application automatically updates the reported. The responsible authorities can then react to it. (Flexense Ltd 2011.)

The figure shows the monitoring option with the option to showing available directories for monitoring and then choose which should be monitored which not. As mentioned on the above paragraph, any change detected notification sends to the administrator.

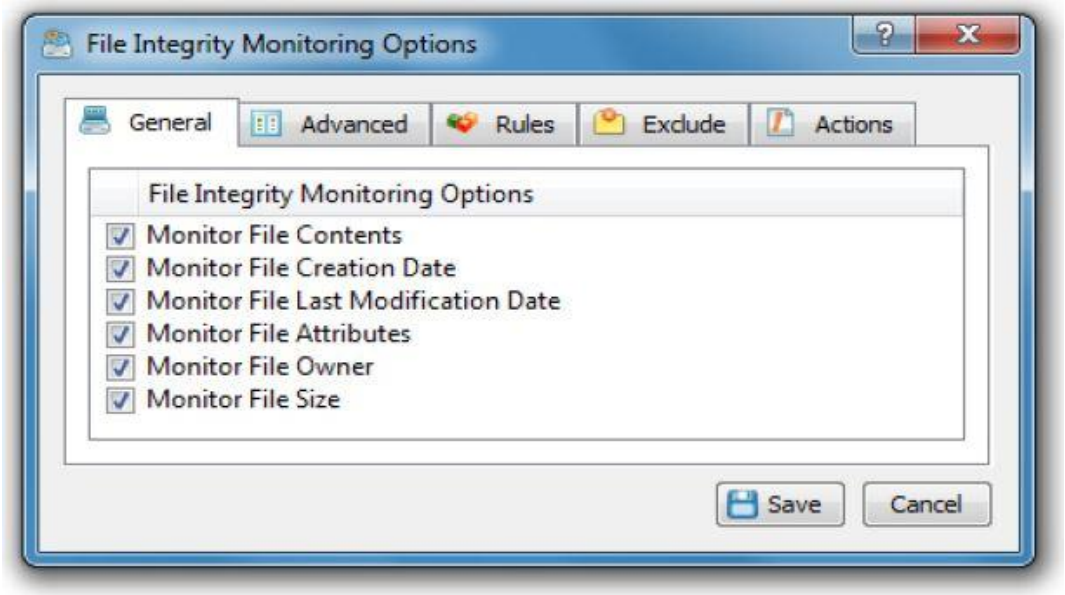

Figure 15. File Integrity Monitoring (Flexense Ltd 2011)

6.4.3 Recommended Guideline Procedure

The following Guidelines procedures of Information security are meant to protect information. The Protection of confidential information needs acknowledging the cycle of the business. Working on CBIS requires paying attention from the simplest to hardest level of the cycle. Protecting CBIS and the reliability, accountability of confidential information they hold are not a one-time job. Information are added, shared, transmitted

and removed from the system on a regular basis. Therefore, the process requires paying attention to every stage. The simplest ignored stage of the process can cause the hardest disaster.

The figure 16 depicts the cycle of securing confidential information. The cycle contains four steps circulating, and all steps have their own transition message. The steps such as before getting connected, after getting connected, in between work and after work completed parameter listed down to guides the user what to do. Therefore, the figure is meant to show the procedures of protecting the CIA of information during the process of business activities. The balanced scorecard outline was used to compile the cycle of securing confidential information for the purposes of this thesis work.

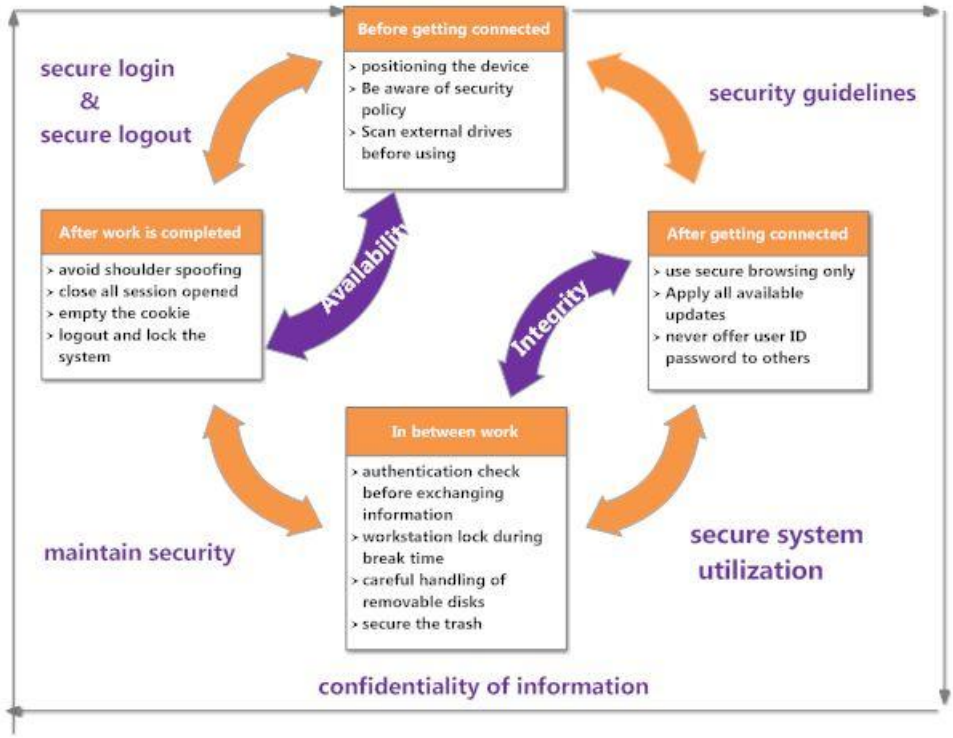

Figure 16. The cycle of securing confidential information

7 DISCUSSION AND CONCLUSIONS

The objectives in this thesis were about finding out the factors for information disclosure outside the company premises, categorize action or procedure need to be followed to secure information during information communication, enhance information security and avoid information disclosure. Information security is hard to attain because those who deal with the information are human, humans are likely to make mistakes or deceived by temporary benefit offered in exchange of the information they process. Information is very crucial because the company have invested money to make the information meaningful. The severity of compromise in information is witnessed by the case company and the consequence in terms of tangible and intangible costs. The severity to the case company was in terms of, lost of loyal customers, lost of reputation, lost of revenue, and incurred unnecessary expenses. The existence of security policy by itself does not simply save the company. The company can be safe, if they have a security policy which is in action. The same is true for the technology since it is not the technology that keeps the company safe, rather it is how it is implemented and used.

The factors of information disclosure seen from the point of view of systems, network, access control, use of application, and insider related. The case does not make use of available technologies to secure the company information because the technologies cost money. Investing money to secure the business does not have to be seen as just as an expense for the company. Investing money to secure information has to be seen as maintaining profit consistently and attracting customer and business partners to join the company. The dynamic nature of the information security makes it necessary to apply the latest technology to secure the mandatory information. Therefore, the case company has to spend some money to use the available technologies and strengthen the security layer. The nature of information security requires a multiple layer to make it extremely hard to the hacker to break through and gain access to information. The advancement of the technology gives an equal opportunity either in the right way or wrong way. If the case company uses it carefully and knowingly, it can facilitate the company performance. However, if the case company fails to use technologies carefully and properly it can be more devastating than estimated.

The case company and other companies that operate their business under computer based information system and support many of their information virtually have to invest money to keep operating safely. Finally, companies have to bear in mind that there is an expectation from different angles such as customers, employees, business partners and those who have direct or in direct contact with the company. This expectation has to do with the information they offer to facilitate the business process. Therefore, the case company and other companies have to work hard to meet the security requirements expected from them and regain trust.

As a final note, it can be suggested that future research can be done to continue on this thesis work. Continuity is extremely essential, since this thesis work has analyzed the consequences of information security breach and recommended some technologies that can be used to assist the process of secure information flow. The recommended technologies are security event correlation tools, content filtering applications, file integrity monitoring tools, fingerprint recognition built in mouses and keyboards and inbound and out outbound email filtering. In addition, the current challenges of the organization are investigated and discussed, and the recommendations of Technologies proposed. The recommendations of technology are limited to the case company. Therefore, researchers can conduct research on technologies that make information security harder to break through and gain access to confidential information than leaving space to hackers. Researchers can research on which technology to protect what and at which cost and how the technologies can be beneficial to companies. Most of all, the effectiveness and helpfulness in order to achieve secure information distribution.

REFERENCES

Printed

OGPLC Private Limited Company 2012, "The Greenland Quality!"

Bayuk, Jennifer 2010. Cyberforensics: Understanding Information Security Investigation: In Shane, Sims (ed.) Insider Threat Investigation. Springer Science+Business Media, LLC, New York. 45-52.

Bishop, Matt 2005. Introduction to Computer Security. Pearson Education, Inc, Boston, USA.

Boyce Joseph g. & Jennings Dan w. 2002. Information Assurance: A Practical Guide. Elsevier Science, Wildwood, USA.

Calder, Alan 2005. A business guide to Information Security. Kogan Page Limited, London, UK.

Colantoni, Laura 2009. Securing intellectual property: Protecting trade secret and other information assets. Elsevier Inc, Burlington, USA.

Gollmannn, Dieter 2006. Computer Security. John Wiley & Sons Ltd, West Sussex, UK.

Krausz, Michael 2010. Managing Information Security Breach: Studies from Real Life. IT Governance publishing, Cambridgeshire, UK.

Laudon, Kenneth C. & Laudon Jane P. Management Information System: Managing the Digital Firm. 8th edition. Pearson Education, Inc, New Jersey, USA.

Iivari, Pekka 2008. Business Security and Russia: Security Consideration in the Development of Business Operation in Russia. Rovaniemi University of Applied Sciences, Rovaniemi.

McCumber, John 2005. Assessing and Managing Security Risk in IT System: A structured Methodology. Auerbach Publications, CRC press LLC, USA.

Pfleeger, Charles & Pfleeger, Shari 2006. Security in Computing. 3rd edition. Pearson Education, In, New Jersey, USA.

Robson, Colin 2002. Real World Research: A Resource of Social Scientists and Practitioner-Researchers. 2nd edition. Blackwell Publishers Inc, Massachusetts, USA.

Saunders, Mark & Lewis, Philip & Thornhill, Adrian 2007. Research Methods for Business Students. 4th edition. Pearson Education Limited, Edinburgh, UK.

Stolfo, Salvatore & Bellovin, Steven & Hershkop, Shlomo & Keromytis, Angelos & Sinclair, Sara & Smith, Sean 2008. Insider Attack and Cyber Security: Beyond

the Hacker: In Bellovin, Steven (ed.) the insider attack problem nature and scope. Springer Science+Business Media, LLC, New York. 1-4.

Whitman, Michael & Mattord, Herbert 2005. Principles of Information Security. 2nd edition. Thomson Course Technology, a division of Thomson Learning Inc, Boston, USA.

Woodside, Arch G. 2010. Case Study Research: Theory, Method, Practice. Emerald Group Publishing Limited, Wagon Lane, UK.

Yin, Robert.K 2003. Case Study Research: Design and Methods. 3rd edition. Applied Social Research Methods Series Volume 5. SAGE Publications, California, USA.

Not Printed

Cashell, Brian & Jackson ,William D. & Jickling, Mark & Webel, Baird, 2004. CRS Report for Congress: The Economic Impact of Cyber-Attacks. Downloaded 27 February, 2012. <http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf >

Sharp, Walter L 2006. Information Operations, United States of America, department of the army, United States Marine Cory, department of the navy, United States of America, department of the navy, United States of America, department of the air force, Joint Publication 3-13, Glossary GL-9. Downloaded 25 April, 2012. < http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf >

Lyons, Sean 2008. Risk Management's Role in Corporate Defense. Downloaded 18 February, 2012. <http://www.soa.org/library/monographs/other-monographs/2008/april/mono-2008-m-as08-1-lyons.pdf >

Mr.MK2012a. Interview of the information security officer and server Administrator, OGPLC. 10.02.2012

Mr.MK2012b. Interview of the information security officer and server Administrator, OGPLC. 05.03.2012

Mr.MK2012c. Interview of the information security officer and server Administrator, OGPLC. 11.04.2012

KeyTronicEMS 2011. Keyboard and Mice, Security. Downloaded 4 April, 2012. < http://keyboards.keytronic.com/home/keyboards/biometrics/biometrics.html>

Vaidyanathan, Ganesh & Mauton, Steven 2009. Security in Dynamic Web Content Management Systems. Applications. Vol. 52, No.12 2009. 121-125. Downloaded 07 March, 2012. <http://web.math.jjay.cuny.edu/fcm745/codes/SecurityInWebContentManagementSystems.pdf>

Appendix 1

Observation List

Information Security of workstation	Comments
Update operating system regularly	
Keeping virus protection up to date	
Using firewall	
Secure shared resource	
Prevention of remote use	
Check application security properties	
Using proper password	
Managing user account	
Back up handling	
Security awareness	
Download restriction	
Email use	
Encryptions	
System access restriction	
Incident handling team	
Security policy	
Proper directory and file permission	
Workstation lock	
Device positioning	
Securing trash	
Use lockable file cabinet	
Virus protection	
Checking browser cookie	

Appendix 2

Interview Questions

Cased related

1 How much damage does this particular breach cost the company be it tangible or intangible?

2 What are the incidents that caused the breach in information asset and harm the company confidential information its availability and integrity?

3 How likely is such incident to happen again?

4 Does the company considered the possible ways that information can be leaked?

File sharing related

1 How does the company share and distribute information?

2 What experience does the company have using active directories?

3 Does the company use some application to store information and distribute, which application does the company uses?

Systems/workstations related

1 what kind of security measures does the company take to protect the system from compromise?

2 which technology does the company use to secure the systems from unauthorized individuals?

3 Does the company have incident handling team or investigation team who look after the systems?

Business communication related

1 How do you explain the business process of the company in relation to confidential information?

2 What kind of approach the company follows to share information with outsider?

3 How do you describe the level of awareness in information security and the risks related to information security is in the company?