TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor's Thesis

ORGANIZATIONAL SECURITY MANAGEMENT CONCERNS IN E- BUSINESS

Barlon Kimuli

Degree Programme in

Business Information Technology

2010

TURKU UNIVERSITY ABSTRACT

OF APPLIED SCIENCES

Degree Programme: Business Information Technology

Author: Barlon Kimuli

Title: Organizational Security Management Concerns in E-business

Specialization line: Business Information Technology Management	Instructor: Minna-Kristiina Paakki
Date: August 2010	Number of pages: 49

The evolution of internet has opened up many opportunities for businesses and organizations that are willing to take risks and embrace the e-revolution with a big part of transactions being made over the internet. In contrast, the Internet, which is the primary medium for conducting e-business is by design an open non-secure medium.

The objective of this thesis is to describe the importance of secure e-business transactions to organizations and their customers/business partners by analyzing the importance to which organizations attach to the information they transfer through the web.

The point of view of the thesis is mainly on organizational matters as attention is given to the security management of customers' and business information transferred during e-business transactions. A case study is done through questionnaire and interview to find out the organizations' awareness on information security issues based on the ISO/IEC 17799 standard.

As a result of the case study, several information security areas require more attention and therefore a need to revisit and emphasize information security in these organizations. Workers need to know the value of the information they handle during e-business transactions through teaching and organizing regular education programs to their staff about importance of information security.

Key words: E-business, internet, information security, Organizations.

Deposit at: Turku University of applied sciences, Salo

TABLE OF CONTENTS

ABBREVIATIONS

B2B	Business to Business
B2C	Business to Consumers
E-Business	Eletronic Business
EDI	Electronic Data Exchange
LAN	Local Area Network
ISP	Internet Service Provider
ISO	International Organization for Standardization
FICORA	Finnish Communications Regulation Authority

1. INTRODUCTION

"Information is the cornerstone of e-business" (Heimann, 2001). The products of advanced technology and, in particular, information technology (IT) is at he centre our lives. The internet allows businesses to use and access information more effective through the exchange of business information between partners, employees, suppliers and customers.

One of the essential aspects in e-business today is streamlining business processes in order to remain in operation and have a competitive edge. This is achieved through finding out cost-effective and time-saving ways to carry out e-transactions that will be secure in order to maintain and improve customer/partner relations and trust (Pennanen & Paakki, 2007). Such ways were made possible by the advent of the internet. E-business is now perceived to have more efficiency in dissemination of information in b2b relationships than ever before (Saarinen T, et al. 2005).

The internet has become a shopping centre for all sorts of goods and services and also an avenue where people can exchange ideas. The internet is transforming and reshaping the nature of inter-firm business by enabling B2B and B2C electronic interchanges (Paul A. Pavlou, et al. 2001). But as the world continue to use the internet, security concerns have become enormously important for entrepreneurs around the world.

With e-business on its course of success, online customers are much concerned about the security of the transactions done on the internet. The worry is mainly about the information deemed confidential that is transferred during transactions for instance through mastercards/visa electron cards, online purchase forms or direct purchases from companies' premises. Information security is an important aspect for companies as they try to convince online users that they can offer safer transactions without overriding on their privacy and confidentiality. Companies need to put more value to the information security of their customers in order to guarantee continued trust and relationships for future survival.

This thesis will focus on examining information security in transactions in the e-business environment. The research is conducted in Organizations in Salo city area by method of case study using questionnaire and short interview. The case analyzed how the Organizations valued information shared internally and externally through examining their current situation concerning secure information transfer and sharing on both workers' and administrative point of view. An analysis is done based on the results to find out how the current security situation affects the trust of customers, suppliers, shareholders and partners have towards the company.

The objective of this thesis is to describe and analyze organizations' role in maintaining their e-business trust and partnership by putting attention to the information that is transferred across the internet. The argument is used to find out key security aspects that firms need to address to enhance security and thus instill and maintain trust in online transactions. For instance: payments, managing accounts, placing for orders as well as physical security both on and off the premises.

The purpose of the study is to act as reminder to firms of their role in keeping information secure and also helping their employees understand the key security areas in order to improve their trust and relationships with their customers and other trading parties.

The audience of this thesis is mainly organizations that use internet as their medium of handling transactions. The thesis addresses different security aspects and in the end a reminder on the role of secure transactions. Because of the increasing need to review security measures and implementations, the thesis will also act as a platform for the big companies in order to avoid extra costs in difficult times such as economic recession.

2. ELECTRONIC BUSINESS

2.1. Definition of e-business transactions

It is common to use the terms e-business and e-commerce as synonyms(Sherif Kamel, 2006). However, there are differences between the two. The fact is that the two concepts are related and interconnected but e-business is broader than e-commerce (Zorayda .R. Andam, 2003). E-commerce is the exchange, procurement, and distribution of products, services, and/or payments between two or more economic entities via computers or other electronic means (Pitre, 2000).

It has become both a venture for entrepreneurs and a culture of learning especially for busy employed people and learners located apart from education institutions all over the world to access education in their convenient time and places (Fernández et al 2007).

The Internet has become an incredibly powerful tool for conducting business electronically. Companies have taken the proactive approach and are jumping on the new way to conduct business (Lubbe 2003). E-business enables organizational change and conduct business with improved efficiencies and productivity. Many people are earning their lives through working from home and this is an easy way to work thanks to the coming of internet.

E-business is indeed emerging as the next generation business opportunity. The global development and acceptance of the internet as standard for communication and commerce provides us a powerful new global internet-based e-business network that is projected to drive billions of dollars in revenues and dramatically reduce the costs of conducting transactions online(Warren D. Raisch,2000). Organizations are staking their claims in a market that will be measured not only in billions but trillions of dollars.

2.2. E-business legislation in Finland

Finland like any other country in the European Union has substantive controls over electronic agreements concerning privacy. The major concern here is whether the messages will not be altered during transactions (integrity) and how to guarantee authenticity and preserve these messages (confidentiality). In Finland, confidentiality of electronic communication is guaranteed by law.

FICORA (Finnish Communications Regulatory Authority) is the regulatory body in Finland that is concerned with these information interchanges. Its role is to supervise providers of communications services, such as e-mail service operators. The Finnish service providers are bound by law to ensure information security and the confidentiality of communications in the services they provide. The legislation of some countries does not ensure the absolute protection of the confidentiality of communications in the way that Finland's legislation does (FICORA 2008).

One of the recent regulations in Finland in e-business security is the Act on the Provision of Information Society Services (458/2002) that entered into force on 1 July 2002. The Act enforces Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular e-business, in the Internal Market (Directive on electronic commerce). This Directive seeks to promote electronic business in the internal market by ensuring the free movement of information society services between the Member States (FICORA 2008).

According to the law, information society service providers must provide the service recipients with certain information about themselves and their functions. Also, service providers must, prior the consumer makes an order by electronic means, provide them with instructions and information and to provide consumers with means for detecting and correcting eventual errors in orders in advance. Another regulation body similar to FICORA is the Consumer Ombudsman which supervises that provisions of the Consumer Protection Act (38/1978) are obeyed (FICORA 2008).

The law provides how to fulfill the formalities of the contract electronically, and on liabilities of service providers offering delivery and storage services for electronic data concerning the unlawful contents of the data it forwarded or stored (FICORA 2008).

There also other laws in Finland intended to make ensure trust and security in transactions between parties. Among which include: Sales of goods Act, transactions pertaining to property Act and Electronic signature Act.

2.3. Characteristics of E-business transactions

E-Business is one of the highest growing form of businesses in the world today. It entails a great number of e-transactions between firms and individual customers. E-business transactions involve the exchange of information, goods, services and solutions across the internet. E-business transactions need secure applications to support transfer of information between different business entities. These applications are meant to support up-to-date valuable information and enhancing e-collaboration between the firm's suppliers.

E-business transactions can be perceived to encompass three broad categories: Intra-business, Inter-business (B2B) and B2C transactions (Kalakota & Whinston, 1997).

E-business transactions are characterized by the exchange of valuable information across the internet. Historically companies have trusted paper or ‘hard copy’ documents when trading with one another. This has slowly been overtaken with direct system-to-system messaging. This is particularly the case for suppliers to retail outlets such as supermarkets or large retail stores.

The EDI is a typical two-way electronic messaging (EDI) exchange that takes place to facilitate the B2B transaction i.e. Purchase Order, Advanced Shipping Notice, Goods Receipt and Invoice.

A need for more quick and streamlined financial processes has rendered Electronic business a necessity. Accounts and billing information can be made available over the internet to partners and suppliers and orders and payments generated electronically. This potentially facilitates the expansion and development of new linkages across the

globe and enabling the sharing of information and knowledge with other partners (El-Mashari 2002)

E-procurement is yet another important aspect of business across the web: The ability to purchase all your firm's needs from a single portal offers logical time and money savings benefits. Typically, an e-procurement system allows authorized users to purchase products from specific suppliers where supply contracts have been negotiated by their firm’s procurement team. These systems are designed to streamline a company's purchasing processes by placing and approving orders and arranging delivery thereby eliminating many paper-based procedures and labor-intensive processes (Dale, 2001).

Business links across the web make e-marketing possible. Firms are placing their advertisements across the web. Firms no longer have to depend on newspapers to advertise but can use the internet to accomplish their marketing objectives. The use of e-mails has over-taken phone calls. When a firm wants to inquiry about given commodities, the e-mail service is so quick and cost-effective.

3 INFORMATION SECURITY MANAGEMENT

3.1 Definition of information Security

There is much debate in the information world regarding the proper definition of information security. First of all, Security is the process of maintaining an acceptable level of perceived risk (Gary Stonebumer, et al. 2002): That is to say security looks at four major pivotal issues such as likelihood, threat-source, vulnerability, and impact of the security attacks to the information system. Information security refers to securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization. It deals with the prevention and detection of unauthorized actions by users. It includes confidentiality, and integrity and availability of information.

Customers need to assurance that they can trust the company's servers, employees or even websites. When some one for instance uses a company website to make transactions, this means he/she has the willingness to be vulnerable to the actions and results. This shows the trust the consumers have in the company.

Consumers expect that the e-vendor will treat the consumer's information fairly (Shankar et al. 2002). In recent years, privacy and confidentiality have become enormously important in e-business transactions; laws have been enacted to deal with real and perceived dangers arising from use and transfer of consumers' personal data across the web. In the EU for example, the Privacy Directive also known as EU Data Protection Directive was developed and enacted in 1990 to protect the personal information of EU citizens against loss/theft, unauthorized access and disclosure.

As business tends to go internet, companies are becoming more sensitive on the security of their transactions with other parties and therefore a greater need for them to know the value of the data transferred across the web. This implies that people, companies and their staff plus other parties involved have to know the information and the value of that information in order to develop protective measures. There is also a greater need to know which individuals/parties need unique identities and how much information may be divulged to the outside world.

3.2 Importance of Information Security

Information Security is an important aspect that enables the full exploitation of the Internet for e-business. Online consumers and other business actors like suppliers, partners require maximum information security from the firms. Ensuring maximum information security possess a great challenges to many firms in terms of data protection and enabling secure partitioning of data access by customers, suppliers and other users, while supporting secure data sharing among communities of interest.

The development and successful deployment of e-business applications requires carefully engineered and comprehensive security solutions. Such solutions must address all aspects of system security at the platform, operating system, network, application and infrastructure levels. The key issues pertains the physical security (secure servers, hardware), data storage, data transmission and exchanges between business parties, system administration and authentications (Thomas J. Watson Research Center. 2010).

According to the Internet Security group at IBM's Thomas J. Watson Research Center, Information security involves development of new cryptographic techniques and algorithms, their secure implementations, the design of secure networking protocols and operating environments and mechanisms to monitor and maintain overall system integrity. Such security solutions need to be standardized to provide/preserve inter-operability and to ensure that these techniques are used in a correct way.

In traditional office environment of any firm, any access to sensitive business information is through employees. Employees are not always reliable, so firms need limit access to sensitive information to specific employees and also enforce physical and procedural

controls of this information. With the escalating number of internet users, it is quite hard now days to deter users from accessing companies' information and therefore it is important that companies manage access to sensitive information and prevent unauthorized access to that information before it occurs.

With the greater need for secure transactions, the cost of providing and maintaining security needs has also increased. Information Security is highly needed in maintaining and creating trust amongst parties. Understanding consumers' views on trust, risk, privacy and security is much important than technology in e-business today (Pennanen et al. 2008). Secure e-business transactions offer potentially unlimited opportunities for increasing efficiency and reducing cost and thus profitability, lead to long time relationships between two or more trading parties.

3.3 Key features of Information security

Information security is aimed at prevention, detection and solution measures to data loss, damages and intrusions. To ensure this, there is need for an advanced security that enhances information security from data processing to data transfer involved in online transactions. The purpose of this is mainly to counter information security attacks before data loss occur in order to reassure consumers that they can make e-business transactions that are safer.

According to Gollman, 1999, Information security consists of three main parts: Confidentiality, Integrity and availability (CIA):

Confidentiality refers to limitations of information access and disclosure to authorized users and preventing access by or disclosure to unauthorized users (ISO/IEC, 2004: Parker, 1998). This means that sensitive information should be kept safe from unauthorized users by allowing access to only those individuals for whom the information is intended to. When carrying out e-business transactions, e-vendors are obliged to keep consumers' information confidential by allowing only authorized users to access it.

The concept of integrity refers to prevention of erroneous modification of information. This is aimed at ensuring that information remains accurate for its purpose (Parker, 1998). It means that only authorized users are able to modify the information and only in a way that it stays available and accurate. Measures need to ensure the trustworthiness of information resources through protecting it from malicious attackers that can modify, delete, or corrupt information. However, the company has to protect information from authorized users too, because they can cause errors and omissions and the alteration of information.

Availability relates to the ease of access to information resources when needed by those who need it. Online buyers require for steady availability of information on company websites all the time and therefore a challenge to the e-vendors to maintain systems that allow for those who need information to access it.

In order to ensure confidentiality and integrity, other security features of Authorization and Non-repudiation are important. Authorization means that only authorized users access the sensitive information. These authorized users should also verify that they are who they claim they are (authentication). Non-repudiation also work hand-in-hand with integrity to ensure that the authorized user can't deny what he/she has done. In other words, the user is accountable for what he/she does (Xianping Wu, et al. 2009).

3.4 Implications of Information security to e-business

Every business transaction represents a set of interactions between business actors. The goal is to initiate, arrange and complete a contractual agreement for exchange of goods, services, solutions, information and funds. The business actors are involved in an agreement that is aimed to benefit both parties and therefore much care is needed to successfully carry out the transaction and also maintain the relationship for further gains.

With information security the leading focal point in e-business transactions, firms seek to make dealings in an atmosphere that doesn't undermine the agreed terms and conditions. Many parties fail to meet the agreed standards which in the end undermines the trust one

party has in another. Firms need to know that information security measures need to be put in place to maintain trust between their partners.

The mistake firms make is trying to neglect the information that is deemed confidential to non authorized workers. Several cases have been reported for example in North Korea in September 2008 by the Cyber Terror Response Unit, a police unit in charge of online crimes about two compact discs that were leaked from GS Caltex. According to The Hankyorey, sept 6 2008, these CDs contained personal information for more than 11 million people. Other cases about master cards have been so evident in recent years and many businesses and individuals have lost lots of Euros. The problem is the failure for the providers of these services to distinguish between which employees have access to which information and to what extent they can be trusted. Realizing the role of information security becomes apparently important in e-business transactions.

Businesses are able to develop trust and loyalty with trading partners. A favorable attitude and commitment towards electronic business results in repeat purchase behavior. Both parties are able to realize more profitability, longtime B2B and B2C commitment and reduced costs of acquiring new customers. Each party feels secure throughout the transaction process because there is guaranteed flow of information and secure acquisition of data on both the sending and receiving ends.

Information security is deemed important in inter-dependencies between business and legal requirements, for devising the goals and objectives that are relevant to the company. Failure to exercise the diligence in information security may lead to loss of further business opportunities and revenue, erosion of the company’s reputation/brand to the outside world and scrutiny from consumer advocates and lawsuits.

4 CASE: ORGANIZATIONS' AWARENESS ON KEY IT SECURITY AREAS

4.1 Introduction of the case

The case was conducted in two ways;
The questionnaire was prepared (Source: Senthil A. Thangarajan, 2006). These questions are made simple and few, in order to encourage the participants in the case to contribute and dedicate their time. I made inquiries first before I presented the questionnaire through personal contact and e-mails requesting for a meeting with each participant to present the questionnaire. The questionnaire had 21 questions which are constituted day-to-day security practices in organizations. Alongside the questionnaire, an interview was requested from the participant. Unlike the questionnaire that was targeting both all the participants (Managers and IT support staff), not all the interview questions applied to both.

The questionnaire and interviews in the case were based on the following security areas as a ccording to International Organization for Standardization(ISO). i.e www.iso.org

- Security policy
- Organizational security
- Asset classification and control
- Data protection
- Communication and operational security
- Access control
- Compliance/flexibility within the organization
- Physical and environmental security

Information security awareness among organization's managers and employees is analyzed based on different information management practices in organizations. The

above-mentioned security areas are based on the ISO/IEC 17799 security standards. ISO/IEC 17799 is the international standard that takes a broader view to Information Security. ISO/IEC 27002 standard is being used by many organizations in the world.

4.2 ISO/IEC 17799 Standard

The ISO/IEC 17799 standard is a code of practice for Information Security. It came into place in 2005 as one of the s Information Security Management System standards released every year by International Organization for Standardization (ISO). ISO/IEC 17799 Standard was designed to establish guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The standard was intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities (Praxiom Research Group Limited, 2010)

The structure of the ISO/IEC 17799 contains the following domains i.e. Security policy, Organization of Information security, Assets classification and control, Personnel/Human resources security, Communication and operations Management, Access control, Physical and environment security, Information Systems development and maintenance, Information security incident management, Business Continuity Management and Compliance(ISO, 2010)

4.2.1 Security policy

A Security Policy is a set of objectives, rules of behavior for users and administrators, and requirements for system configuration and management that collectively are designed to ensure security of computer systems in an organization. In other words it is a document that states in writing how a company is planning to protect the company's physical and information technology assets. It is usually referred to as a ‘living

document' meaning, it is never finished, instead is continuously updated to cater for the changing security needs of the organization. It should be a guideline to all IT-related aspects from the grass-root level and therefore need to be understood by all workers.

An organization's security policy is a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

This document is so instrumental to the wellbeing of the entire organization and therefore need to be supported at all levels of the organization. It may include the following security aspects: virus detection and prevention, password use and management, access control rules, physical security, firewall use and configuration, procedures for granting and revoking system access and many more.

4.2.2 Organization of Information security

This is an insider security issue in the organization. As the Organization prepares to earn profits and have a competitive position, proper procedures for approval of acceptable use policy throughout the organization have to be ensured. This entails risk assessment procedures, business continuity panning, security awareness and reviews.

5.2.3 Asset classification and control

In order to maintain appropriate protection of organization's security, assets need to be classified and accounted for. The classification is based on the nature, relative value and importance of these assets. This is important in providing necessary security for these assets commensurate with the value and importance of these assets. According

the Praxiom Research Group Limited 2010, Information system assets may have different classifications as shown in the table below;

Table1

Number	Classifications of Assets	Examples of Assets
1.	Information assets	Database and data files, user manuals, System documentation, continuity plans, training manuals etc.
2.	Software Assets	System and application software, Develoment tools and utilities
3.	Physical/Hardware Assets	Computing Equipments, Communication equipments like phones etc.
4.	Services	Computing services, Communication services etc.
5.	Intangible Assets	Organization's reputation and image
6.	Personnel	Skills and experience

After the organization has clearly classified these assets, assignment of responsibilities to these assets is made. This means that all assets are accounted for and have a nominated owner to ensure that appropriate protection is maintained. The owner is thus responsible and accountable for controlling these security assets.

4.2.4 Compliance

This is an act of adhering to regulations/laws. As an important aspect of security, the organization has to make sure that it follows the national and international IT regulations/laws pertaining copy rights, handling personal information, dealing with disputes, software use and handling and many others. In the IT sector, Organizations have to follow the ISO standards, who set up standards, procedures and processes for all organizations involved in e-business transactions.

4.2.5 Human resource/Personnel security

In accordance with the Commonwealth of Virginia (COV) Information Technology Resource Management Standard (ITRM), COV ITRM Standard SEC2001-01.1, Personnel security must be an integral part of a VCCS Entity's information technology security plan. Personnel security reduces the risk that key information technology assets will be compromised by securing all VCCS systems and related data to access by authorized personnel only. And as a directive from COVITRM and ISO, Organizations have to make sure that personnel security safeguards are applied.

As a characteristic of all humans, negligence and human errors are so common and this need to be avoided when handling sensitive data and therefore a need to ensure that organization's staff has the necessary competence to use information processing facilities correctly. In case they lack the competence, specific security and procedures-related training should be given. Logins and access to a certain resource or information need to be safeguarded from both insiders and outsiders in order to avoid fraud, loss, misuse, modification or disclosure of sensitive information.

4.2.6 Business continuity management

Organizations need to develop and implement business continuity plans to avoid/mitigate disasters before they happen (Andrew Hiles 2007). Identifying these events that may cause harm to the business is an important aspect in ensuring both technical and physical security. And as a plan is being implemented, regular updates,

tests and reviews should be made to the plan to ensure that it goes hand-in-hand with the changing security needs.

4.2.7 Access control

This is yet another important aspect of information security. It has existed as long as humans have has assets to protect (David Ferraiolo et al. 2003). Access control takes many forms and apart from determining whether the user has rights to access a given resource, it may constrain how and when the resource may be used. By use of the three major categories of information technology i.e. Confidentiality, Integrity, and Availability (CIA), Organizations can monitor that sensitive and confidential information such as passwords, customer IDs and data, are accessed in its originality/modified by those claiming authority to use and can be available when needed.

4.2.8 Information System development and maintenance

This involves the development, implementation, enhancement and maintenance of the hardware and software aspects of the system. In the development phase, the system developer has to start with identifying the system security requirements those new information systems, new software packages, business, infrastructure and user-developed applications, enhancements to the existing system must meet. The controls that new information systems, new software packages, enhancements to the existing system should have.

4.2.9 Communication and operations management

This is yet a key a key element in keeping the Confidentiality, integrity and availability of sensitive information. It is therefore the organizational responsibility to establish procedures and responsibilities protect against malicious attacks by third party users. This can be through exchange information for instance via vulnerable media such as e-

mails, telephone and computer intranets/extranets. Organizations need to carry out system planning activities, establish backup procedures to information and software, protecting and controlling computer networks and monitoring information processing facilities (ISO-27002:2005).

4.2.10 Physical and environmental security

Identify the main physical areas to be protected and provide access control to restricted areas from unauthorized access to the company premises. This involves designing physical security perimeters to protect data, core network facilities like offices, cabling and equipment rooms, laptop computers, Personal Digital Assistants (PDAs), smart phones, external hard drives and USB flash drives from natural and human threats.

This can be done through designing entry IDs, electronic keys and providing entry codes to workers and authorized users. This can also be done by ensuring safe power and communication cables, isolating public access, identifying which staff /external contractors have temporary/permanent access to the premises and facilities. It is also of paramount importance to protect off-site facilities like laptops, backup CDs, USB flash drives which may be vulnerable to theft and copying of sensitive information.

5.0 CASE RESULTS

The case was carried out in different kinds of organizations in Salo City region. There were a total of 10 respondents from 10 organizations, seven of which were IT support personnel and three managers.

The case results were collected through interview and questionnaire. The interview questions and questionnaire were based on the ten ISO/IEC 27002 domains. Though the areas covered were the same, different aspects under these domains were targeted in the interview and questionnaire.

A total of 6 IT support personnel and 2 managers accepted the interview, 2 respondents including a manager and an IT support personnel were not available at the premises but responded through the questionnaire. The respondents who participated in the direct interview also filled the questionnaire. A given period of time was given to the respondents to complete the questionnaires and 3 of them were returned through e-mail, 2 through post and 5 were collected from the Organization premises.

The interview and questionnaire targeted employees, managers and awareness on the key information security issues but less was achieved from the employees other than the IT support staff. More than 15 employees contacted first were referring me either to managers or IT support staff, which seem to indicate that they knew less about information security issues. They also appeared less concerned and responsible for security of the information they handle in day-to-day work.

5.1 Security policy

Through the Questionnaire, respondents who had IT security guidelines in their organizations totaled to 5 with 3 of them having no security guidelines and 2 did not know whether their organizations had IT security guidelines or not. Among the 5 who

acknowledged having IT security guidelines, all of them understood them, 3 of them practiced them regularly while one followed it strictly and another followed it sometimes.

Among the 8 organizations which were represented in the interview, 6 of them of were subsidiary organizations and 3 of them were actually from the same parent Organization, which means they followed the security guidelines set up by the parent organization. Only 2 of the respondents interviewed represented organizations which were not subsidiaries but one of them was a parent organization, which means it had some other organizations that operate under it.

5.2 Organization of Information security

According to the case results, 4 organizations conducted IT security awareness programs for employees and 6 of them had no training at all for their employees. Among the organizations which had these programs conducted, 3 of them conducted the programs within a period of one year and only one of them conducted the training in a period more than a year. When asked who was responsible for Information security matters, all respondents who took part in the interview answered that it was the IT Support Personnel.

5.3 Assets classification and control

A few questions were asked to find out how Organizations classified assets and who was responsible for the different assets in their organizations. The possible classifications of these assets were availed in the questionnaire and each classification defined. The results were:
4 organizations considered the company telephone directory as an open asset meaning that it can be accessed by insiders and outsiders of the organization, 5 organizations considered their company telephone directory as an internal use asset

available for inside use which means that it is only while one organization considered it confidential, with a few groups in the organization able to access it.

When it came to customer records, one organization considered it an open asset, 2 organizations considered it an internal use asset, 3 organizations viewed the customer record as a confidential asset while the other organization considered a customer record a restricted asset.

The company's strategic plans were considered an open asset by one organization while 3 Organizations valued it as an internal use asset. 5 organizations considered the company's strategic plans as confidential while the rest considered it a restricted asset.

The press release was considered an open asset by all the 10 organizations. It was not clear if all employees or their Organizations really knew how to classify their assets correctly because all respondents answered what they thought were the right answers.

5.4 Personnel/Human resources security

With the personnel aspect of security, the analysis was based on the interview of which only 8 respondents took part. When asked the measure these organizations used to ensure that new staff had necessary competence to handle IT facilities correctly, all organizations noted that they always require some basic IT skill. The organizations also take responsibility to provide further training in management of facilities and IT security awareness when they get recruited.

5.5 Communication and operations Management

To find out what measures the employees and organizations had in place to cater for security breaches and attacks, respondents were asked to answer the following questions:

If you see some breach in Security policy, what will you do?

- Try to fix it by myself.
- Send a report to a Team Leader/ Administrator

- I will only concentrate in my work.

Have you ever experienced a security breach?

Hint: External act that bypasses or contravenes security policies, practices or procedures.

- Yes
- No

If yes, what you did?

- You fixed it by yourself.
- Reported to a Team leader/ Administrator
- No action.

According to questionnaire results: When asked what they could do incase they experiences a security breach: 7 respondents could try to fix them themselves and all those who gave this answer were all IT security personnel, 3 respondents could call for help from IT security personnel. 6 out of the 10 respondents had experienced security breaches while 4 had not received any cases of security breaches.

Among the 6 who had experienced these breaches, 5 of them were IT security personnel and acknowledged having also received several complaints of the same kind from employees and managers in their organizations. Only one respondent who was a manager accepted having experienced a security breach and could not fix it himself instead had to call for help from the IT security personnel.

5.6 Access control

As organizations are responsible for keeping information safe, access to such sensitive data need to be safeguarded from unauthorized users. In order to know if these organizations had control of the logins in their systems, the following questions were asked;

Are you instructed to change your account login password at certain times?

- Yes

- No

How often do you change your account login password?

- Monthly once
- Once in 2 months
- Once in 6 month
- More than 6 months

What do you do when you leave your workstation?

- Logoff/Lock the system even for short break like coffee breaks, toilet breaks etc
- Logoff/Lock the system only for a long break like lunch breaks, meetings etc
- Logoff only when I go home.
- No one will use my system when I am in office, so I leave as it is

According to the questionnaire results: All the ten respondents from the 10 organizations accepted requirement to change their passwords at certian times and when asked how often they change these passwords, 5 respondents change are required to change their passwords on a monthly-basis, 2 respondents change their passwords once in two months, one respondent is required to change the password once every half a year(6 months) while 2 respondents change their passwords with in a period more than 6 months. However, one respondent added that they do not require travelling users to change their passwords.

Respondents were also required to answer questions concerning logoff when they are in or out of their work stations: 6 of them logoff their systems even for a short break like coffee breaks or toilet breaks. This means that they were more sensitive to unauthorized users accessing their systems even within limited period of time and 4 respondents could only logoff when they were going for long breaks like lunch breaks or meetings.

From the interview part on this issue: In 4 organizations, passwords are issued to employees and managers with cards while in the other 4 organizations, passwords have to be personally selected, though in accordance with certain instructions and guidelines on how their passwords should look like and what they should contain. In

the organizations where passwords are made by the employees themselves, the strength of these passwords is highly valued and have to be accepted by the system which guarantees whether the password meets the given guidelines or not.

6 CONCLUSION

As the world continue to widen as a global village, internet-use is becoming increasingly important to Organizations and its customers. Information Security is now at the heart of every transaction between the trading parties. From the thesis case study, it was clear that there is need for Organizations to attach more value to information security.

The main objective of this thesis was to describe and analyze organizations' role in maintaining their e-business trust and partnership by putting attention to the information that is transferred across the internet. This was achieved by looking at the key security areas. The objective was achieved after analysis of the results which showed that there is need for management to emphasize the role of information security in their organizations and there fore need to be careful and responsible knowing that a few mistakes can spoil the security system and thus lose customer trust during the transaction process.

Among the organizations in question there were signs that workers needed extra education on the key security areas and their role to information security in e-business transactions. The moment the leaks appear in the security of useful information, the more hackers are able to break into this information. Almost 7 of the employees involved in the study, didn’t know that they are also responsible for information security-related issues in their organizations, meaning that they were not concerned.

A clear security policy is needed to the employees in organizations, and this security policy need to be understood by all workers and managers. Employees need to know their collective and individual roles in handling the basics in this security policy and also have incident handling skills such that they have an idea on what do incase they are faced with security breaks/breaches on their computers. They should also know how to avoid these security problems happening through keeping their passwords well, report any signs of security breach, guard their offices to avoid unknown people from getting to their computers, backup their files, running antivirus software, etc.

Organizations need to have an IT disaster recovery planning such that lost information can be recovered. For instance backups and restoration processes need to be well scheduled and managed and also ensure that these backup media/devices are kept in secure places on and off the site. IT support staff should employ the necessary countermeasures to ensure that the right people get access to the sensitive information. For instance; constantly review those people allowed to access the sensitive IT systems.

Another important suggestion is encryption of data: this allows security of confidential data from non-authorized people from reading it. This is important in protecting data kept on laptops, USB flash drives or even data in that can be accessed through Bluetooth, wireless phones etc. from being hacked into and also incase of hacked, the hacker find it difficult to read the data.

Because of the sensitivity of the information security, I encountered a few problems during the case study. The biggest percentage of the employees who were my major target referred me to their IT support staff. Some of them even didn't know how far they are responsible for Information security (Others, if there was any). Another reason for referring me to the IT support was the fact that many employees had less knowledge on Information security, meaning they needed more education and regular awareness programs at least twice a year, acknowledging the value of the information they handle in their daily work thus employing a more-responsive approach to any situations that can undermine the confidentiality of customer data.

Managers too did not want to let out information about their information security systems, which on another hand was a sign that Organizations were responsive to information security attacks. I found it difficult to administer questionnaires and many were not returned and less was told through the interviews. Analsis of the data was also a bit difficult since a few organizations were put into conderation.

In future, more use of internet will instill its own challenges because every aspect of human living will be controlled by the master of the digital business i.e. the web. Therefore Organizations, consumers, governments and all concerned parties will have to step up and work together to protect sensitive information. As the growth in number

of online shopping and online information transfers go up each day, as the number of defaulers ready to take advantage of the loopholes in the use of the internet. Organizations still have a lot to do to protect their image by ensuring safer transactions in attempt to increase market share and have a competitive edge over others in this increasingly competitive business world.

REFERENCES

Commonwealth of Virginia (COV) Information Technology Resource Management Standard. 2008. http://inside.southside.edu/security/documents/COVITRMStandardSEC501-01rev4.pdf. Retrieved 21.3.2010.

Neef. Dale 2001. E-procurement From Strategy to Implimentation. Prentice Hall,Inc.

David F. Ferraiolo, D. Richard Kuhn, R. Chandramouli 2003. Role-based access control, Artech House, Inc

Turban, Efraim et al. 2002. Electronic Commerce 2002: A managerial perspective. Pearson Education, Inc.

Majed, El-mashari. 2002. Electronic commerce: A best practice perspective. Emerald Group publishing Limited.

Farlex, 2010: Internet, The free Dictionary http://encyclopedia2.thefreedictionary.com/internet

FICORA. 2008. http://www.viestintavirasto.fi/en/index.html. retrieved 20.09.2009

Stonebumer Gary, Alice Goguen & Alexis Feringa. 2002. NIST Special Publication: Risk Management Guide for Information Technology Systems. Booz Allen Hamilton Inc.

Gollman, D. 1999. Computer Security, John Wiley & Sons Publishing.

Hauben, Michael.2007. History of ARPANET: Behind the Net-The untold history of the ARPANET.

Hiles, Andrew. 2007. The Definitive Handbook of Business Continuity Management, Second edition, John Wiley & sons Ltd

International Organization for Stardardization(ISO) , 2010 www.iso.org

Thomas J. Watson Research Center. 2010. Internet Security group. http://www.research.ibm.com/intsec. Retrieved 06.05.2010.

O'Brien James A. & George Marakas, 2008. Introduction to information systems, 14th edition Irwin/McGraw-hill publishers.

Bosch Jan & Morven Gentleman. 2002. Software Architecture: System Design, Development and maintenance, Kluwer Academic Publishers Group.

Kalakota & Whinston, (1997). Electronic Commerce : A manager's Guide. Reading Massachusetts: Addison-Wesley.

Pennanen, Kyösti & Minna-Kristiina Paakki. 2007. A Qualitative Analysis of Consumers' Perceptions of the Trustworthiness of e-Commerce.

Internet. http://en.wikipedia.org/wiki/Internet. Retrieved 20.01.2010.

Väkiparta, Iikka. 2004. Seminar on Internetworking: Security of Inter-Autonomous Systems Routing. Helsinki University of Technology.

Mimoso Michael S.. 2002. "Security news"- Common security mistakes still haunt enterprises.

http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci857890,00.html. Retrieved 20.03.2009.

Krause Micki, Harold F. Tipton. 1997. Handbook of Information Security Management. http://www.cccure.org/Documents/HISM/041-044.html. Retrieved 13.04.2009.

Parker, D, B.1998. Fighting Computer crime - A New Framework for Protecting Information, United States: Willy Computer Publishing.

Raisch, Warren. 2000. E-marketplace: Successful Strategy in B2B E-commerce. McGraw-hill Professional Book Group, New York City.

Robert, Westervelt. 2003. “SQL Server news”: Common Security mistakes. http://searchsqlserver.techtarget.com/news/article/0,289142,sid87_gci1052719,00.html

Saarinen, T, Tinnilä, M, e tal. 2005. Managing Business in Multi-channel World: Success factors for E-business. Idea Group Publishing, London.

Samuel Greengard. Six common IT security mistakes and how to avoid them. Retrieved 06.04.2009. http://www.microsoft.com/uk/business/security/securitymistakes.mspx

Shah, Shreeraj. 2007. Web 2.0 Security: Defending Ajax RIA and SOA. Course Technology.

Shankar, V, G.L. Urban and F. Sultan. 2002. Online trust: a stakeholder perspective, concepts, implications and future directions. A journal of Strategic Information Systems.

Braithwaite Timothy. 2002. Securing E-Business Systems: A Guide for Managers and Executives.

The Hankyoreh, 2008. http://english.hani.co.kr/arti/english_edition/e_national/308826.html

Tyson, Jeff. 2008. How Internet Infrastructure Works http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm

Praxiom Research Group Limited, 2010. Information Security Standard. http://www.praxiom.com/iso-17799-2005.htm Retrieved on 20.10.2010.

Zorayda, R, Andam. 2003. E-Commerce and E-business. E-ASEAN Task Force, UNDP-APDIP.

Sherif, Kamel. 2006. Electronic business in developing countries: opportunities and challenges. Idea Group Publishing, UK.

Val Thiagarajan B.E. 2003. Information Security Management. http://www.sans.org/score/checklists/ISO_17799_checklist.pdf.

"World Internet Users and Population Stats". Internet World Stats. Miniwatts Marketing Group. 2009-06-30. Retrieved 06.11.2009.

Xianping Wu ,Huy Hoang Ngo, et al. 2009. International Journal of Computer Science and Applications. Technomathematics Research Foundation Vol. 6, No. 3, pp 57 – 74

Appendix A

Instructions: Make a cross (×) on your option.

(I) Security policy

1. Do you have IT security guidelines in your organization?
   - Yes
   - No
   - I don't know
   -

   If yes continue, if No, skip Q2 and Q3

2. Have you read and understood it?
   - Yes, I understood
   - No, I haven't read
   - I didn't understand

3. How often do you practice it?
   - I follow it rarely
   - I follow it regularly
   - I follow it strictly
   - sometimes I follow it

(II) Organizational security

4. Is there any IT security awareness-training programs conducted in your Organization?
   - Yes
   - No

5. How often is it conducted?
   - Every 6 months or less
   - Every year
   - More seldom than a year

6. Have you ever undergone any security awareness training programme/seminar within this organization or at any other organization?
   - Yes
   - No

(III) Asset classification and control

Organization Information assets can be classified in any one of the following:

·□Open/Public - Available open to all in and out of Organization.

·□Internal use - Available only for organization internal use.

·□Confidential - Confidential within certain groups/team in an Organization.

·□Restricted - Highly confidential with in very few inside the organization.

According to the above four classifications, please answer your view of asset classification for the following questions 7, 8, 9&10

7. The Company telephone directory is _ _ _ _ _ _ asset.
   - An open
   - Internal use
   - A confidential
   - A restricted

8. The customer record is _ _ _ _ _ _ asset.
   - An open
   - Internal use
   - A confidential
   - A restricted

9. The company Strategic plans _ _ _ _ _ _ _ asset.
   - Open
   - Internal use
   - Confidential
   - Restricted

10. The press Release is _ _ _ _ _ _ _ _ _ _ asset.
    - Open
    - Internal use
    - confidential
    - Restricted

(IV) Data Protection

11. Do you back up your work externally to discs/tapes/or by some other secondary memories?
    - Yes
    - No

If yes, please continue If No skip Q12 to Q13.

12. How often?
    - Every day
    - Every week
    - Every month
    - Every 3 months

13. Where do you store those back up discs/ tapes?
    - Same place where my working area is located.
    - Same building where we work but in different room.
    - In different building
    - I don't know

14. Who have access to the room where the backup discs and tapes are stored?
    - Team Leader
    - only administrator
    - everyone
    - I don't know,

    Other: _ _ _ _ _ _.

15. Who is responsible for preventing the organization from IT security attacks?
    - The IT Administrator

- The Team Leader
- The whole team
- A Security device

Other: _ _ _ _ _ _.

(V) Communication and operational Security

16. If you see some breach in Security policy, what will you do?

- Try to fix it by myself.
- Send a report to a Team Leader/ Administrator
- I will only concentrate in my work.

17. Have you ever experienced a security breach?

Hint: External act that bypasses or contravenes security policies, practices or procedures.

- Yes
- No

18. If yes, what you did?

- You fixed it by yourself.
- Reported to a Team leader/ Administrator
- No action.

(VI) Access control

19. Are you instructed to change your account login password at certain times?

- Yes
- No

20. How often do you change your account login password?

- Monthly once
- Once in 2 months
- Once in 6 month
- More than 6 months

21. What do you do when you leave your workstation?

- Logoff/Lock the system even for short break like coffee breaks, toilet breaks etc
- Logoff/Lock the system only for a long break like lunch breaks, meetings etc
- Logoff only when I go home.
- No one will use my system when I am in office, so I leave as it is

(VII) Compliance / Flexibility with in organization

22. Have you ever used your colleague's system when he is logged in?

- Yes sometime with his permission
- Yes sometime without his permission
- No, I will always login with my account

(VIII) Physical and environmental Security

23. Do you have an identity card to enter in to the office?

- Yes, I always show it or use it when I enter the office
- Yes, but I only show it if someone asks me
- No, I don't have one.

24. What do you do when a stranger walks in to your office working area?

- Escort the stranger and complete his work in lobby and will not allow him in the working area
- Politely ask the stranger about him
- Ask for his visitor identification badge
- I will do my work and don't care about the stranger.

The interview questions were based on

1 Security Policy

1. Is the business a subsidiary of a larger group?	YES / NO
2. If so, where are the headquarters?	
3. Do you consider that Information Security has the active support of your Managing Director or Chief Executive?	YES / NO
4. Name?	
5. If not, does it have the active support of a main board director?	YES / NO
6. Position of that board member	
7. Name?	
8. Has the board set a policy for Computer Security?	

9. Is there a copy of the Policy available for all employees?	

2 Security Organisation

1. Who is the budget holder for Security Issues?	
2. What is the size of the budget £	
3. Number of Staff	
4. How often does the board receive reports on security issues?	
5. Which individual in the company is responsible for Information Security?	
6. What proportion of their time is devoted to this job?	%

7. When was this manager appointed?	
8. What was their previous role in the business, if any?	

3 Asset Classification

4 Personnel Security

1. Describe the measures to ensure that staff have the necessary competencies to ensure that they can use the Information Processing facilities correctly and effectively	
2. Describe what steps are taken to assure the trustworthiness of staff	

3. Is there an acceptable use policy?	YES / NO
4. What policies are in place to control the unauthorised use of the IP facilities by staff and to prevent the installation of unauthorised software or data.	
5. Who is responsible for the instruction of staff in incident recognition and general security issues?	
6. What steps have been taken to ensure that users are aware of information security threats and concerns in general and acceptable use in particular?	
7. Describe the communications procedures for ensuring that security matters are kept at the forefront of staff awareness.	

8. Have users been given specific training related to security and related procedures?	
9. What penalties exist for the breach of acceptable use?	
10. What procedures are in place to check servers and workstations for compliance with acceptable use?	
11. Have users been instructed in the procedures for dealing with a security breach?	YES / NO
12. Describe the process whereby the lessons learned from any security incidents can be used to improve security procedures.	YES / NO

5 Physical and Environmental Security

1. How is physical access to the Company's premises controlled?	
2. If staff carry ID or access control items what measures are taken to prevent and detect theft or forgery?	
3. What classes of external staff have temporary or permanent access to the premises?	
4. Where external contractors have access to the premises, how are their activities controlled and supervised?	

6 Computer and Network Security

7 System Access Control

1. How are legitimate internal users of the system identified?	■ account name / password ■ biometrics ■ other
2. describe the hierarchy of system	■ root

access	■ manager ■ user group 1 ■ user group 2 ■ etc
3. How are passwords issued?	
4. Describe the process for removing system access from ex-employees etc.	
5. How frequently are passwords changed?	
6. Are audit logs kept for the purpose of detecting security breaches or challenges? Where are these logs stored and how are they analysed?	YES / NO
7. Describe any specific measures designed to prevent unauthorised access.	

8. Describe how any successful or unsuccessful attempts at unauthorised access will be detected.	

9. Describe any specific measures to ensure security when using mobile computing and tele-networking facilities	

10. Is the system accessible via the internet?	YES / NO

11. Describe anti - virus provisions for gateways, servers and workstations.	

10 Compliance

1. Are the Company's Information Processing operations subject to any criminal or civil law statutory or regulatory requirement?	
2. Which laws and regulations apply?	
3. Describe the measures taken to ensure that software licensing conditions are adhered to.	
4. Are the Company's operations subject to other contractual requirements?	
5. Specify other contractual requirements	
6. Is the company certified under any recognised quality standard (eg ISO 9000)	