HACER TUGBA EROGLU

SELCUK UNIVERSITY, TURKEY

HAYRIYE SAGIR

SELCUK UNIVERSITY, TURKEY

,

THE NECESSITY AND FUNCTIONALITY OF INFORMATION MANAGEMENT SAFETY: A CASE ANALYSIS IN TURKEY PERSPECTIVE

Abstract:

Today, the use of information is gradually increasing in private sector and public sector. Besides that the importance of information increases, keeping and storing it in a safe way also appeared as an important need. Also, transferring it from one place to another place became inevitable need. This dependency to information made a current issue the need of keeping information. The attacks to information, its destroying, its cleaning, and being damaging of its confidentiality causes informational infrastructure to fall into decay and this, together with it, also leads the things to go wrong. Thus, the safety of information system gradually becomes more important. However, in information age, taking information under control gradually becomes difficult. Making the information flow more safe, from now on, has become a policy of governments. On this purpose, Information Safety Management System was developed. Informational Safety Management System is a systematic approach adopted for being able to manage the sensitive information of institute. The main purpose of this system is to keep the sensitive information. The works on this system includes work systems and information technology (IT) processes. Lack of information flow actualizing thanks to various environments in internet threatens the future safety of information. Information is easily obtained without permission. Performing the information circulation through open networks increases the risk. Information Safety Management System includes what kind of actions should be taken toward keeping the easily obtained information and how a policy should be followed.

In this study, in related to information management safety, SWOT Analysis toward what kind of strategy public institutes in Turkey follow will be carried out. Thus, emphasizing strengths and weaknesses on information safety, what the institutes will be able to do will be suggested so that they eliminate their weaknesses. In addition, how the institutes prevented the possible threats and evaluated the opportunities will be included in the study.

Keywords:

Information safety, information safety management system, information technologies.

1. Introduction

The Information Security arena has expanded over recent years-growing from a technical initiative and labelled information security towards a broader, more business focused concern, for the protection of information in all its forms across the organisation. It is no longer simply the aim to protect confidentiality, integrity and availability of information but Information Security aims to deliver real business benefits now by both protecting and yet facilitating the controlled sharing of information and managing the associated risks across a changing threat environment. This change in emphasis means that many more functions within the enterprise have a role to play-some at a general level and some with a specific niche role. Information Security as a concept has developed both breadth and depth and, as it rightly becomes an embedded function in the organisation, it needs the overlay of a strong management system to determine how these aims can be achieved efficiently and coherently (Debi, 2008: 4).

2. Information Security And Key Concepts Of Information Security

Information security is a whole. The different parts of this whole process creates. These parts can be listed as follows:

-Availability

-Privacy

-Identification

-Authentication

-Authorization

-Accountability

Availability: Availability is making information accessible to user access without interference or obstruction in the required format. A user in this definition may be either a person or another computer system. Availability means availability to authorized users (web2.utc.edu/~Li-Yang/.../Introduction.ppt, 2014).

Privacy: Information is to be used only for purposes known to the data owner and this does not focus on freedom from observation, but rather that information will be used only in ways known to the owner (web2.utc.edu/~Li-Yang/.../Introduction.ppt, 2014).

Identification: Identification and authentication are essential to establishing the level of access or authorization that an individual is granted (web2.utc.edu/~Li-Yang/.../Introduction.ppt, 2014).

Authentication: Authentication occurs when a control provides proof that a user possesses the identity that he or she claims (web2.utc.edu/~Li-Yang/.../Introduction.ppt, 2014).

Authorization: After the identity of a user is authenticated, a process called authorization provides assurance that the user has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset (web2.utc.edu/~Li-Yang/.../Introduction.ppt, 2014).

Accountability: The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process (web2.utc.edu/~Li-Yang/.../Introduction.ppt, 2014).

3. Information Security Management

Information security management activities should be driven by organizational objectives so that no resources are expended on security without an explicit documented understanding of how it supports the organizational mission (Choobineh, et al, 2007: 959).

In other words information security management, ‘that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security’. It states that this includes, ‘organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources’. This seems to align well with our previous definition of what management means and its primary aim of configuring resources (Debi, 2008: 4)

4. Process of Information Security Management

Information security management contents with also vary with different researchers and institutions. There are five components for any information security architecture (Hong, et al, 2008: 243):

-Security organization and infrastucture

-Security policy, standards and procedures

-Security baselines and risk assesments

-Security awareness and training programs

-Compliance

Information security managers using this approach will first identify and select the processes to be implemented, such as the screening of new employees, then implement the processes to enable screening. The next step is to check if all new employees are indeed screened. The process is an iterative system with feedback and continuous improvements. The concept of ‘Plan-Do-Check-Act’-PDCA is important when implementing an information security management (Eloff and Eloff, 2003: 131). An effective ISMS is based on the PDCA cycle (Saint-Germain**,** 2005: 63):

Plan (establish): Define the ISMS scope and the organization’s security policies, Identify and assess risks. Select control objectives and controls that will help manage these risks. Prepare the Statement of Applicability documenting the controls selected and justifying any decisions not to implement, or to only partially implement, certain controls.

Do (implement and operate the ISMS): Formulate and implement a risk mitigation plan. Implement the previously selected controls to meet the control objectives.

Check (monitor and review): Conduct periodic reviews to verify the review the ISMS effectiveness of the ISMS. Review the levels of acceptable and residual risk.Periodically conduct internal ISMS audits

Act (maintain and improve): Implement identified ISMS improvements. Take appropriate corrective and preventative action. Maintain communication with all stakeholders. Validate improvements

It is very important that an organisation is able to check how effective its information security management is in practice. In order to enable this to happen, the organisation needs to establish a measurement process to be able to measure and assess how effective the controls are at protecting their information assets. An example might be to measure how good the controls are that have been implemented to avoid insider threats, such as the effectiveness of the access control methods that are being used, separation of duties, monitoring the misuse of system resources or user awareness and reporting of events and incidents that might be linked to insider activities that might compromise policies or procedures (Humphreys, 2008: 250).

5. A Situation Analysis On Information Security Management

Information security management guidelines, which attempt to provide the best information security management practices, are used by organizations. By adopting an authoritative guideline, organizations can demonstrate their commitment to secure business practices; organizations may then apply for certification, accreditation, or a security-maturity classification attesting to their compliance to a set of rules and practices (Siponen and Willison, 2009: 267).

Information security management for both public sector and private sector is very important. This approach strengths, weaknesses, opportunities and threats can be summarized as follows (http://www.iso27001security.com/ISO27k_The_business_value_of_ISO27k_case_study.pdf, 2014; Whitman, Mattord, 2010; http://www.slideshare.net/mgraham213/information-security-management-5980916, 2014; http://www.msudenver.edu/~cis2010/pdf/CHAP12.pdf, 2014):

Strenghts:

-Increased reliability and security of systems, increased profits and an increase in share value for organizations
-Cost effective and consistent information security

-System rationalization and compliance with legislation

-Increased predictability and reduced uncertainty of business operations by lowering information-security-related risks to definable and acceptable levels

-Protection from the increasing potential for civil or legal liability as a result of information inaccuracy or the absence of due care

-Optimization of the allocation of limited security resources

-Assurance of effective InfoSec policy and policy compliance

-A firm foundation for efficient and effective risk management, process improvement, and rapid incident response

-A level of assurance that ciritical decisions are not based on faulty information

Weakness:

Human error and mistakes stem from employees and nonemployees:

-They may misunderstand operating procedures and inadvertently cause data to be deleted

-Poorly written application programs and poorly designed procedures may allow employees to enter data incorrectly or misuse the system

-Employees may take physical mistakes like unplugging o piece of hardware that causes the system to crash.

Opportunities:

-Improved management control

-Better human relations

-Improved risk management and contingency planning

-Enhance customer and trading partners confidence

Threats:

Malicious human activity and natural events and disasters. Malicious human activity result from employees, former employees, and hackers who intentionally destroy data or system components. These actions include: breaking into systems with the intend of stealing altering or destroying data, introducting viruses and warms into a system, act of terrorism.

The last source of threats to information security are those caused by natural events and disasters. These threats pose problems stemming not just from the initial loss of capability and service but also problems a company may experience as it recovers from the initial problem. They include: fires, floods, hurricanes, eartquakes, other acts of nature

Conclusion

Information security management is an area of growing importance. In the private sector and public sector focuses strictly on. Improving the quality of service is important for security information management. Carried out in stages as a process that aims to provide ease of control.

In addition to confidentiality, integrity, and availability, the responsibility, integrity, trust and ethicality principles hold the key for successfully managing information security (Dhillon and Backhouse, 2000: 128).

Organizations should do the following for information security management (Humphreys, 2008: 250):

-Their risk assessment is up to date.
-There is an effective set of controls in place.
-There is an effective incident management process in operational use.
-There is an appropriate measurement process in place.
-There is adequate training and awareness given to all staff.
-There is regular monitoring and reviewing activities taking place to check the effectiveness of their information security.
-Improvements are made to their set of controls as indicated by the monitor and review process.

As a result It is widely accepted that ISM guidelines play an important role in managing and certifying information security in organizations.

References

Choobineh, Joobin Gurpreet Dhillon, Michael R. Grimaila, Jackie Rees (2007). Management of Information Security: Challenges and Research Directions, Communications of the Association for Information Systems, Vol. 20, pp. 968-971.

Debi, Ashenden (2008). Information Security Management: A Human Challenge?, Governance And Risk Management, Information Security Technical Report13, pp. 247-255.

Eloff, Jan, Mariki Eloff (2003). Information Security Management-A New Paradigm, Proceedings of SAICSIT, pp. 130-136

Gurpreet Dhillon and James Backhouse (2000), Information System Security Management in the New Millennium, Communications Of The Acm July 2000/Vol. 43, No. 7, s. 128

Hong, Kwo-Shing, Yen-Ping Chi, Louis R. Chao, Jih-Hsing Tang (2008). An Integrated System Theory of Information Security Management, Information Management & Computer Security 11/5, pp. 243-248.

http://www.msudenver.edu/~cis2010/pdf/CHAP12.pdf, 07 September 2014

http://www.slideshare.net/mgraham213/information-security-management-5980916, 07 September 2014

Humphreys, Edward (2008). Information security management standards: Compliance,

Saint-Germain, René (2005). Information Security Management Best Practice Based on ISO/IEC 17799, T h e I n f ormation Management Jour n a l, J u ly/August.

Siponen, Mikko, Robert Willison (2009). Problems and solutions Information & Management 46, pp. 267–270.

web2.utc.edu/~Li-Yang/.../Introduction.ppt, 11 August 2014

Whitman Micheal E., Herbert J. Mattord (2010). Management of Information Security.