Why Information Security Management is Important

Rahul Ravella

East Carolina University

07/21/2014

Abstract

Information security management deals with the implementation, operation, establishment, reviewing, monitoring, maintaining and improving the information security management system. Information security management plays a very big part in today's businesses and from what the paper analyses, it is important for any business to implement it. The organizations have to hire highly qualified employees who have knowledge in both their field as well as experience with information security management, it's principles and how it is integrated with the business environment. The paper will cover a few topics and mainly looks into the advantages and disadvantages of information security management in the organization, the properties which talks about confidentiality, integrity and availability, the tools used in information security management systems which help in the prevention of hacking, irregularities, loss of data etc.

Why Information Security Management is important

In this day and age, business compete with each other ruthlessly to get a better edge over their competitor to sell their product. These businesses have some guidelines. One of the guidelines is to guard the business's information and the information of their customers from the prying eyes of the hackers and their rivals. In order to do this, it is very important to implement an information security management answer that provides enough security for different types of data that is in the business that could be either digitally stored or contracts or written down documents on paper. (leod1, 2011)

The threat to the company's data and their information is growing at an alarming rate and systems need to be placed so as to reduce the level of these threats as much as possible. Different types of businesses and different types of departments have to face problems with data security and these problems have to be taken care of. As the linking of computers and networks in a company or the linking of business partners, the control for the systems and the users will be lost to a significant extent. With the creation of a set of regulations and rules for the users and some set of rules for the IT systems combined called Information Security Management, the chances of the data getting into the wrong hands is significantly lowered. Security controls will not be able to form an IT environment that is secure by itself. It has to be given support through the use of operational controls. They help to give the users a set of actions and behavior so that they can be a part of the security of the IT environment in the future. (Solms, 1998)

Properties of Information Management System

The main properties of an information system that are required to provide security are integrity, confidentiality and availability.

Confidentiality:

Confidentiality is stated by ISO 2700:2005 as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Computers are made and designed to provide functionality. Confidentiality is looked into when the developers perform the design of the software in the later stages. The storing of the organization procedures for confidentiality is more or equally important. Confidentiality can be attained by using authentication methods such as username and passwords.

Availability:

Availability for information can be described as the way it is accessible and can be used whenever there is a demand by an entity that has the authority. The availability of information for a company is an important factor that affects the business continuity of a company. When a company losses business continuity then the company will probably have financial losses, loss of clients, and loss of reputation and will most likely need to close. Availability, similar to that of other aspects of security could be affected by technical issues, human causes or natural phenomena.

Integrity:

The last property is integrity. Integrity is making sure that assets of the company are complete and accurate. Integrity refers to the trustworthiness of information resource. The problem of integrity comes up with the collection and processing of data by the workers. It also includes what the origin of the data is and if the data from the source has been manipulated with. The failure to follow with integrity can lead to the delays in the making of decisions which can subsequently lead to the lack of actions that can reduce the effects of oncoming threats.

Other than the properties that were mentioned, a large importance to other attributes of information is given such as reliability, updateness, unambiguity, comparability, completeness, flexibility, processibility, cost, response time, addressability, detail, priority, ease of use, value, security and clarity. (Wawak, 2010) (Xuemei, Yan, & Lixing, 2009)

The risks that can occur because of these categories may depend on the situation, but the main rule is that human interference is the weakest link and hence the data and information must be managed through the use of technology systems. (Miller, 2008) (Ekelhart, 2009)

Advantages and Disadvantages of ISMS

Following are the advantages and disadvantages of information security:

Advantages:

- It is very easy to use information security. For material that requires less protection, a simple username and password is enough to protect a file. For material that is more sensitive, users can put in biometric devices, intrusion protection detection systems and firewalls etc.
- Important information that is private can be kept out of the hands of the wrong entity.
- With the improvement in technology, there is also a rise in the number of crimes related to technology and hence it is better to have an information security management in place.
- The information can be protected while the data is being used or while it is being stored.
- In higher levels such as the government, it can keep important confidential data out of the hands of hackers and terrorists who would love to have that kind of information.

Disadvantages:

- With the changes that are made constantly to technology, the companies have to keep purchasing updated versions of the information security technologies and the methods.
- These changes in technology also means that not everything is totally secure.
- When a human error is made where a specific area is not secured, the whole system or business can be compromised.
- There are times when setting it up can be really complicated and the users may not understand every detail of the system.

- Productivity might slow down if the user has to enter his password constantly to authenticate. (Capria, 2009)

The information security management process is given by ISO 27001. The international standard gives out a model for implementing, establishing, monitoring, operating, improving, maintaining and reviewing an ISMS. The ISO 27001 follows a particular process model called the Plan Do Check Act. Following are some of the actions that are carried out in each phase.

Plan: In the phase, ISMS policies, processes, objectives and the procedures are established which are meant for the management of risk and the improvement of information security to give better results that follow the organizations overall objectives and policies.

Do: In this phase, the implementation and the operation of the ISMS policies, processes, controls and procedures is done.

Check: Measurement and assessment of the process's performance is done against the ISMS objectives, policies and practical experience and the reports are given to the management for their review.

Act: Preventive and corrective actions must be taken based on the results that were obtained from the internal ISMS management review and audit so that there is constant improvement of the ISMS. (Montesino & Fenz, 2011)

Tools of ISMS

Some of the main tools of ISMS are:

Management Review:

A regular meeting is done by the executives for the dedication for the working of the system. This regular meeting is called the management review. Smaller meeting are held many times a month but the main reviews are held a few times every year. These reviews provide an opportunity to collect information while comparison of information and discussions can be created between the different representatives of the organization. This allows better understanding of the current situation of the organization for all the participants. It also allows a better understanding of the relationships between different entities of the organization. Better detection of the problems can be made by managers because of this understanding between the entities.

Corrective actions:

The steps that are taken to manage the non-conformities and for making improvements is called corrective actions. These actions are based on real problems that have already happened. They are solved by the removal of their source of the problem. It is considered to be a problem solving process. The responsibility comes under the information security manager for conduction the actions. The employees based on their capabilities are the ones who remove the non-compliance. The faster removal of these sources can reduce the harsh effects and make the

organization immune to these types of problems in the future. (Praxiom Research Group Limited, 2006)

Preventive actions:

These kinds of actions help to remove and detect the problems that can cause problems potentially in the future. To perform these actions requires all the employees to take part and help discovering potential problems that could come up. Preventive actions is similar to that of corrective actions in that the procedures of doing these actions is similar. Locating the sources gives a better understand of the problems as well as a better knowledge about the organization and the environment it has. These actions can be harder to implement but doing so will make the system more efficient.

Incident Management:

Unwanted events and their quick detection and handling is the main agenda of the incident management tool. Employees have a responsibility of identifying and reporting the problems. The tools helps to improve the employee's sensitivity and awareness towards the problems that occur in the organization and the organization's environment. The incident management tool also gives information to the corrective action.

Risk assessment:

The constant review of risk factors and the discovery of the new factors is called risk assessment. The main review is done once or twice a year. Other than the main review, smaller assessments are done a couple of times a year. Performing risk assessment right after finding out about a new factor or changes in risk factor will give the necessary information to make changes in the risk treatment plans and take preventive steps.

Risk mitigation plans:

On the chance that a risk factor occurs, a risk treatment plan is made which gives out instructions that have to be followed in steps. Plans have to be made by the organization based on audit reports, risk assessment and the information coming from outside. The risk treatment plan is the end product of the risk assessment tool. There are multiple options that can be taken when a risk does occur. Following are those options:

- Accept the risk if the management allows it after comparing it with the cost of improving the necessary controls to mitigate it is more than the loss.
- Implementation of a control or the combination of controls that are suitable which can lessen the risk to a level that is more acceptable.
- Avoiding the risk by not performing the business activity that the risk is related to.
- The transfer of the risk to another organization. (Safe Mode, 2009)

Compliance metrics:

The compliance metrics is a series of metrics that help to monitor the systems functioning. The monitoring should be done not only in the computer system but in the whole

organization. Using metrics that are accurate can help detect faults and irregularities faster and earlier. The only drawback is that metrics that are more accurate cost more. This again falls under the management's decision where they will weigh the cost of installing these metrics with the losses that would occur because of these threats.

Internal audit:

This tool is used for the monitoring dedicated areas of the organization and also its processes. The improvement of the information system is the main objective of the internal audit. The internal audit also helps in the detection of non-compliance. The audit tool fits in well with the other tools because of its flexible and less formal approach. This allows it to detect risk that cannot be found by other tools mentioned.

Summary

Implementation of information security management is a complicated process because of a large number of variables. Therefore it is a requirement to staff people who are very qualified in the branch of information technology and also who have a good understanding of the principles in the implementation of the information security management system based on the ISO standard.

Works Cited

Capria, A. (2009, February 19). *Blogspot.* Retrieved from anton-capria.blogspot.com: http://anton-capria.blogspot.com/2009/02/information-security-advantages-and.html

Ekelhart, S. F. (2009). Formalizing information security knowledge. *ACM*, 183-194.

leod1. (2011, June 11). *Hubpages.* Retrieved from Hubpages.com: http://leod1.hubpages.com/hub/Why-Information-Security-Management-Is-Important

Miller. (2008). *Miller School of Medicine*. Retrieved from Unversity of Miami: http://it.med.miami.edu/x904.xml

Montesino, R., & Fenz, S. (2011). Automation Possibilities in Information Security Management. *IEEE*, 259-262.

Praxiom Research Group Limited. (2006, June 12). *Praxiom*. Retrieved from praxiom.com: http://www.praxiom.com/iso-27001-definitions.htm#Corrective actions

Safe Mode. (2009). *safemode*. Retrieved from safemode.org: http://iso-17799.safemode.org/index.php?page=risk_treatment_plan

Solms, R. v. (1998). Why information security is important. *Information Management & Computer Security*, 174-177.

Wawak, S. (2010). *Academia.* Retrieved from academia.edu: https://www.academia.edu/1649676/THE_IMPORTANCE_OF_INFORMATION_SECURITY_MANAGEMENT_IN_CRISIS_PREVENTION_IN_THE_COMPANY

Xuemei, L., Yan, L., & Lixing, D. (2009). Study on Information Security of Industry Management. *IEEE*, 522-524.