INFORMATION SECURITY OF ORGANISATIONS: ISSUES AND POLICIES

Dr. Dipak Kumar Kundu
Librarian, Stage-IV (Sl Grade)
Satyapriya Roy College of Education
Salt Lake, Kolkata- 700 064, West Bengal
Email: dkksrcel@yahoo.co.in

Abstract:

Currently information security is crucial to all organization to protect their information and conducts their business. Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The purpose of the work is to know the importance of organisational information security. The present study is based on the analysis of literature regarding the information security and its policies with the help of various sources. The pathway of protecting information in an organisation is traced under the study. The study concludes that the development of modern organizations depends on the availability, confidentiality and integrity to ensure information security.

Keywords: challenges of information security, Information security, Risk management, Security policies

Introduction

In general, information security can be defined as the protection of data that is owned by an organization or individual from hackers or threats and risk. According to Whitman and Mattord (2005), information security is the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information. Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure

With the advent of high technology in the age of globalisation, all the organizations more depend on their information systems. The public become anxious of the use of the system in saving their information, data and especially their personal information. In addition, the threat

from the system hackers and identity theft has added their concern on the use of information system because nowadays there are so many hackers from all around the world. Because of this, many organizations will identify what type of information as their important operation which they need to protect as their one of internal control. The scares issues about stolen or missing data are becoming a frequent in all headline news as organizations rely more and more heavily on computers to store sensitive corporate and customer information. It is necessary to be worried about information security because much of the value of a business is concentrated on the value of its information. The Study of information security has so many concepts and also topics that every IT professionals should become a master or have some basics knowledge and skills of information security are just some few that is essential for all those that are involved in the IT technology sector. For example, Cyber-security analyst, forensics analyst, network administrators, systems administrators, application developers. With lack of knowledge in this important field of information security will be more likely to develop.

Organizations of all sizes will collect and store a huge volume of confidential information which may be about their employees, customers, research, products or financial operations. Most of the information is collected, processed and stored on computers and disseminated across networks from one computer to other computers. It could lead to lost business, law suits, identity theft or even bankruptcy of the business if this information fell into the wrong hands. Nowadays, information security also has evolved significantly and grown even more important in recent years. Therefore, information security has become a keen interest for all the organisations and institutions.

Objectives

The objective of the study is to know about the pathway of protection of information security. The other objectives are as follow:

i) To interpret the importance of the information security
ii) To know the characteristics of the information security
iii) To analyse the role of information security
iv) Identification of the policies taken for information security.

Methodology

The information regarding the information security has been gathered from various primary and secondary sources. The present study is based on the analysis of reviewing literature

obtained from internet and other primary sources, monographs, research reports. After reviewing all the papers, the actual information was sought and presented to enable in depth understanding of information security

Characteristics of information security

All the information in an organisation have important value that must be sorted and preserved in a systematic way to be accessed easily and protecting this information is crucial task for all the modern organizations. There are three main characteristics of information security.

i)The collection of influences to which each organization is exposed varies with the other organization. The information security in which the information technology that the organization uses, its personnel or employees, the area or field in which it does businesses and the physical location. All of these have an effect on information security.

ii) It effects every structural and behavioral aspect of an organization. This means that the gap or lack in a security fence can permit information to be stolen. As for example, an infected computer such as expose to viruses, malware, Trojan and so on, that is connected to an organization's network can destroy the information. Other than that, a cup of drink spilt on a computer keyboard can prevent access to information because the computer keyboard is damaged.

iii) Each individual that consist of employees, employers and also the top management that interacts with an organization in any way is also the characteristic of information security.

Importance of Information Security

It is well known about the fact that information security has become important task for most of the organizations. This is because, the information access and use and also the resources have become easier with the emergence of information technology especially after the advent of the internet and other electronic media that is used by certain organization. So, in order to make sure that the information security is well organized, the organization need to ensure that their information is properly preserved and protected and that they maintain a high level of information security.

There are four main reasons why information security is important to an organization. The reasons are as follow:

1. The information in an organization need to be protected because it has a value to the organization. The organization usually hold records of its own individual staff.

2. Proving that the organization has a secure and stable network assuring the customers that their information is safeguarded.

3. As more and more of information are stored and processed electronically and transmitted across company networks or the internet, there is a risk of the unauthorized access and the organization are presented with growing challenges of how best to protect it.

4. Information security is needed to reduce the risk of unauthorized information disclosure, modification, and destruction and to reduce risk to a level that is acceptable to the business.

How to protect the information

The organization's first important task is to make its computer network secured with safely configured and actively prevented from unknown threats. A new method to protect from unknown threats are emerging day to day to protect from malware programs that can be unintentionally installed on customer's or employee's machine, which an attempt to phishing that deceive them into giving up confidential information, to viruses, worms, and strategic identity theft attempts. One of the benefits of having a consistent technology expert on the organization roster is that the expert can offer a fast reaction time and be proactive in safeguarding organization IT system when new warnings first emerge. The IT network professional can also help the organization to maintain a secure virtual environment by reviewing all computer assets and determining a plan for preventive maintenance.

Role of Information security

Information security performs four important roles.

1. Protects the organisation's ability to run various functions.
2. Enables the safe operation of applications implemented on the organisation's IT systems.
3. Protects the data procured and preserved by the organisation for long run uses.
4. Protects the technological innovations and instruments of the organisations.

Organisational Information Security Policies

An information security policy (ISP) is a set of rules that guide individuals who work with IT assets. The company can create an information security policy to ensure its employees and other users to follow security protocols and procedures. The written policies about information security are essential to a secure organization and its employees. Everyone in a company needs to understand the importance of the role they play in maintaining security. The way to

accomplish the importance of information security in an organization is by publishing reasonable security policies. These policies are documents that everyone in the organization should read, sign and compulsory to be followed when they come on board. In the case of existing employees, the policies should be distributed, explained and after adequate time, need for questions and discussions. One key to create effective policies is to make sure that they are clear, and as easy to comply with as possible. Policies that are overly complicated only encourage people to bypass the system. In order to implement this, there a few policies that need to be followed by the employees.

All personnel within the organization should be sent to the appropriate training programmes on information security policy and the organization's security expectations, aligned to their functional roles. As an example, the corporate internet usage policy should be communicated in a clear manner, read, understood and acknowledged by all personnel within the organization, while a specific policy such as the enterprise software management policy, should be included all the relevant personnel, for example, the IT Systems department.

1. ***Authority & Access Control Policy***

Hierarchical pattern: Typically, a security policy has a hierarchical pattern. It means that inferior staff is usually bound not to share the little amount of information they have unless explicitly authorized by the higher authority. Conversely, a senior manager may have enough power to make a decision what data can be shared and with whom, which means that they are not tied down by the same information security policy terms. So, the principles of the organisation is that ISP should address every basic position in the organization with specifications that will clarify their authoritative status.

Users' access: Users are only empowered to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. The dealing staff authorised by the company should monitor all systems and record all login attempts.

2. ***Visitor Management***

The visitor means the people other than the employees of an organization. The visitor management must be managed properly so that an unauthorized or unescorted visitor do not intrude in the organization. This is because an unauthorized or unescorted visitor can be a physical threat and can also steal sensitive information. Before a visitor can enter into the organization, all the information about the visitor must be checked. If any problem is detected,

the security guard must take an action. Based on the policy, the visitor might be escorted at all times especially in confidential areas. The visitors are required to wear a badge and should sign in and sign out if necessary. If the policy is being used, the organization will feel more secured and protect the importance information.

3. ***Password management***

Strong passwords only work if their integrity remains intact. If you leave them written down, share them or select 'remember this password' on a public computer, you risk them falling into the wrong hands. The same is true if you use the same password on multiple accounts. Let's say a criminal hacker breaks into a database and finds the password for your personal email account. If the crook can work out where you work (which they have a good chance of through a Google, Facebook or LinkedIn search), they'll probably try that password on your work email and other work-related accounts. It's therefore essential that you include a policy that instructs employees not to share passwords, write them down or use them on multiple accounts.

4. ***Password creation***

Everyone uses passwords at home as well as at work to access secure information. Unfortunately, most of the people set weak passwords before they get their hands on some valuable company information. Organisation should mitigate this threat by creating a password policy that outlines specific instructions for creating passwords. The wise decision to make passwords is that they should be a combination of at least eight letters, numbers and special characters. However, this doesn't always guarantee a strong password, as employees are still susceptible to easily guessable phrases such as 'Password @1'.

5. ***Data Classification***

The policy should classify data into categories, which may include "top secret", "confidential", and "public". The objectives in classifying data are:

- To ensure that sensitive data cannot be accessed by individuals with lower clearance levels.
- To protect highly important data, and avoid needless security measures for unimportant data

6. ***Key Control***

Unlike an electronic access device, mechanical keys can be duplicated and used without leaving a trail. The organization key control policy should include a means to track who is

currently holding mechanical keys and who has permission to duplicate those keys. Besides, all the keys that has been duplicated must be placed on a secure place such as in security room. Employees must write their name on the book to make sure that when the key is lost, the last name of the employees that use the key can be track down. Other than that, the organization must make a policy to use the smart card reader other than using the mechanical keys. The authorized person such as the employees only should have the smart card to be used to scan when entering the places which contain importance information.

Recommendations for Information Security in an Organization

In order to make information security in an organization, a few suggestions may be recommended. It is been recommended to overcome the current issues or challenges that have been occurs these days. There are a few solutions that are related to the current issues or challenges to be followed.

1. Find a subject expert in information security

In order to implement the good information security, the organization must find a subject expert in information security. If the organization has the right people to implement security, meaning individuals who take ownership of security and build good relationships with others in the organization and external partners, the information security can be implemented successfully. Nowadays it is not a difficult to find the expert, but the organization can find the people who really know and understand how to explain the risk-reward trade-off and can sell solutions within the organization.

2. The use of mobile security (ForeScout)

In order to prevent from the stolen of personal information and organization's information, mobile devices must be protected by using the mobile security. The most famous mobile security is the ForeScout. ForeScout is a platform that provides continuous security monitoring and mitigation. It allows IT organizations to efficiently address numerous access, endpoint compliance and threat management challenges even within today's complex, dynamic and expansive enterprise networks. With ForeScout, it can let users to enjoy the productivity benefits of mobile computing devices while keeping the network safe from data loss and malicious threats.

3. Skills of the employees within the organisation

An organization's success depends on the skills and expertise of its individual employees which can attributed to them. To make sure that all the employees had the skills in information

security, the training should be arranged. The organizations can make a workshop or short-term graining programme about the information security and its related matters to become familiar on the use of information and its preservation properly. Besides, the organization also can release its staff slot wise to attend the training programmes on the information security organised by other organisations or institutions to help the employees in managing and protecting the valuable information in their places. Although the training will cost more time and money, but it is worth because the information which had the

4. Protect computers from anti-viruses

Protecting the computer from viruses and other threats is very easy task nowadays, but users have to be more conscious. There are a few steps that can be adopted by the users or employees in preventing the computer from viruses and threats. Firstly, by installing an antivirus program and keeping it up to date timely can help defend the computer against viruses. Anti-virus programs scan for viruses trying to get into the email, operating system, or files. The new viruses may appear daily, so users must set the anti-virus software to install updates automatically. Secondly the use of firewall. Windows Firewall or any other firewall can help alert to suspicious activity if a virus or worm attempts to connect to the computer. It can also block viruses, worms, and hackers from attempting to download potentially harmful programme.

Conclusion

Information security is importance to the development of an organization that keep the data or information about their customers or company. The development of modern organizations depends on the availability, confidentiality and integrity to ensure information security. Other than that, the extensive use of information technology improves the efficiency of the business, but exposes the organization to additional risks and challenges such as failure to understand about information security, mobile workforce and wireless computing, shortage of information security staff and information security attacks. The information security awareness increases day to day. Many organizations have implemented the information security to protect their data. Information security is needed to reduce the risk of unauthorized information disclosure, modification, and destruction.

To ensure information security, the organization should understand that information security is not solely a technological issue. The organization should also consider the non-technical aspect of information security while developing the information security. Besides, it should be

noted that, well implemented information security in organization has the ability to reduce the risk of crisis in the organization.
Other than that, information security management committee play an integral part in the successful of information security implementation in organization. Organization should emphasize the formation of this committee to ensure that the implementation of information security in the organization achieve the organization's goals. Besides, the written policies about information security are also essential to a secure organization. Everyone in a company needs to understand the importance of the role they play in maintaining security. The way to accomplish the importance of information security in an organization is also has made a great effort in implementing the information security in an organization.
Information security is crucial in organization. All information stored in the organization should be kept secure. Even though the information is important in organization, there are several challenges to protect and manages the information as well. One of challenges faced in an organization is the lack of understanding on important of information security. When employees have lack of information security knowledge in terms of how to keep their information secured, the organization is easy to being attacks by hackers or other threats that try to stole or get the organization's confidential information. So, it is crucial and important to all staff in an organization to have knowledge and understanding about the importance information security practice to protect the confidential data.

REFERENCES

Charles, K. (2013). The C.I.A. triad or C.I.A. triangle and other security concepts. (http://www. securityorb.com/2013/10/c-i-a-triangle-security-concepts/).

D. Paterson, T. Taylor, S. Brooks, J. Glanfield, C. Gates, & J. McHugh. (2009). Activity Plots: A Multi-sEntity Time Series Visualization. (URL: http://www.cert. org/flocon/ 2009/ proceedings.html).

Deutsch, W. (2014). Security policies you need: an introduction to creating effective security policies. (http://bizsecurity.about.com/od/creatingpolicies/a/6_policies.htm).

Scout, Fore. (2014). Mobile security. https://www.forescout.com/solutions/mobile-security.

Garret, C. (2012). Importance of a security policy. http://www.slideshare.net/charlesgarrett/importance-of-a-security-policy-11380022.

Information Security Handbook. (2009). What is Information Security? (http://ishandbook.bsewall.com/risk/Methodology/IS.html).

Johnson, M. E. & Goetz, E. (2007). Managing Organizational Security: Embedding Information Security into the Organization. IEEE Security & Privacy, 2, 16-24.

Mellado, D. & Rosado, D. G. (2012). An Overview of Current Information Systems Security Challenges and Innovations. Journal of Universal Computer Science, 18, 1598-1607. http://www.jucs.org/jucs_18_12/an_overview_of_current/jucs_18_12_1598_1607_editorial.pdf.

Sattarova, Feruza Y. and Kim, Tao-hoon (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering, 2(2); 17.

Schneider, L. (2014). Information security: learn about information security. (http://jobsearchtech. about.com/od/historyoftechindustry/g/InfoSecurity.htm).

Singh, Rajinder & Kumar, Shakti. (2014). Network Security & Vulnerable Security Aspects, Global Journal of Engineering Science and Researches, 1(6); 75-89.

Slade, E. (2009). Top 3 Reasons Why Information Security & IT Maintenance is Important. (http://www.howardcounty.com/Top_3_Reasons_Why_Information_Security__IT_M

aint enance_is_Important-a-1224.html.).

Solms, Rossouw von. (1998). Information security management: why information security is so important. Information Management & Computer Security, 6; 174-177.