Research in Analysis IT Security Policy and Security Solution

Kai Liao, Feng Li

The Library of Huazhong Agricultural University, Wuhan, China

Keywords: Information Technology, Organisation, Security, Policy.

Abstract: This research paper will state the IT Security Policy, and list all of component of that. The main problem of IT security policy is from the people, mistake of staff and hacker attack, and all of this is hard to avoid. Therefore our Security Policy should include the various methods facing difference situation. For example we establish firewalls to improve the security and install Anti-Virus for every computer. Furthermore, setting different viewing permissions and the entire in-house network will be monitored by administrators. And then, build a thorough backup system by on-line database, removable drivers to save data and information completely. Even if every method all data have been destroy or the operation system clash, we can recovery because of back-up frequency is plan of policy. According the size of organisation, we can change the main policy.

1. Introduction

1.1 General Topic and Background

Nowadays, the Information Technology plays an indispensable role in an organisation. The IT security issue attributes organisation manger care and IT Security Policy is the most basic element of the IT Security Program. Security policies identifies the rules and procedures that all organisation staff using computer or network resources must observe in order to ensure the safety, integrity, and availability of data and resources.

1.2 Definition

Information Technology, in this research the word means computer and related software, feasibility, and information database of the organisation.

Organisation, generally refer companies develop the policy to.

Security, in this research means keep far from the virus and Trojans, and the data and information of organisation will be not reveal and lost.

Policy, the word means a series of plan to develop the organisation security level.

2. Purpose

This research paper aim to highlight the importance of IT Security policy, IT Security policy force on develop security level of an organisation which avoid the risk of organisation data and resource reveal and missing. This research let reader make sense about the components, processes, and methodologies of IT security policy.

3. Literature Review

IT security policy is important for an organisation. Initially, the general principle and common sense of IT and IT Security must be known. According a book (*Whitman & Mattord 2009*) that describes a larger amount of principle of information security has been found to develop our concept for IT security. However, creating a successful security policy can not only rely on the principle of protection, but also need people to develop a suitable security program to improve.

Two articles are found that about which IT security issue is a classification problem. In the article ‘Information and system security’ (*Information Technology Newsweekly 7 Sep 2010, p328*), it analyses the component of IT security. According component of this article, people can develop a

policy that is correctly and accurately. The component includes staff security awareness training, the user accessing rights, password, E-mail, Internet, back-up and recovery. On the other hand, when a policy has been created, it should be implemented in an organisation. Lacey (2007) admit the method and the difficult of will facing in the policy processing. In the following part of this research each source will be analysis and discussion.

The first source describe the concept of IT Security. In the book (*Whitman & Mattord 2009*), the author explains what the Information Security is, and the IT Security Policy is most basic element of the IT Security Program. Security policies identifies the rules and procedures that all organisation staff using computer or network resources must observe in order to ensure the safety, integrity, and availability of data and resources. However, only knowing the principle is alone far from enough. Although this book almost lists all of principles of Information Technology, but creating a successful security policy should not only rely on the principle of protection. I think people should develop a suitable security program to improve it. The policy is based on realistic surrounding of organisation, it is necessary to understand which IT security issue is classification problem.

Baker (2006) and Smith (2005) illustrate the surrounding of organisation in their journal article. Articles include the structure of organisation, computer device that using in routine work. They want to people to know that a successful security policy is not constant and change in various organisation, because of every company have own characters and unique problems. According the size and type of organisations, the policy should be modification to suit this company. The majority parts of the policy are similar about these two articles, so people know about the component of security policy is necessary.

When people know about surrounding of workplace in organisations, we could start develop an IT security policy. In the article 'Information and system security' (*Information Technology Newsweekly 7 Sep 2010, p328*), it analyses the component of IT security. According to component of this article, people can develop a policy that is correctly and accuracy. The component includes the user accessing rights, password, E-mail, Internet, back-up and recovery. When the policy completes those whole components which the article mentioned, the policy is almost done. From this article we can know about the tasks what we will conduct. Although this article list all components of IT Security, but it just roughly describe every component rather than analyse detailed. Creating a successful policy should totally understand each component of IT Security, so need more sources about these to apply.

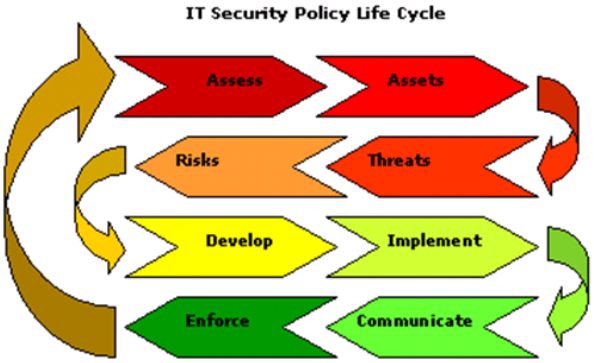

Figure 1 a IT Security policy life Cycle

All of the tool and the measure are subsidiary, they can only assist the organisation to keep far from the dangerous, and the staff security awareness training is still critical (*Schwabach 2006*). Staff security awareness training is long-term reciprocation, and they know how to use the tool and how to avoid the dangerous which will instance the risk.

Becker (2009) discusses the user accessing rights in his journal article. User accessing rights is set up classification authority, limited junior and external visitor accessing the database place. Of course, they should not entry or get the secret of organisation. Backer (2009) notes a view that depending on the sizes of organisation, various networks are applied, which is LAN (Local Area

Network), WAN (Wide Area Network) and VPN (Virtual Private Network) respectively. Different network have different setting method, the most common method is setting administration password and restrictions on the IP address of visitor. But problem are following, which kind of password is safety password? Password security is the key part of IT security.

Wood (2008) admits the cryptography and the setting method in his journal article. The password is key component in the whole security policy. SEM (Small and Medium Enterprise) have no enough funds to bridge a gigantic security system, so the password became simplest and effective tool. A weak level of password will increase the risk of information security not only by external thief, but the outside staff. Author of this article (*Wood 2008*) describe the social engineering and some password cracking technical. The hacker can though these tool to invade the information system to get business secrets. In this article author describe the method how to set a safety password. A safety password should not be the same as your personal details include phone number, date of birth, or student number, and you'd better using combine symbol, number, capital and small letters.

Schneier (2005) in his book *How to Keep Your Electronic Messages Private* described the E-mail Security. E-mail is a convenience and free tool to transfer mail and document, but it also has high rate to spread virus or Trojans. At the same time the junk mail will influence the efficient of work, when the users check their mail boxes, they always filled with junk mails. Virus and Trojans have possible spread though the attachment or the mail website link. Some e-mails use fraud method to lust users by clicking their websites and those websites are probably fish websites which can filch users' password. For example, this kind of website lie to people won a random prize or proclaimed a method can earn lots of money. If the attachment file is end of .exe, the file have high possible is Virus or Trojans.

Lessig (2004) in his journal article talked about the harm of Internet surrounding for the organisation security. Internet is the greatest invention for organisation, but Internet has dangerous and have a large amount threatens. From the last part of E-mail security we know that the Virus and Trojans spread is fast and easy. When the user clicks a website especially the unfamiliar website, they have risk infecting the Virus and Trojans. The search engine makes the work and living convenient, but at the same time some websites which are people searched maybe hangs Virus and Trojans.

Virus and Trojans endanger the IT security. Therefore main task of IT security policy is protecting the computer safe from them. Alderman (2004) consider every computer have to install an anti-virus software. Anti-virus software can always alert and looking out for harmful intruders. The common Anti-virus software is MacAfee, Norton, and Avast. On the other hand, maintain and update OS (Operation System) is good method to avoid the virus and Trojans, because the loophole of OS is main path of Virus and Trojans.

IT Security policy should prepare to every possible and make a full spectrum protection. For this, the back-up and recovery became an important part, because of that is the last chance to save data and information when the system clash or suffering from the Virus and Trojans.

When the Policy completed, how to identify the policy is good or bad, and how to implement the policy? In the article (*Lacey 2007*) list points of good policy should include and difficulty of implement process. An excellent policy should under the business rules and discuss with organisation manager, and according their viewpoint to modify the policy. On the other hand, the IT Security policy should suit the organisation themselves. For example, SEM (Small and Medium Enterprise) have no enough funds to bridge a gigantic security system, so the staff security awareness training is important.

4. Methodology

The policy created includes two main parts, one is staff training, the other is maintains and update software. Training makes the staff can have security awareness to prevent the dangerous. At the software side, it including install anti-virus and back-up. Based on the size of organisation to decide which part is main part. If the organisation is SEM, then the training is main part. And if the

organisation is large company, we will force on the software part. When IT security policies have been created, it should be implemented in the organisation. As following, the guideline of implementing process will be presented.

4.1 Modification and decision of Policy

A successful policy must be the most suitable for organisation. It needs to be discussed with the organisation manager, and according to their viewpoint to modify the policy. Of course, the decision of policy should assist to complete the mission and goals of an organisation.

4.2 Staff security awareness training

This step tries to let the staff know how to use the security tool and how to avoid the danger of Internet. In this process, teaching the common sense of IT Security to staff is normal to see.

4.3 Make a strong password

This step is to teaching staff how to set a safety and strong password. For this, the password has to be different from the personal details included phone number or date of birth or student number. The strong password is combine symbol, number and capital and small letters as possible as.

4.4 Safe E-mail use

Suggestion the staffs use Yahoo! Mail, Gmail or other trusted mailbox, because these mailboxes can support a junk mail filtration system and virus scan.

4.5 Safe Internet use

Let the staff know how to simply identify which websites perhaps have the virus and Trojans. As possible as do not fill their personal information in unfamiliar websites.

4.6 Install the anti-virus software

Install the anti-virus software on every computer of organisation. In these computers, staff will set to automatic update and automatically scans all incoming and outgoing files.

4.7 Classification accessing rights

Classifications accessing rights from various level staff. The top manager has whole accessing rights, and the accessing rights will reduce with the level of staff decrease. Maybe the normal staffs only have the rights that can view some small parts of database. Of course, the outsider people have no access to entry the organisation database.

4.8 Back-up

Back up original OS and save some important data.

4.9 Post policy

Regularly return the organisation to accept feedback and give the useful advice to them. And then, assist them to maintain and update OS, repair loophole and update the back-up file.

5. Recommendations

From the source, I understand that the principle of IT security from this article (*Whitman & Mattord 2009*), and know about some common security problems with the workplace (*Smith 2009*). According to different size of company people can choose different policy. The view point of Schwabach (2006) let me know the importance of training. Schneier (2005), Lessig (2004), Alderman (2004) respectively talk about the component of the IT Security in their article. An IT security policy is important for an organisation. Initially, the general principle and common sense of IT and IT Security must let all the people to know in a company. Therefore, this book (*Whitman & Mattord 2009*) describes a larger amount of principle of information security have been found to develop our concept for IT security. However, creating a successful security policy should not only

rely on the principle of protection, people also should develop a suitable security program. In the article 'Information and system security' (*Information Technology Newsweekly 7 Sep 2010, p328*) it analyse the component of IT security, according to component of this article, we can develop a policy that is correctly and accuracy. The component includes staff security awareness training, the user accessing rights, password, E-mail, Internet, back-up and recovery. When a policy has been created, it should be implemented in an organisation. Lacey (2007) admit the method and the difficult of will facing in the policy processing.

6. Conclusions

The IT security is a series of plan to develop the security level of organisation, and keep far from the Virus and Trojans. The data and information of organisation will be not reveal and lost easily than before. This research makes people understand the definition of IT Security policy. Security policy identifies the rules and procedures to let all organisation staff can use computer or network resources correct. Everyone in the organisation should observe the Security policy in order to ensure the safety, integrity, and availability of data and resources.

References

[1] Alderman, R 2004, *Prevention and deal with computer viru, Homely technology,* vol.125, iss.3, pp45-49.

[2] Baker, J 2006, *CIOs Surveyed Say Employees Complain About IT Security Policies, Journal of daily IT*, vol.14, iss.5, pp126-127.

[3] Becker, J U 2009, *An integrated view of human, organizational, and technological challenges of IT security management*, *Information Management & Computer Security* vol.17, no.1, pp4-19.

[4] Lacey, D 2007, *Implementing information security policy in a large international organisation, Elsevier Advanced Technology,* vol.8, iss.2, pp199-208.

[5] Lessig, S 2004, *E-mail security: how to keep your electronic messages private*, The Penguin Press.

[6] Schwabach, A 2006, *the principle staff should know, Communication of VCM,* vol.8, iss.3, pp15-17.

[7] Sever, T n.d., *Ruskwig-IT Security Life Cycle*, C.stone, gif, accessed 10/09/2010 http://www.ruskwig.com/pictures/it_security_policy_life_cycle.gif

[8] Smith, J 2005, *E-WORLD: An eye for technology vision, Scientific American,* vol.28, no.4, pp35-43.

[9] Whitman, M & Mattord, H 2009, *Principles of Information Security 3rd Edition*, Course Technology, Canada.

[10] Wood, S 2008, *Information and Communications Technology Passwords Procedures, Journal of science,* vol.4, iss.2, pp16-21.