Security measures paper essay sample

Business, Company

Security Measures

In the field of information technology, the physical security of the organizational infrastructure is not enough to secure the confidential information from the unauthorized access. Therefore, the organizations are required to develop and implement a security plan along with Standard Operating Procedures (SOPs) for using the information, communication and technology (ICT) systems. Being a security administrator of the organization, it is required to develop the security plan, including standard operating procedures for using electronic mail (email), acceptable use, physical security and incident response. Therefore, the document presents recommendations for utilizing the ICT system in a way that the confidential information can be secured from the intruders and abusers.

E-mails

The electronic mail is one of the easiest, fastest and cheapest ways of communication (exchanging information among stakeholders). But on the other hand, the communication through electronic mail associates various vulnerabilities of information leakage, spammers, viruses and malicious content. The information can be leaked through electronic mail and it may cause various losses include, financial and time cost. Therefore, the development of the security plan and standard operating procedure for the electronic mail is significant to stop the intruders to access the information.

The following paragraphs are the recommendations for consideration while developing the security plan for the emailing system of the organization.

In the standard operating procedure of the email, the organization is required to implement strong password to open or view the emails. Each of the employees should have a unique login name and strong password to access and exchange organizational information. Particularly the user authentication system should be implemented in the operating system of the email server.

The organization is required to secure the operating system of the email server by updating and configuring the operating system regularly. Moreover, the unnecessary applications and services installed on the email server should be disabled or removed.

“ Mail servers and user workstations running mail clients are frequently targeted by attackers. Moreover, mail clients have been targeted as an effective means of inserting malware into machines and of propagating this code to other machines. As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected” (Tracy, Jansen, Scarfone and Butterfield, 2007)

Antivirus should be installed on not only the email server, but also each computer system and laptop should have installed the antivirus application. And each of the emails either received or sent should be scanned for the viruses, malware and suspicious content.

In order to secure the email server, the network infrastructure should be secured by implementing the Demilitarized Zone and email gateways.

Moreover, the intrusion detection and prevention system along with the firewall should be configured in the computer network.

Acceptable Use

The Acceptable Use Policy (AUP) is one of the integral parts of the information security framework that facilitates the organization to define the rules for the fair utilization of the website or network or service. It is specified in the GFI software white paper (2011) that “ 30 to 40% of Internet access is spent on non-work related browsing, and 60% of all online purchases are made during working hours”. In order to avoid misuse of the internet, computer or email by the employees during working hours and usage of the internet inline with the company’s goals and objectives, the AUP should be implemented. The AUP should not be developed and applied to the employees of the company, but also the customers / clients of the company. The AUP should address the maximum use of the services provided by the company. The following paragraphs provide guidelines to be considered while development of the AUP (GFI Software, 2011).

The employees of the company should be encouraged to report any theft or unauthorized disclosure of the company’s information. In this regard, the employees should be held responsible for their actions during the working hours.

The network monitoring tools should be installed to keep an eye on the actions performed by the employees for fair utilization of the voice mail, email and computer. The monitoring of employees during working hours is legal, therefore, the same should be included in the AUP.

The employees should not be allowed to use the company’s resources for their personal use. In this regard, the network administrator should block the websites include, but are not limited to the social networking websites, shopping portals, stock trading websites, pornography and chat rooms.

Physical Security

The Physical Security Policy is required to develop to avoid the unauthorized access to the information, facilities, resources and equipment. The physical security policy should facilitate the multi-layers security include, the access control protocols, security human resources (guards), locks, CCTV surveillance and physical barriers. The guidelines or recommendations for development of the physical security policy include the following.

The employees should be guided to properly dispose the papers contain sensitive information of the company. In this regard, the standard operating procedure should state that the papers which are of no use should immediately be disposed off utilizing the machine.

A proper inventory of the physical assets of the company should be maintained, specifying the serial number and specifications. The server room should be out of bound for all, except the authorized employees of the company. In this regard, the access control methods should be implemented to restrict the unauthorized. Moreover, an alarm system should be implemented to avoid any illegal or unauthorized access. The implementation of the above-given measures can help the company to physically secure the computer system and unauthorized access.

Incident Response

It is critical to respond rapidly and effectively upon an occurrence of any information security breach. In the words of Cichonski, Millar, Grance and Scarfone (2012), “ A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices”. In this regard, the incident response plan is significant to implement for limiting the damages and reducing the recovery cost and time. The incident response plan should include, the reasons of the unwanted incident and a step-by-step guide to be followed for overcoming the damages of the incident.

The incident response plan should contain at-least four (4) phases include, preparation to avoid unwanted incidents, a detection and analysis of the incident, containment and recovery phase, and post event activities. In the first phase of the incident response plan, it is to ensure that the an appropriate information security policy is implemented in the organization. Moreover, the contact information of the employees going to response the incident is maintained properly. In the detection and analysis phase of the incident response plan, it is required to identify the strength of the attack, the signs of the incident and the sources of the indicators. Moreover, the observations are required to be documented as per the prescribed format. In the phase of the containment and recovery, it is required to respond the incident based on the analysis. It is pertinent to mention that the analysis and recovery phases have to iterate until the situation becomes normal. In the post incident phase of the recovery plan, it is required to document the experiences, the strategy adopted to recover and the lessons learnt from handling the situation. It would facilitate the company to overcome the similar situations in the future (Cichonski, Millar, Grance and Scarfone, 2012).

Conclusion

The security plan and standard operating procedures are developed to support the information security policy of the company. In this regard, the security plans for the emails, incident response, physical security and acceptable use are required to implement to avoid information leakage threats, vulnerabilities and recovery after an incident. Therefore, the document presented the guidelines and recommendations for the development of the security plan and standard operating procedures for utilization of the company's information, communication and technology resources. The information security was breached in the company, because neither security plan nor standard operating procedures were implemented by the company. Therefore, it is expected that the recommendations provided in the document would help the company to improve the information security in a way that the company would not face any information security breach in future.

References

Cichonski, P. Millar, T. Grance, T. and Scarfone, K. (2012). Computer Security Incident Handling Guide. Retrieved on 2nd October, 2014 from: http://csrc. nist. gov/publications/nistpubs/800-61rev2/SP800-61rev2. pdf

GFI Software. (2011). The importance of an Acceptable Use Policy. Retrieved on 1st October, 2014 from: http://www. gfi.

com/whitepapers/acceptable_use_policy. pdf

Tracy, M. Jansen, W. Scarfone, K. and Butterfield, J. (2007). Guidelines on Electronic Mail Security. Retrieved on 1st October, 2014 from: http://csrc. nist. gov/publications/nistpubs/800-45-version2/SP800-45v2. pdf