Information security and ethics

Business

Information Security and Ethics Security Threat A of the security threat, its impact, and an example. What can be done keep information secure from the threat. (Technology: software or hardware), organizational strategies.

Computer Virus

Description: these are created programs or data that are introduces in the networks or even the personal computer, with the intention of destroying the computer.

Impact: the viruses change the coding of the program hence making them unusable. Others will destroy or even scramble the saved data in the computer. Some of the characteristics of these viruses are that they undertake the damage in hidden form and only notice after the damage is done. They also carry out their activities very rapidly.

Example of a Computer Virus; auto run virus, worms.

Technology (software,

Hardware): this will require the organization to install antivirus in their computers to ensure the viruses are destroyed before they attack. The organization may also be required to back up the data in safe external hard disk.

Organizational strategies (policies, leadership, training, etc.) specification is one policy that would be required where each employee has his or her computer, to prevent spread of viruses when one is infected. Further, the organization should control the sites in the network and also external devices plugged into to the computer.

Adware

This can be appropriately be described as type of software that support advertisements. It displays or downloads a banner that is not wanted by the

user, within his or her software. The software is most of the time embedded with the software of interest by the manufacturer, with the intent of sinking the cost of development.

The impact of the adware to the network or the computer is over loading. This leads to computer breakdown or even slow transfer of data. Also, this gives room for the entrance of viruses.

Example adware is the advertisement of a link involving courses offered by a university, location and also their facilities.

With regard to protecting the organization system from adware, the organization should ensure that, only licensed and registered software is purchased. They should also install antivirus to attack the abrupt advertisements. Furthermore, it should within the planning of the organization, to trades with licensed software producing companies. It should also ensure that employees have clear instruction as to whom to consult in case of software installation in their computers.

Spyware

This is software that is referred to as malware, which invades the privacy of the user, by gathering the user information and gaining access to his software and then display the adverts on it.

The impact of the threat is that it can either corrupt the data or steal the information stored by the user. Example is the computer virus which decodes or corrupts the system information of the computer, autorun

For this threat, the organization will be required to install both firewall and antivirus. Furthermore, the information being transmitted should be encrypted and backed up in safe external disks.

The organization should only trade the software with registered companies.

They should be the only legal operators of the software.

Trojan

It is defined as a malicious set of instructions that executes actions within the machine without user's legal authorization. The impacts of Trojan include data copying, modification, blocking, deleting or even disruption of network and computer performances.

Example is Backdoor Trojan.

This threat requires antivirus installation. Data backup would also serve as a solution.

The organization management should ensure that external portables are fully scanned before plugging.

Sniffer

It is also referred to as network monitor. It is defined as set of instructions, which analyses and monitors the traffic within the network. It also detects problems and bottlenecks.

The impact on the organization is that; it can be employed illegitimately by hackers, to siphon the information being transmitted.

Example is a network router

Installation of firewall, security passwords, and data encryption should be done. The local connection within the organization should have identification, such that; only those people permitted to access, can gain entry in to the system.

Any other threat

Another threat experienced by the organizations is hackers. These are unwarranted users of network or computer. Their impact to the organization includes stealing of data, or even worse deleting the crucial system

information.

With regards to hackers, the organization would be required to install a firewall, to block unwarranted users. They would also be required to encrypt the information while transmitting the information.

The organization should ensure there is a system centre where all the operational computers and networks are monitored. Furthermore, they should educate the employees the essence of data protection and encryption.

Work cited

Internet Security, Encyclopedia of Business 2nd ed. Retrieved from http://www. referenceforbusiness. com/small/Inc-Mail/Internet-Security. html#b

Moore, A. P., & Shimeall, T. J. (2007), Protecting Against Insider Threat Retrieved fromhttp://www. sei. cmu. edu/library/abstracts/news-at-sei/securitymatters200702. cfm

http://www. epolicyinstitute. com/

Elleithy, Khaled. Innovations and advances in computer, information, systems sciences, and engineering. New York, NY: Springer, 2013. Print.