Cyber security plan critical thinking samples

Law, Security

Information Security Portfolio Project

Review of Organization’s Infrastructure

Identification of Vulnerabilities

Since last era, organizational infrastructures did not need to build or invest much on security issues. But now, larger infrastructures and networks are being deployed which has also increased the needs of security. As compare to the closed networks, LANs and WANs face far more security threats. It is due to the reason that closed networks do not allow the public networks to access their personal network but is only open to known sites and parties. However, LANs and WANs are more open and so more intermediary networks and individuals have chance to access the network and thus are more vulnerable to threats.

Vulnerabilities are the weaknesses in the network design, configuration, technology, or security policy that provides an opportunity to the hackers or the natural threats to damage the organizational data or other important information. Therefore, it is highly important to identify all types of vulnerabilities in the network design and consider appropriate solutions for the design. There are different types of vulnerabilities associated with the specific type of network design. Vulnerabilities can be of two types. They either generate naturally/physically or by human interference. Depending upon the design of the Company’s network, the two will be discussed accordingly.

- Environmental Vulnerabilities

Environmental Vulnerabilities relates to the threats due to natural or environmental disasters; for example floods, earthquake, lightning or fire

that can cause damage to the complete computer system including the hardware, software, data and services. In order to avoid such threats, natural disasters can of course not be stopped but the designers need to make the network stronger. For this purpose, all the components of the network are carefully examined for any kind of vulnerabilities. Moreover, contingency and recovery plans are developed.

At XYZ Computer Manufacturing Business, every building is handling its data independently. If in case, any building experiences a natural disaster then stock and all may be lost. So, there is a high need to set up plans that can control any such vulnerability. First, the building should be shock resistant. It should be able to withstand in case of earthquake, or other natural disasters. There should also be a backup for all data, saved at any other location.

- Physical Vulnerabilities

Physical vulnerabilities mainly relate with the hardware issues. In comparison with the environmental, physical vulnerabilities comes in due to weakness in the system components; for example, if the network system is easily accessible to the unauthorized public or the system or network room locks can easily be broken.

In case of XYZ Computer Manufacturing Business, physical vulnerabilities can be avoided by keeping the servers and other important network machines in the room where there is tight security, doors have strong locks, servers or other machines have an encrypted data and any person other than network administrator should not be able to access the system through USB or other data transfer device. Moreover, the room should be located in the prohibited area where any unauthorized staff is not allowed.

- Human Vulnerability

Human vulnerability refers to the attacks on data or important information by hackers or crackers. These attacks are made by either insiders or outsiders of organization. The insiders or employees are the most dangerous attackers because they know about the security locks at the network of the organization. However, if the system is strong and has least number of vulnerabilities then these attacks can be controlled. In order to control such human attacks, the network should be incorporated with firewall, data sent over network should be encrypted, authorization settings should be enabled, or network should be password protected .

In case of XYZ Computer Manufacturing Business, employees should be given limited access; network authorization should only be done after verifying the profile of the individuals, strong passwords should be applied and firewall and strong protocol design is necessary.

Security Models

Mainly, there are three types of security models that have their own set of pros and cons. These include, open access, restrictive access, and closed access. Here, each model will be discussed in view of XYZ Computer Manufacturing network requirements.

- Open Access security model is easy to implement but it does not provide enough security to the network system because only few measures are included. Network administrators only configure basic software and hardware settings. Simple passwords are applied on servers and systems. Other measures including virtual private networks, firewall, intrusion detection system and ones that require additional cost are not implemented. These

models are usually implemented in the scenarios where there is no need for LANs to connect to the internet or WANs, there are least security threats, all networks users are trusted and there are minimum assets to protect. This type of design allows users access any area.

- In case of restrictive security model, there are many security measures implemented and so it is difficult to execute as well. Administrators deploy costly software and hardware solutions including intrusion detection systems, firewalls, VPNs and identity servers. This model is usually applied in scenarios where there are number of assets that needs to be protected, large security threats, and some users are not trusty. Moreover, they are used in case if the LANs are connected to either public WANs or to the internet. However, it is not as easier for the users to connect to the network with this type of model as because the security tightens.
- In type of closed security model all available measures of security are implemented. All costly security measures are also implemented to ensure maximum security. This design is implemented in case if there are premium assets to protect, large threats are expected, and all users are unreliable. In this type of design, it is highly difficult for the users to access the network .

Design of Security Plan for the Organization

In case of XYZ Computer Manufacturing, restrictive security model would be most appropriate. Since, there can be various security threats to the company’s network, therefore staff members cannot be allowed to access all information, and there are also important assets that needs to be secured. Since, the LANs of individual buildings need to connect with the WAN and also to an internet because company’s employees may need to connect with

an internet to access various informational resources and communicate with the clients. Each building is internally connected by LAN and then these LANs are connected to WAN. In order to ensure high security firewalls, and strong network passwords will be applied. Firewalls are already deployed internally at LANs. Clients in different offices at one building are connected via router and centrally access the email, database server and file server. The users from other network will be inquired to enter password before accessing the Company’s WAN network.

In addition to the WAN firewall and encryption settings, the security measures will also be applied internally at local area networks. Employees will be provided with limited access and passwords and encryption techniques will be applied .

Design of Code of Ethics related to IT Profession at the Organization

Besides the security reasons, some organizations are also liable to take on appropriate security measures. There are certain Acts and Directives being passed in law regarding the network security and privacy. In 1998, EU passed Data Privacy Directives that ensures the security of consumers’ personal data. According to this, the data of users will not be allowed to be traced or used for other purposes but this data should be totally confidential. US organizations are also formulating and implementing Information Security and Privacy Acts in order to provide confidence to users .

Bibliography

Goldberg, I., Hill, A., & Shostack, A. (2003). Trust, Ethics, and Privacy.

ISACA. (2009). An Introduction to the Business Model for Information Security

. USA.

Kark, K., & Dines, R. (2010). Security Organization 2. 0: Building a Robust Security Organization. Forrester.

Nayab, N. (2011, 10 18). How to Develop and Implement a Cyber Security Strategy for Your Business. Retrieved from Bright Hub: http://www. brighthub. com/computing/enterprise-security/articles/125746. aspx

Rufi, A. (2007). Network Security. Pearson.