THE IMPACT OF COMPUTER NETWORK SECURITY ON BUSINESSES

Name

Course

Tutor

Date

The impact of computer network security on businesses

**Introduction**

In the modern computer age, it is difficult to find a company that does not have some forms of computer networks within their ranks. Just it has been the cases in modern residential houses and offices; the large corporations are continually incorporating the application of computer networks to run various operations in the facilities. Some of the activities that are performed with the systems include data storage, management of the employees, stock monitoring as well as the keeping of customer information. While the involvement of the computers in the commercial institutions has been positive developments in the industries, there are a lot of challenges that are posed by the reality (White, 2015). One of the primary issues of concern is security. When designing any computer network, the question of security is in the mind of any the developers. That has become important in the world where there has been a steady rise in cybercrime. It becomes incredibly necessary for the institutions to determine the best strategies that they can put in place to protect their businesses from the security lapses that may occur within the systems. The occurrences of security challenges within the computer networks adopted by business organizations may pose threats that may utterly destroy the institutions.

**The concept of business computer networks**

In the modern practices, small business organizations have resorted to the use of the local area networks (LAN) to prove internet to their facilities. When business grows, there is a tendency by the institutions to expand their LAN and may adopt the Wide Area Networks (WAN) to provide internet over a large geographical area. Admittedly, with the nature of most organizations, with the increased need to share information and coordinate the activities of different departments, it becomes essential that the commercial institutions adopt these technologies to improve their operations.

In the modern practices, commercial institutions allow their employees to carry their personal computers and access the internet from within the facilities. Admittedly, technologies have improved to such an extent that the management may lock out access to the employees from accessing some unwanted sites such as pornographic websites as well as the gambling sites. These policies are supposed to make sure that the individuals not to misuse the resources of the company (Laudon & Laudon, 2015). Besides, it has become a standard practice for a business to allow for remote access of the company's resources from outside of the facilities. It is called remote access. In this regard, it is possible for an individual to gain access to the company's resources as though the individual is working from within the facilities.

In the process of setting up these networks, the issue of security will always be at the balk of the mind of developers. Because most business organizations have bulks of information and sensitive data that they would want to protect, peoples usually go for the best technologies that have the most advanced security features. The following is an examination of some of the security threats that are affecting the computer networks within organizations;

**The security threats facing computer networks**

*Denial of service attacks*

The denial of service attacks is one of the most common and most troublesome security threats to computer networks. When this attack occurs, a user is prevented from accessing some of the websites that they would ordinary access. In this respect, the individuals are sabotaged and may not do a lot of things with their computers until the source of the attacks is detected and fixed. In this process, the attackers would gain access to the networks without being notices and alter or manipulate the data on these computers (Shabana et al, 2016). As a result of these attacks, the company is likely to lose a lot of data. These situations usually present considerable problems to the organizations.

*Hacking*

Hacking is the most commonly used term to refer to those sets of activities that allow individuals to gain illegal access to computers. All over the internet, there are materials, manuals as well as bugs that may be used by an extensive network of individuals to carry out these activities. When hacking occurs, it is possible for the companies involved to lose massive amounts of data. When unauthorized individuals gain access to sensitive pieces of information belong to foreign organizations, they may decide to do whatever they please. The individuals may choose to copy the data, manipulate the data or even destroy the information. All these situations are undesirable to any organization since they place institutions in very adverse conditions. Confidential client information may land into the wrong hands, and that may lead to legal proceedings. Besides, it is possible that such an action may expose the weaknesses of an organization to the rivals and that may ultimately affect the competitiveness of a team.

*Phishing*

 Phishing is another famous online crime that is committed by a considerable number of cybercriminals. One of the reasons that have contributed to the rise in the cases of phishing is that it is easy to execute. In this practice, an individual would see some messages propping up fake notes on the screens of computers or other devices. In most cases, these messages would require the internet users to respond to some queries and demands. When successful, the persons would be in a position to access bank accounts and commit financial crimes.

**The impacts of the computer security threats**

There are a lot of consequences that arise with the rise of the computer network threats within an organization. The following is a discussion of some of the impacts that are caused by the security threats within the company's computer networks;

*Loss of data*

 There are instances in which the compromise of the computer networks may lead to total loss of data. It takes a lot of time and resources for an organization to make and store data. When some of the attacks occur, they may lead to deletion or compromise of the data in such a manner that they may not be in a position to be seen again.

*Data manipulation*

 The attackers may use bugs that will alter the compositions of data. For instance, there are situations in which malware may be injected into the computer systems to make them unreadable. Besides, the data may be altered to reflect in untrue positions of the activities of the business. In such circumstances, the institution may lose immense amounts of resources.

*Exposure of sensitive information to the public*

 Some rules require institutions to treat customer details with utmost confidentiality. Agreements existing between an organization and its creditors and debtors need to remain as confidential as possible. However, when hackers gain access to these pieces of information, they may want to expose them to the public. Apart from exposing the company to scrutiny from its rivals, it is possible that customers and associates who may feel aggrieved with the release of the information to third parties may sue for damages (Papp et al, 2015). These events, if they are not handled properly, may lead to the collapse of an institution.

**Solutions to the threats**

While it is not possible to stop the threats to computer systems from occurring, it is, however, possible to put in place various mechanism and approaches that would significantly mitigate the effects of these attacks;

*Use tested, proven and original software*

 One of the issues that predispose organizations to attacks is the possession of software that is untested and does not meet the market standards. It is essential for institutions to settle for pieces of software that are of the right quality. That would be important in reducing the chances of success of attacks. Since unlicensed software may not have the necessary security features, they at times become easy targets for the attackers.

*Keep changing the security passwords*

 It is necessary for administrators to continually shift the security passwords of the computer networks in the organizations. When a password stays unchanged for an extended period, it is easy to master it and be used by people to cause problems with the functioning of the computers. To be unpredictable, it is necessary to keep changing the passwords.

*Do not allow employees to carry personal laptop to work*

 Since the security features of the laptops may not be ascertained, it is possible that the attackers may use them to gain access to the company's databases and cause manipulates the files. It is advisable that organizations do not allow different laptops to be used to gain access to the network system since that may expose the group to tremendous security challenges.

**Conclusion**

There has been an increased use of computers in the modern business practices. However, the increase in these methods has also caused immense challenges to the organizations. Some of the problems that usually occur include phishing, hacking and denial of service attacks. If these risks are not adequately addressed, it is possible that a business may be brought down to its knees. Given the above facts, it is essential for institutions to take precautionary measures to prevent themselves from these attacks. One of the ways of doing this is to make sure that the software being used by the companies have been tested and proven. That would significantly reduce the chances of success of attacks.

References

Laudon, K. C., & Laudon, J. P. (2016). Management information system. Pearson Education India.

Papp, D., Ma, Z., & Buttyan, L. (2015, July). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In Privacy, Security and Trust (PST), 2015 13th Annual Conference on (pp. 145-152). *IEEE.*

Shabana, K., Fida, N., Khan, F., Jan, S. R., & Rehman, M. U. (2016). Security issues and attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, 5(7), pp-81.

White, C. (2015). Data communications and computer networks: a business user's approach. Cengage Learning.