Essay on cyber threats and their vulnerabilities

Law, Security

Cyber threats to Computers and Productivity

The security of computer and information systems is a fundamental aspect in any organization because nearly all organizations, in the current information age, depend on computer networks and information systems to execute their daily operations. Attacks to computer systems can lead to detrimental effects to an organization because it can lead to loss of important information and worse, breakdown of the entire organization system. For this reason, Information security measures must be implemented using vigilant approaches in order to control the pervasive effects of cyber threats and vulnerabilities. Control of inadequacies to cyber threats and other forms of malicious attacks should be an ongoing process that must be updated from time to time (Shih et al., 2004). It is emphatically crucial to note that cyber threats to information systems within organizations is evolving and expanding at an increasing rate. This paper highlights the true threats posed by viruses, the extent of the virus and malicious code problem, virus hoaxes, and their effect on computers and productivity. Information systems have distinct capabilities and the use of internet connections is ubiquitous, and hence, cyber threats and vulnerabilities should not be underestimated or undermined. Insider threats are other forms of threats to many organizations because it leads to breach of private and confidential data (Shih et al., 2004).

Cyber Crime

This refers to unlawful conducts undertaken using computers, ancillary, and electronic devices. It entails the process of disrupting network traffic through the distribution of viruses, email bombing/service attacks, cyber stalking, identity theft, and fraud among others. The effects of viruses and malicious attacks can be categorized according to the effects committed against different groups. These groups include crimes committed against individuals, individual property, organizations, and organizations at large. Virus and malicious effects on individuals include indecent exposure, hacking/cracking of personal emails, and harassment (Robert and Dacey, 2007). Effects to individual property include the process of transmitting viruses, unauthorized intrusion into computer systems, and hacking. Threats committed to an organization and society includes cracking, hacking, distribution of pirated software, and polluting the environment with indecent materials.

Extent of Cyber threats to computer systems

The dramatic increase in the number of internet users has expanded the exposure of computer and information systems to susceptibility of attacks such as virus attacks and unauthorized intrusions. The ability of propagation and increased multiplication of viruses and worms can lead to increased damages to the computer and information systems. Sadly, many organizations are still unaware of the threats posed by malicious hackers and cyber criminals. Good examples of the extent of cyber threats can be evidenced in the following scenarios.

According to BBC News story in 2005, the amount of money lost in internet financial fraud in Brazil outstripped the amount of money lost through bank robberies. In the same year, a computer hacker managed to obtain confidential details of 40 million credit card users while British police uncovered efforts by a cyber-gang to steal $412 million from a Japanese bank (Nigel, 2007). Such examples shows that even at the best of circumstances, all organizations are vulnerable to internet threats and cyber insecurities. Data and information is critical for productivity and sustainability of many organizations. Access to sensitive information by hackers or malicious attacks, may prove detrimental to the organization in question because the accessed information may contain sensitive trade secrets or private and confidential information that might be used for doing the wrong things (Nigel, 2007).

While it can be easier to reach a consensus regarding the urgency of risks caused by viruses, worms, and other forms of malicious attacks to computer and information systems, the right answers for addressing such vulnerabilities are hard realize. This can be attributed to constant changing nature of such risks coupled with their level of dynamic and varying effects (Wright, & Harmening, 2009). Additionally, the ability and scale of such risks in compromising computer systems and the integrity of the network framework is wanting. The introduction of host networks and systems, antivirus software, malware, and removal tools had increased the strengths of user administrative features in addition to minimizing the true threats posed by viruses, the extent of the virus and malicious code problem, virus hoaxes, and their effect on computers and productivity.

Conclusion

The increasing sophistication of computer and information systems, coupled with the increased use of the internet has led to an increase in the volume of cyber vulnerabilities. The problem is yet to become worse with the introduction of open systems, cloud computing, and the emergence of intranets. This calls for the implementation of new measures security of computer and information systems. The need to manage, asses, and monitor such systems is critical and even more urgent. Equally important is the need to prioritize and examine the most significant computer and information systems and other network vulnerabilities in order to guide the process of setting priorities and allocating resources towards the prevention of such risks (Robert and Dacey, 2007). With such measures, it becomes possible to minimize the true threats posed by viruses, the extent of the virus and malicious code problem, virus hoaxes, and their effect on computers and productivity.

Nigel, F., (2007)," Challenges for regulating financial fraud in cyberspace,” Journal
of Financial Crime, 14 (2): 190 - 207

Robert F. and Dacey, F. R. (2007). Critical infrastructure protection establishing
effective information sharing with infrastructure sectors. Washington DC: DIANE
Publishing

Shih Dong-Her, et al., (2004)," Internet security: malicious e-mails detection and
protection", Industrial Management & Data Systems, 104 (7): 613 - 623

Wright, J. & Harmening, J. (2009). Computer and Information Security

Handbook. New

York:

Morgan Kaufmann Publications Elsevier Inc.