Network security issues

Law, Security

This three-page memorandum addresses the network security issues concerning the business that are identified by the IT Steering Committee. Top network security threats, security laws that protect networks and proposed processes and procedures for disaster recovery, data backup and data restoration are included, with attached articles sourced from scholarly journal in order to accurately support the choices for the processes and procedures proposed.

TOP THREE NETWORK SECURITY THREATS

Never before have there been greater security threats to the information stored in business computer systems. Information, which was once vulnerable to unauthorized disclosure, modification, or destruction by a relatively small group of users within an organization, now faces these same risks from the millions of individuals worldwide who use computer networks. Below are the top three network security threats which concern the business.

Unauthorized Data Modification. An intruder could make undetected and unauthorized modifications to the contents of a transmitted message. Information may be deleted or delayed, or changes could be made to the order in which a series of messages are transmitted. The destination address of a message could be changed, causing the message to be directed to another party.

Or the origination address could be altered, causing the receiver of the message to believe that the transmission was sent from a different source. Legitimate messages could be recorded and later played back, allowing an

unauthorized user to establish a connection under a false identity, or causing a transaction to be performed twice.

Denial of Service (DoS). There are a variety of ways an outsider could hinder the data transmission of the organization by employing several applications. One such is the denial of service attacks prevent legitimate users from entering a website (Flynn and Kahn, 2003). These attacks can bring systems down by damaging information and preventing software from operating correctly.

Unauthorized Disclosure of Network Information. This threat to security arise whenever messages are intercepted and read by outsiders. In some cases, the mere existence of message traffic is important to an intruder because the pattern of messages may reveal the amount of business being transacted between different users. This attack is easier to prevent than to detect.

TOP THREE LAWS AFFECTING NETWORK SECURITY

The top three laws which affect network security are: (1) *18 US Code 1030,* which Neilforoshan (2004) related that this law forms the basis for federal intervention in computer crimes; (2) *18 US Code 2701,* which Sabbah (2006) notes as being the law which prohibits unlawful access to stored network communications and prohibits preventing authorized users from accessing systems that store electronic communications; and (3) *18 US Code 1831-39,* which Flynn and Kahn (2003) explains as the law that punishes criminal theft of trade secrets, or obtaining without authorization proprietary trade secrets related to a product.

PROPOSED PROCESSES AND PROCEDURES

Information security requires more than the physical protection of computers. An effective information security program incorporates a combination of technological and human controls in order to avoid the loss of information, deter accidental or intentional unauthorized activities, prevent unauthorized data access, detect a loss or impending loss, recover after a loss has occurred, and correct system vulnerabilities to prevent the same loss from happening again.

The organization could use network-monitoring software. Such software monitors the data flow and detects weak points--hardware configurations or software arrangements that are likely to cause transmission errors (Messerges et. al., 2003). Likewise, the enforcement of backup and recovery procedures is essential. No network is fail-safe. Backup and recovery procedures provide contingency planning for network downtime and include securing alternate network facilities, planning for alternate means of data transmission and eliminating confusion over what data were preserved in instances of transmission interruption.

More importantly, the use of network access controls is deemed necessary. Depending on the organization, passwords should be assigned to every user at various levels of the operation. In some cases, this may even mean assigning selective access to specific computer files.

CONCLUSIONS

All organizations face the risk of a breach in information security. Although no system can be completely secure, most security breaches can be

prevented, or their impact minimized, with the implementation of effective technological and human controls. When used in combination, these controls provide an acceptable level of protection for sensitive information.

FUTURE ACTION

To address such network security challenges, the organization needs to develop an effective strategy fit for the proposed processes and procedures aforementioned. Effective strategies require operational efficiency; within the organization’s information systems, this means an emphasis on information security and controls. A cost-effective business internal control system for network security should also be designed and implemented toward the goal of reduced operating expenses and therefore increased profits.

WORKS CITED

Flynn, N. & Kahn, R. (2003). E-mail Rules: A Business Guide to Managing Policies, Security and Legal Issues for E-mail and DigitalCommunication. New York: AMACOM.

Messerges, T., Cukier, J., Kevenaar, T., Puhl, L., Struik, R. & Callaway, E. (2003). A Security Design for a General Purpose, Self-Organizing, Multihop Ad Hoc Wireless Network. *Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks,* 1-11.

Neilforoshan, M. (2004). Network Security Architecture. *JCSC* , 19, 4, 307-313.

Sabbah, E., Majeed, A., Kang, K., Liu, K. & Abu-Ghazaleh, N. (2006). An Application-Driven Perspective on Wireless Sensor Network Security. *Q2SWinet,* 1-8.