EXECUTIVE SUMMARY

The XYZ Hardware Company, Inc. infrastructure features high volumes of sensitive and confidential corporate data relevant to internal and external transactions. From 1999 to the middle of 2004, XYZ has utilized the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Model version 1e to protect its network. The OCTAVESM Model has proven to be helpful for XYZ by identifying over 198 potential security breaches. However, in 2004, when XYZ began to enhance its existing network infrastructure to include telework, 210 security breaches occurred. These breaches cost the company over $350,000 in lost profits between July and December of 2004. To safeguard their network, upper management wanted to invest the money in a series of generalized training including working ethics, virus scanning, and backing up files. However, instead, XYZ’S chief information officer (CIO) invested over $100,000 in research in order to modify their existing protection strategy, to better safeguard their new telework infrastructure by identifying its specific strengths and weaknesses in an effort to create more concentrated and specialized training at the root of the problem.

Keywords: access control; authentication; computer crime; computer viruses; hacking; IS case study; IS problems; IS project risk management; IS security risks; office to future; opportunities threats analysis; risk assessment; security management

ORGANIZATIONAL BACKGROUND

XYZ Hardware Company Incorporated (XYZ), located in Pennsylvania, USA, is a wholesale distributor for more than 160 of the best-known hardware product companies including Amerock, Broan, Classic Brass, 3M, Stanley, and Dupont. The company was founded in the early 1950s. The company employs over 430 and is regarded as one of the most technology-oriented companies in its line of business. In 2001, XYZ was awarded a national Cisco Technology Award in recognition of its innovative Internet and corporate network usage supporting internal operations and customer relationships. Furthermore, in 2004, XYZ enhanced its network communications to accommodate telework. As a result of telework communications, over 210 security breaches occurred between July and December of 2004. To safeguard their network, XYZ’S Chief Information Officer (CIO) wants to invest over $100,000 in research in order to modify their existing protection strategy, the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OC-
TA VE\textsuperscript{SM}) Model version 1e along with the OCTA VE\textsuperscript{SM} Catalog of Practices, to better safeguard their new telework infrastructure by identifying its specific strengths and weakness in an effort to create more concentrated and specialized training at the root of the problem. Meanwhile, the upper management wants to invest the money in a series of generalized training courses including working ethics, virus scanning, and backing up files.

**SETTING THE STAGE**

The OCTA VE\textsuperscript{SM} Model developed by Carnegie Mellon University (CMU) Software Engineering Institute (SEI) is a repeatable methodological approach for identifying and managing information security risks of actual threats including disclosure of a critical asset, modification of a critical asset, loss or destruction of a critical asset, or interruption of access to a critical asset, via an organizational self-assessment (Alberts & Dorofee, 2003).

The OCTA VE\textsuperscript{SM} Model’s Catalog of Practices are currently used as a measurement for what XYZ is currently doing well with respect to physical security or current security practices, as well as its organizational vulnerabilities. The OCTA VE\textsuperscript{SM} Model’s Catalog of Practices comprised a collection of strategic and operational security practices (Allen, 2001; British Standards Institution, 1995; Gramm-Leach Biley Act of 1999, 2000; Health Insurance Portability and Accountability Act [HIPAA] of 1996, 1998; Swanson & Gutman, 1996). Strategic practices focus on organizational issues at the policy level. Strategic practices included issues that are business-related as well as those that require organization-wide planning and participation (Alberts & Dorofee, 2003). The operational practices focus on technology-related concerns including issues related to how workers interact with and protect technology (Alberts & Dorofee, 2003).

The purpose of the OCTA VE\textsuperscript{SM} Model & Catalog of Practices is to create a comprehensive protection strategy that reduces the overall risk of an organization’s information assets via the use of a systematic, context-driven approach (Allen, 2001). A risk is defined as a threat that results in a negative impact on an organization through the disclosure of a critical asset, the modification of a critical asset, the loss or destruction of a critical asset, or the interruption of access to a critical asset (Alberts & Dorofee, 2003). The OCTA VE\textsuperscript{SM} Model categorizes threats into four groups:

- network-based threats,
- physical threats,
- system threats, and
- other problems.

Network-based threats are deliberate or accidental actions involving an individual using an organization’s network access. Physical threats come from the utilization of systems, hardware, software, or information with ill intent. System threats are problems such as viruses, trojan horses, and trap doors within an organization’s information systems. Other problems are the result of natural disasters, terrorist threats, or any asset-altering event that is outside an organization’s control (Alberts & Dorofee, 2003).

“An asset is defined as something of value to an organization” (Alberts & Dorofee, 2003, p. 103). In general, information technology assets are a combination of systems, software, hardware, information, and people. Systems are combinations of information, software, and hardware that are used to process and store information. Software consists of applications and services such as operating systems, database applications, networking software, office applications, e-mail applications, and security applications that process, store, and transmit information. Hardware is made up of physical devices such as servers, routers, and remote computers. Information consists...