SECURITY CONSIDERATIONS IN AN E-COMMERCE ENVIRONMENT: GUIDELINES FOR SUCCESS

Hossein Bidgoli
California State University, Bakersfield, CA 93311

ABSTRACT

Security issues and threats in an e-commerce environment are varied and can be caused intentionally and unintentionally by both insiders and outsiders. Many experts believe that insiders create the majority of the security threats and issues. At the same time experts believe that security concerns are one of the major reasons that many individuals are reluctant in doing online transactions and conducting e-commerce activities. Security issues and threats related to an e-commerce environment can be categorized as controllable, partially controllable, and uncontrollable. This paper presents a series of guidelines that identify various security issues and threats in an e-commerce environment and then offers a comprehensive security plan and guidelines for recovery if disaster strikes. The guidelines include:

Creating security awareness, employees and key decision-makers first should understand what security is and why it is important to create and implement a comprehensive security program in an e-commerce environment. Also, the consequences of not having such a plan should be explained.

Conducting risk analysis, information should be considered as a commodity with a value attached to it. This means more/less financial analysis and capital budgeting techniques could be applied to this process.

Formation of the security task force, key employees and decision-makers have to be involved in the design and implementation of a security program. A buy-in process and sense of ownership have to be created at the early stages of the security program design and implementation.

Identification of basic security safeguards, Uninterruptible Power Supply (UPS), redundant arrays of independent disks (RAID), and mirror disks are the most basic security safeguards that have to be in place in any security program development.

Identification of general security threats, natural and human created disasters as they apply to an e-commerce environment have to be identified.

Identification of intentional threats, computer viruses, worms, Trojan horse programs, and other intentional threats must be identified.

Identification of security measures and enforcements, as a part of an e-commerce security program biometric, nonbiometric, physical, software, and electronic transaction securities must be identified and be integrated into the security program.

Identification of computer emergency response team services, network administrators, webmasters, and e-commerce site managers should always review the latest information provided by CERT (Computer Emergency Response Team). This information may assist in protecting vital e-commerce and network resources.
Formation of a comprehensive security plan, a security plan should include hardware, software, and policy measures that collectively protect the information resources of an e-commerce site. Preparing for a disaster, an organization must be prepared to respond to a disaster if it occurs. One of the best security measures is to plan for disaster. The response process known as the disaster recovery planning or contingency planning system can play a major role in putting the organization back on its feet.

REFERENCES


