Physical Security – A Critical Component of Information Security

An Executive Update Volume 1 Number 4 February 2008

Information technology has transformed traditional business models and facilitated the creation of entirely new ones by integrating technology into business processes. With this integration, the lines between information security and traditional physical security have become blurred.

Physical and Information Security

It has become a truism that physical security is a critical component of information security.

Information security professionals have long recognized the importance of protecting the technology that supports critical business functions. The best technological controls can be rendered useless by introducing an internal wireless network to bypass a firewall or sitting down at the server console to bypass the virtual controls in place. With physical access to internal networks and servers, all bets are off.

In the late nineties, a very popular commercial website was unavailable for several weeks, not because of remotely exploited vulnerabilities, but because someone was able to circumvent the modest physical security in place and steal the servers out of the data center.

"As with business processes that rely on technology, so too, information security and physical security have become inextricably linked."

Physical and Logical Security - The role that information security plays in physical security is less frequently recognized. Often, technology is a critical component of physical security. A recent physical security assessment for a software development and

continued on page 2

Guidance for Physical Security

International organizations have established standards and guidelines for physical security as part of an overall security management program that also includes information security and meets governmental requirements and consumer expectations.

The following are examples of internationally recognized standards and guidelines that are used to implement management systems to effectively manage physical security. These are complementary to related ISO standards.

- BS 25999-1:2006: Business Continuity Management Code of Practice (management system for disaster recovery and business continuity)
- BS 7799-3:2006: Guidelines for Information Security Risk Management (management system approach for the assessment and treatment of risk)
- ISO/PAS 28000: Specification for Security Management Systems for the Supply Chain (management system specification for physical security)
- ISO 22000: Food Safety Management Systems - Requirements for Any Organization in the Food Chain (management system for preventing the introduction of food safety hazards)
- OHSAS 18001: Occupational Health and Safety Management (specification for health and safety management systems) ◙

continued from page 1

system integration company highlighted good perimeter security, lighting and physical isolation of high security areas with only one exception. The desktop system that managed access control for the entire building resided in an un-monitored and publicly accessible lobby area. Anyone could walk up to the system and get to the software that managed access control for perimeter doors and secure areas within the building.

Security Convergence - Technological advances facilitate the leveraging of economies of scale by putting voice and video over IP networks. Closed circuit video surveillance that used to travel over dedicated coaxial cable now shares bandwidth with data and voice on common IP networks. Many business processes now rely on technology and similarly, information security and physical security have become inextricably linked.

Comprehensive Solution - The most effective approach to assessing the physical security needs of your organization is a comprehensive and holistic one. Physical security should not be considered in isolation but as a critical component in a comprehensive framework that recognizes and supports the organization's strategic business objectives.

An international standards-based approach provides many advantages over technology-focused, proprietary and other approaches by providing a measurable, repeatable, scalable and continually improving security program. The security framework can also be assessed by an independent third-party and certified as conformant. Certification by an accredited certification body provides a level of assurance to customers and business partners that the organization is effectively managing security.

John B. Weaver, president and CEO of JBW Group International, advises executive management and board directors to view physical security in the context of an overall information security program and address physical security requirements in the same holistic manner one would address information security.

JBW Group International would like to work with you to implement an effective information security system that also addresses your physical security needs. ◙

What is Physical Security?

Physical security can refer to a wide variety of security-related activities depending on the organization. "Guards, gates and guns" are what usually come to mind, but physical security involves much more.

Perimeter access control may be the most recognized component but the primary goal of physical security is the safety and protection of human life. This can take the form of emergency evacuation plans, fire suppression, controls to prevent accidents and executive protection, as well as keeping the bad guys out. Loss prevention is also a focus of physical security. The gaming industry has instituted highly sophisticated closed circuit television (CCTV) monitoring to catch cheats on the casino floor. Loss prevention is important to retailers as well. "Inventory shrinkage" accounts for $31B in losses annually for the retail industry according to the National Retail Security Survey, conducted by Richard C. Hollinger at the University of Florida. Also falling within the purview of physical security are activities such as fraud prevention, investigations and managing the processing of employee background checks for HR. ◙

"The merging of physical and logical access controls will account for more than $7 billion in U.S. spending in 2008, a ten-fold increase from 2005"

Forrester Research Inc.

FOR MORE INFORMATION...

JBW Group International

P.O. Box 19373

Minneapolis,

Minnesota 55419 USA

www.jbwgroup.com

Email: info@jbwgroup.com

1.877.97.27001