

Business Consulting

- *Regulatory Support*
 - Policies and Procedures
 - Regulatory Compliance
 - Sarbanes-Oxley
 - GLBA
 - HIPAA
 - BSA
 - PCI (Payment Card Industry) Security Audit
 - Information System Audit Outsourcing
- *Enterprise Support*
 - Business Continuity Planning
 - Attestation and Assurance
 - SAS-70
 - E - Discovery
 - Forensic Examinations
 - Security Remediation

Technology Consulting

- *Application Security*
 - Application Security Assessment
 - Application Penetration Test
 - Web Application Security Assessment
 - Web Application Penetration Test
- *Network Security*
 - Risk Assessment
 - Vulnerability Assessment
 - Penetration Testing
 - Internal
 - External
 - Social Engineering
 - War Dialing
 - War Driving
 - Blue Snarfing
 - Wireless Security Assessment
 - Information System Security Audit
 - Information System Control Audit
 - Network Architecture Design and Assessment
 - Physical Security Assessment
 - Log Analysis

Control Essentials

Volume II, Issue XII

December 2007

Physical Security

Physical Security is easy to overlook today, with network security breaches swarming all over the headlines. Networks and computer systems have always gained more importance when organizations have planned their security strategies. However, physical security remains, even today, one of the first links an organization must look to strengthen.

Physical security is vital to the security infrastructure of an organization as it protects not only the information assets but also the most critical assets, the employees. A number of regulations require organizations to ensure that appropriate physical security is implemented. Some of these are the Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Graham-Leach-Bliley Act (GLBA), The Homeland Security Presidential Directive/Hspd-12 and the standard FIPS PUB 201-1. Many organizations have been at the receiving end of lawsuits for not practicing due diligence and due care in physical security.

A Layered Approach

Physical security encompasses defensive mechanisms to prevent, deter, and detect physical threats of various kinds such as the following:

- *Environmental Threats:* This category includes damages that are caused by natural calamities such as hurricanes, tornados, fires, floods, etc.
- *Human Threats:* This includes all damages provoked intentionally or unintentionally by people. An intruder accessing a restricted area, a terrorist attack or an employee error are all examples of threats belonging to this category.
- *Supply System Threats:* Supply system threats refer to harm caused by an interruption in any form of energy supply (electrical power, water, gas) that affects the computer systems of an organization.

The defensive mechanisms against these threats must be implemented following a layered approach so that a threat needs to traverse multiple controls before harming an asset. Physical security should also include both security and safety controls. As a matter of fact, the first goal of a physical security program is to safeguard employee life. If employees feel safe, they can focus on their responsibilities and be more productive. In addition, physical security needs to provide the security triad (availability, integrity, confidentiality) for the resources and information assets within an organization.

Physical Security Program

Very similar to an information security program, the first step in creating a physical security program is to perform a risk assessment. The risk assessment will show the gap in terms of vulnerabilities, threats, threat agents, assets and business impact between the current status of the organization and the acceptable risk level depending on the regulatory domain that governs the organization. Regardless of the industry and the characteristics (size, location, etc.) of the organization, any reputable physical security program should include the following elements:

- *Policies and Procedures:* Policies and procedures form the foundational blocks of a physical security program. They define the security controls that should be in place and should therefore be used as a reference to fill the controls gap identified during the risk assessment. Policies and procedures should be written keeping existing laws and regulations in mind. Additionally, policies should address legal issues such as liability issues, assets and employee safety. Furthermore, organizations based in the U.S. need to ensure that their policies address compliance with environmental requirements such as those defined by Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA).
- *Deterrent Controls:* Deterrent controls are typically used to prevent or, at the minimum, discourage any attempt of breach or intrusion (e.g. fences, security guards, mantraps, warning signs, dogs, etc.).

- *Delaying Controls:* Delaying controls (e.g. locks, access controls) have the primary goal of slowing down the intruder in achieving his/her objective.
- *Detective Controls:* Detective controls are useful for early detection of incidents (e.g. CCTV, smoke and fire alarms).
- *Incident Response Controls:* Incident response controls include the personnel (e.g. security guards), security mechanisms (e.g. fire suppression systems, backups and alternate power supplies) and procedures that help respond to detected incidents and assess the damage. The procedures should address, at the least, the emergency response process (e.g. emergency roster), law enforcement notification and external consultations.
- *Auditing Controls:* Audit logs recording physical access to the facility and all restricted areas should be maintained. All visitors and employees including external consultants, contractors and temporary employees should be asked for an identification document prior to entering such areas. Logs of audit trails should be able to uniquely identify each attempt of access. Therefore, each audit trail should record, at least, the following information:
 - Date and time of the access
 - Area of access
 - The user ID or identification document used
 - Whether or not the access was successful

Logs should be reviewed on a regular basis in order to detect suspicious activity. Audit trail logs are also an effective means to monitor access to different areas and resources.

A sound physical security program should include planning for additional elements such as heating, ventilation, air conditioning, water and gas lines, ceilings, windows and flooring to ensure the facility's stability, and the safety and protection of employees and assets.

It is important to plan a physical security program in a dual-mode: the first should be organized during regular office hours and the second when the facility is closed. The latter requires the activation of all safety and security mechanisms, monitoring controls and the surveillance of suspicious activities by security personnel. During office-hours, monitoring becomes more complex, particularly since it is necessary to distinguish from those who are and are not authorized to access the resources of an organization.

Periodically, organizations should measure the effectiveness of their physical security program and the controls in place. The measurements can be performed on the basis of various metrics such as:

- Number of successful crimes or disruptions
- Number of unsuccessful crimes or disruptions
- Time between detection, assessment, and recovery steps
- Business impact of disruptions
- Number of false-positive detection alerts
- Time taken by a criminal to defeat a control
- Time taken to restore the operational environment



Laptops, PDAs and Blackberries

Stolen equipment such as laptops, PDAs and Blackberrys pave the way for the leakage of sensitive information and public embarrassment. To avoid such events, organizations must implement policies and controls that ensure the physical security of their equipment. By acknowledging the simple precautions listed below, organizations can reduce the leakage of information and theft:

- All the laptops, PDAs and blackberries should be registered with their respective vendor. The vendor should be notified immediately when a device is stolen so that they can track it down easier.
- An up-to-date inventory of all the laptops, PDAs and blackberries along with the people who are in possess of the equipment should be maintained and updated accordingly.
- Laptops should have the BIOS protected by a password, the operating system hardened and all the sensitive data encrypted.
- When traveling, laptops, PDAs and blackberries should be never left unattended and laptops should never be checked as luggage.

Regulatory Compliance

Physical security plays an essential role in compliance. Typically, organizations designate a Facilities Safety Officer to protect assets and employees, and ensure compliance with the organization's physical policy, laws and industry regulations. Let us take a look at some of the well-known regulations that govern physical security today:

Sarbanes-Oxley (SOX)

Sections 302 and 404 of the Sarbanes-Oxley Act require management to establish and maintain effective internal controls. The sections also mandate management to ensure on internal controls and procedures for financial reporting. While these sections do not directly refer to physical security controls, or for that matter, even information security in general, it is implicit that these type of controls need to be included in the review of the security of financial information systems. Physical security is the first layer of security in ensuring that only authorized users can physically access financial information systems and the information residing on them.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Security Rule lays down security safeguards in the form of physical measures that must be implemented by organizations that process or facilitate the processing of ePHI (Electronic Protected Health Information). Specifically, the HIPAA Security Rule was enacted to ensure the confidentiality, integrity and availability of ePHI and its protection against reasonably foreseeable threats or hazards. HIPAA requires physical access controls in the facilities that house customer information systems to restrict access only to authorized personnel and also to prevent authorized employees from providing customer information to unauthorized/malicious individuals.

Organizations must specify policies and procedures that detail the restrictions on workstations that access ePHI, the functions performed by them and their environmental attributes. The HIPAA Security Rule suggests enforcing physical security around all workstations that have access to ePHI.

Policies and procedures must also ensure the proper use, handling and disposal of electronic media that hold ePHI, including the transfer of such media between different facilities of the same organization.

Additionally, HIPAA outlines the need to have incident response programs in place that define the exact actions to be taken in the event that a financial institution faces or suspects a security incident related to customer information or the system(s) on which it resides. Such incident response programs must define guidelines for informing appropriate law enforcement agencies of the incident or suspected incident.

Graham-Leach-Bliley Act (GLBA)

Section 501(b) of the GLBA was set up to ensure that financial institutions adopt suggested administrative, technical and physical safeguards to:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats/hazards to the security or integrity of customer information.
- Protect against unauthorized access to or use of customer information.

Banks and financial institutions are encouraged to implement physical security controls that restrict access to customer information only to authorized employees who have a valid business need for accessing such information. Further, physical security controls are needed to ensure the availability and safety of customer information in the event of any kind of damage or loss due to environmental hazards, such as fires, floods or technical failures.

Homeland Security Presidential Directive/Hspd-12

The HSPD-12 mandated by George W. Bush requires Federal facilities and other facilities, which may be potential targets of terrorist attacks, to implement secure and reliable forms of identification for Federal employees and contractors before providing physical access to controlled facilities and logical access to controlled information systems. The directive titled "Policy for a Common Identification Standard for Federal Employees and Contractors" requires identification controls as outlined below:

- Effectuate a reliable and efficient mechanism to verify and authenticate employee identity.
- Are resistant to identity fraud, counterfeiting, tampering and terrorist exploitations.
- Are issued by a reliable and accredited provider.

The directive requires Federal departments and agencies to comply with the standard no later than eight months after the date of promulgation.

FIPS PUB 201-1

The FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors standard defines the minimum requirements to meet the HSPD-12 security objectives. It also provides technical specifications to implement a PIV platform that can support a suite of authentication mechanisms and ensure interoperability among Federal departments and agencies. The PIV platform requires the usage of several physical controls such as PIV cards, card and biometric readers, and personal identification number (PIN) input devices.

PIV Cards are smart cards that the holder uses for authentication to various physical and logical resources whose access is safeguarded by biometric and PIV card readers. These readers compare the biometric data stored in the memory of the card with real-time biometric sample data. The level of protection can also be increased with the use of PIN numbers to control access to information on the card. The combination of these controls provides a tri-factor authentication: something you know (the PIN), something you have (PIV Card) and something you are (biometrics).

Conclusion

Physical security entails a wide array of controls and deals with various types of threats such as natural disasters, intruders, and human errors. Organizations need to have an ongoing physical security program in place that addresses all the issues and requirements outlined by laws and regulations. The physical security program should be planned carefully considering the areas requiring higher priority and the types of threats endangering the assets. As for any other security project, it is essential to have the support of senior management throughout the project's lifecycle and the availability of necessary resources. Although, physical security is often overlooked compared to network and systems security, the consequences of an intruder gaining physical access to a server room, or of a fire that is not immediately suppressed might just serve to help you realize the importance of this aspect of security.

Enterprise Risk Management At A Glance

ERM professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

Education

Qualifications

M. S. in Computer Information Systems
M. S. in Information Networking
M. S. in Management Information Systems
Master of Accounting Information Systems
Master of Business Administration

Universities

Carnegie Mellon University, Pittsburgh, Pennsylvania
Syracuse University, Syracuse, New York
Xavier University, Cincinnati, Ohio
University of Miami, Miami, Florida
Florida International University, Miami, Florida

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Microsoft Certified Professional

Prior Work Experience

PriceWaterhouse Coopers
CERT® Coordination Center
SONY Electronics Latin America, Inc.
RJR Nabisco
Diageo plc
Arthur Young
Carnegie Mellon CyLab
Evertec Inc.
American Bankers Insurance Group
Chesebrough Pond's
Starboard Cruise Services, Inc.
Demotte Consulting, Ltd.

Some of our Clients...

ABN AMRO Private Banking
Bacardi-Martini, Inc.
CitiBank
Carnival Cruise Lines
Commerce Bank
Florida Power & Light Company
Knight Ridder
North Broward Hospital District
Ocean Bank
Rinker Materials
Sylvania Lighting International
The International Bank of Miami

KEEPING WATCH OVER YOUR BEST BUSINESS INTERESTS

enterprise risk management

The Control Professionals

800 S. Douglas Road, North Tower (# 835),
Coral Gables, FL 33134.
P: (305) 447 6750 F: (305) 447 6752
Email: info@emrisk.com Web: www.emrisk.com