SOBEL & CO. LLC
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Security 101: Physical Security Requirements for Information Security System

By James G. Mottola, Director, Forensic Investigations/Litigation Support, Sobel & Co.

In the alphabet soup of agencies, organizations and governments each having their own set of standards, compliance requirements and laws mandating business to protect various types of consumer information, wouldn't physical security be last thing to look at?

The answer of course is a resounding NO.

On the contrary, it should be the first thing to address, because physical security of information systems is the foundation for the protection of critical data held by any organization. It is the place where digital information is stored and transmitted with each of the assorted criterion requiring physical security as part of cybersecurity. These standards, when addressed properly, can meet the goals of business owners in satisfying compliance requirements and also provide a basis for security awareness, human behavior and good cyber hygiene, effectively protecting them from financial loss.

M'mm M'mm Good!

The basis for the implementation of comprehensive information security program begins with the two benchmarks, the National Institute for Standards and Technology (NIST) and the International Organization for Standardization (ISO). Each addresses physical security obligations for information systems within the framework of cybersecurity. Businesses should also be aware of the unique standards to physically secure specific types of protected data, such as credit card, customer financial and medical information. The Payment Card Industry Standard, Data Security Standard (PCI-DSS) , Graham Leach Bliley act (GLB) and Health Insurance Portability and Accountability Act (HIPPA) each has their own set of physical security standards which are compliance based or mandated by law for organizations to follow depending on the type of business and information under management. Entities found in violation of these requirements can be the subject of fines and penalties by a governing body such as the PCI Security Standards Council in the case of (PCI-DSS), the federal government in the case of (GLB), the Federal Trade Commission (FTC), and for the protection of health care information (HIPPA), the Department of Health and Human Services (HHS).

Self-Assessment

An information security program should begin with a self-evaluation by business owners to identify what type of information they are responsible for securing. Here are a few questions to get the ball rolling:

- Do you have any customer financial and/or health care information?
- Do you process customer credit cards or other electronic payments?

If no, do you possess any other information that if compromised, would affect your ability to serve your clients?

If yes to either question, where and how is the information processed or retained?

- Are you aware of your responsibilities, legal and regulatory, to maintain protected information?
- What guidelines or standards do you follow to secure it?

- Do you have a process to secure information from the moment you acquire it to the moment you effectively discard it?
- Are your employees aware of these obligations or processes? Do you conduct training?

Once again, a review of the above mentioned standards provides guidance that can assist a business in identifying the type of information and obligations required to remain secure. The good news for businesses is that physical security solutions as part of this process are generally affordable and easily implemented from an environmental controls perspective. However, there are some items required by these standards that may not be as obvious, so a deeper dive is warranted.

Strategic View

The concept for the implementation of environmental controls begins with the moment any item or object under a business' control has physical contact with information, until the information itself or the device, which maintains that information, is destroyed without any discernable evidence or identification of the protected data. In practical application, protecting any object that transfers, processes or retains data such as cables, routers, servers, laptops, desktops, printers, faxes, filing cabinets, etc., is part of the environment which needs to be physically protected. In some cases, these standards specifically mandate that a business have a plan to maintain client access to data in the event that an information system has been compromised and requires a backup contingency.

In Plain Sight

Listed below are a sampling of the requirements derived from the various standards to provide examples of topic areas business' need to consider:

- Server Room: Secured/Unmarked/Limited Access
- Cables Location: Markings and Documentation
- Alternate Transmission Access
- POS System: Segregation/Encryption/EMV
- Emergency Mode Operations Plan: Recovery of Lost Data
- Remote/Physical Access: Third Parties
- Access Control Logs: Logical Security Systems/Video
- Internal Documents: Protected Information Log
- Reporting of Theft Damage: Notification Policies

Below are a few remedies to address physical security of information systems:

- Review of Protected Data: Compliance Requirements
- Clear Screen Policy
- Password Management: (Sharing) Unique User Sign On
- Authorized Machines: Rule of Least Privilege
- Clean Desk Policy: Locked Draws and Files
- Inventory of Physical Devices
- Limited Access to Offices/Rooms

- Alarms/Cameras for Key Areas
- No Off-Hours Access to Unauthorized Personnel
- Physical Penetration Testing
- Documentation of Policy Violations
- Quarterly Review with Stakeholders
- Annual Employee Training and Review of Policies
- Digital File Back Up/Physical Files/Offsite
- UPS – Source – Damage Back Up
- Fire Suppression Systems
- Off-Site Maintenance/Review of Equipment/3rd Party (Cloud)
- Off-Site Transit of Information Systems (Documentation)
- Proper Disposal of Information Systems (Documentation)

Food 4 Thought

Physical security systems comprised of access controls devices use information systems for a variety of functions just like any user application. Securing, monitoring and maintaining those systems themselves should also be part of any information security program.