Physical Security: The Weak Link in Internal Control Design?

Richard T. Henage, Ph.D./CPA
Westminster College
U.S.A.

Dan Henage, CISSP, PCI QSA,CPA
Mountain America Credit Union
U.S.A.

Abstract

This paper addresses physical controls as an integral part of any internal control system. As an auditor of physical controls, one of the authors details the structure of physical control design and the most common physical control weaknesses found in the audit of internal controls. The importance of preparing students to understand physical controls is emphasized.

Introduction

An integral component of designing any accounting information system is building internal controls into the design. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission stressed in their 1992 report that these controls be integrated into, not added onto, system designs. “Internal control is most effective when embaedded in the entity’s infrastructure and its ongoing activities.” (COSO 1992)

Under “Business Process Control Activities,” COSO 1992 requires that the control activities include “Physical Controls – Equipment, inventories, securities, cash, and other assets are secured physically (i.e., in locked or guarded storage areas with physical access restricted to authorized personnel.)”(COSO 1992) “Assets include tangibles such as hardware and software and other physical items such as buildings. Assets also include intangibles such as information, intellectual property and company good will.” (Seider 2004)

Most accounting information systems textbooks provide detailed coverage of control procedures (such as segregation of duties, authorization of transactions, monitoring, etc.). Additionally, a great deal of emphasis is placed on protecting information on computer systems with password controls, data backups,firewalls, and antivirus software. Coverage of physical controls is woefully brief in comparison.

The coverage of physical controls may be weak because both professors and textbook authors come from accounting and information system backgrounds and, while they may be experts in procedural controls, they have little experience with physical security. While they might understand that access to important assets must be restricted with physical controls such as locks and alarm systems, they often lack the expertise to identify whether or not such controls are sufficient.

Partly as a result of the Sarbanes-Oxley Act of 2002, all of the major audit firms now offer penetration testing as a means of determining whether access to confidential information is sufficient. Although the act does not specifically require penetration testing, it does require an “assessment as of the end of the recent fiscal year of the issuer, of the effectiveness of internal control structure and procedures.” (SOX 2002)

Other organizations are more specific in their requirement of penetration testing. ISO/IEC 27001:2005 requires that “information systems should be regularly checked for compliance with security implementation. Compliance checking also covers, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts contracted for this purpose.” (ISO/IEC 27001:2005)The PCI DSS (Payment Card Industry Data Security Standard), to which compliance is mandatory for every business that accepts payment cards, requires that organizations run internal and external network vulnerability scans at least quarterlyand perform internal and external penetration testing at least once per year. The PCI DSS dedicates an entire requirement to physical security controls, covering video cameras, access control mechanisms, access badges, visitor procedures, secure data destruction, and access to computer equipment and data storage. (PCI DSS 2010)

Penetration testing involves attempts by the auditor to breech an organization's security to gain unauthorized access to systems or information. Such tests usually include both social engineering (attempts to influence employees to divulge sensitive information or perform an action to circumvent security) and system attacks (attempts to breech software controls by exploiting program weaknesses.)

A handful of firms are also offering physical penetration testing. In a physical penetration test, the auditor will attempt to gain access to data centers, network equipment, desktop computers, hard copy files, and valuable assets.

Similar to penetration testing for data controls, the purpose of physical penetration tests is to identify weaknesses in the physical controls of the organization. Physical penetration tests involve both social engineering tests and attempts to bypass physical controls.

The purpose of this article is to identify some of the primary weaknesses found in many physical control designs. One of the authors of this paper spent over five years performing penetration tests, with a specialty in physical security tests, for a major, international accounting firm. The balance of this article is dedicated to identifying major physical control weaknesses common among many business and governmental and non-profit organizations. These physical controls that often show weaknesses are organized into three major categories: physical access barriers,alarm systems,and human-based control procedures.

Physical Access Barriers

A physical access barrier is any physical structure that impedes or restricts access to valuable assets to those who have authority to gain access. In its simplest form, it would include locks on doors. However, as the value of the asset and the risk of loss increases, the sophistication of the physical access controls should also increase. This can easily be seen in banks where supply closets may be secured with only locks on door knobs while large stockpiles of cash are secured in vaults with time locks.

Door locks come in a variety of grades. Most inexpensive door locks are easily breeched by anyone with a rudimentary knowledge of lock picking. The standard home door lock with a row of five pins can be picked or bumped open by a locksmith in not much more time than it takes an authorized entrant with a key. A high security lock may include additional side wards to obstruct the keyway, special keys with pits on the sides, and security pins that make picking or bumping more difficult.

In the author's experience, the most common problems in restricting access with locks lie not in the locking mechanism, but with the door. Large spaces surrounding the door (above, below, to the side, or between double doors) allow the attacker to gain access to locking mechanisms with little effort. For example, a push bar on a door can often be exploited from the outside by sliding a bent wire through available gaps and pulling back on the push bar. Gaps under the door may allow the attacker reach under the door to pull down the interior handle to open a door. A gap may allow the attacker to insert a flag beyond the door and activate a motion detector to unlock the door. The seals around a door need to be tight enough not to allow a wire to pass through any gap.

Another common mistake is to install a door with the hinges on the outside of the door. Unless special security hinges are used, an attacker may easily pop the pins on the hinges of a locked door and swing it open. Additionally, both the door and the door frame must be of a sturdy material that will resist pressure.

Ideally, windows should be locatedso that breaking a window will not allow access to locking mechanisms. Additionally, windows should either be designed in manner that an attacker would not be able to access the room through the opening (small openings) or made of unbreakable materials. If a window is such that breaking the window would allow access to the secured area, then alarm systems that sense breakage should be used to add additional security.

Windows are not the only weak points. Weak walls can also allow easy access to a secure area. Additionally, it is crucial that walls around secure areas extend beyond drop ceilings and below raised floors. If this is not the case, the attacker can easily remove a ceiling (or floor) tile to go over (or under) the wall and into the secured room.

Locks should undergo regular inspection and maintenance. Locks on doors that can be shut while locked often have a security tab on the bolt that prevents an attacker from opening the latching mechanism with a credit card or flat blade. (The security tab is the second small bolt behind the main bolt. When a door is closed, the strike plate prevents the security tab from extending with the main bolt, locking the main bolt in place.) In some cases, locking door knobs have been installed using bolts that do not have a security tab. Another common problem is non-functioning or missing security tabs. The locking mechanisms should be inspected on a regular basis, and lubricated and repaired as needed.

For doors secured with magnetic locks, make certain that the wiring to the lock is not accessible from outside the secured area. If an attacker can access the wire, such as by cutting through drywall, then he can simply clip the wire to kill the power to the magnetic lock, disabling it. Without a form of backup power, turning off the power to the building at the electric box can disable magnetic locks.

It is also crucial to remember that security is no better than the weakest link. An attacker is going to look for the easiest access point, be it a door or window. This includes doors and windows that can be assessed from balconies and the roof top.

Access control also includes protecting access to keys. Keys for doors, cabinets and safes must not be stored in nearby desk drawers. If master keys are stored in a manner that allows access by fire departments, security guards, or management, the box should be installed in a recessed cavity and highly secured.

Alarm Systems

While physical-access barriers help prevent attackers from reaching protected assets, the purpose of alarm systems is to detect a breech. Prominent cameras and posting signs that alert potential attackers of the presence of alarm systems and monitoring may serve as a deterrent to attacks. For this reason, it is not only important to have functioning alarm systems, but to also let the public know that the premises are secure.

If an alarm system is present, it is important that it is also functioning properly. A well-designed alarm system will include a variety of intrusion detection devices. These may include sensors for open doors and windows, glass breakage sensors, motion detectors, infrared sensors, and smoke detectors. The alarms should be monitored and tied to procedures for rapid response from emergency personnel, private security guards, or internal security personnel. The alarm system should be regularly maintained and tested to ensure that it is functioning properly at all times.

It is important that when a breech is detected that a careful examination of the premises is conducted. Each room should be individually cleared. If multiple alarms are detected, a guard should be posted on sight until the error in the system is detected and remedied. A good alarm system should alert security personnel as to the exact location and type of breech detected.

Cameras can be effective alarm devices when configured for motion detection. Cameras should be positioned around all entry/exit points of a facility and concentrated in high risk areas. If they are used, they should be recorded to a secured location (such as off-site) and stored for a minimum of three months. Effective use of cameras includes having the camera monitored. Additionally, if the monitoring is done off-site or over a wireless connection, it is important that the signals are encrypted. An attacker that is able to tap into an unencrypted signal can monitor the video feeds to turn the organization’s security system against itself.

Security codes for alarm systems should be secure. Many businesses leave the security code set to the factory default. The codes should not be easy to guess (such as 1234 or 1111). Ideally, each employee that has access should be given their own code. This allows the business to determine who disarms the alarm system at a given time. It is crucial that these codes be immediately changed in the event of the termination of an employee. The key pad should also be placed in a position where it is difficult for an observer to “shoulder surf” to see the codes as they are input.

Human-Based Control Procedures

A key component of any physical security design is training and monitoring employees to react to threats to the security of the business. Even if all of the physical control mechanisms are functioning properly, it is possible that breeches are allowed by employees who have not been properly trained or who are lax in the performance of security procedures.

Ideally, access to the facilities of an organization should be restricted to those who have a valid business purpose. If the organization is large enough that all of the employees do not know each other, security can be improved by requiring employees to wear security badges that identify their position. These should bear a current photo of the employee and be easily identified as belonging to the organization. Visitors should sign a log at reception, be provided with a visitor pass that expires, and should be escorted through the facility. If a visitor is to be unattended, they should be seated in a common waiting area.

In many cases, there may be a need for public access to the premises. For example, retail stores, colleges, hospitals, and many government facilities may have a large volume of public traffic during daytime hours. If this is the case, the building should be systematically cleared at the end of business to verify that no unauthorized individuals are in the building after hours. Further, high security areas such a cashier's office or server room should be off-limits and monitored.

It is crucial to have employees understand their role in internal security. The use of security badges is only effective when employees are trained to stop individuals not bearing proper ID. Employees should have a contact in the firm (such as the security office) where any suspicious behavior should be reported. Every phone should have emergency contact information readily available. Employees should report suspicious behavior or whenever they see unfamiliar people in areas where the public is not invited.

A common means for an attacker to breech the security of a facility is through a process known as piggybacking or tailgating. If a door is secured by a lock, it is important that no employee allow followers to enter behind them without having them unlock the door by themselves. If an employee has someone with whom they are unfamiliar piggyback on their entry to a secured area, the event should be immediately reported to security personnel.

Finally, it is important that employees not disclose confidential security details to unauthorized personnel. The author has seen alarmingly high percentages of employees that can be talked out of passwords and access codes, talked into running software to secretly create a back-door into systems, or talked out of reporting suspicious behavior with the flimsiest of excuses. Any such inquiries or events should be referred to the appropriate office and any requests for such information should be denied. No employee should ever be reprimanded for holding tight to security procedures and referring the subject to one with the proper authority to make such a decision.

Conclusion

Physical security is an area of high interest for most students. Students have been exposed to a variety of entertainment focused around crime and espionage. Many students are fascinated by the methods used to prevent authorized access to valuable assets. Presenting the basics of physical security controls as an integral part of internal control design should serve to heighten the interest of students.

More importantly, students should understand their role in the security procedures of a business. Through conducting dozens of penetration tests for a wide variety of organizations, the author has found that the vast majority of employees are unconscious of basic security measures. For example, most employees will ignore unauthorized personnel in secure areas, will give out security details to anyone with a persuasive story, and will accept excuses for inappropriate behaviors. Adequate coverage of these issues should increase the value of students upon their entry to the marketplace.

References

Committee of the Sponsoring Organizations of the Treadway Commission (COSO).1992. *Internal Control – Integrated Framework.*New York: American Institute of Certified Public Accountants.

ISO/IEC 27001:2005. *Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland. International Organization for Standardization.

Payment Card Industry Data Security Standard (PCI DSS). October 2010. *Requirements and Security Assessment Procedures, Version 2.0*. Wakefield, MA: PCI Security Standards Counsel.

Seider, Dan. 2004 *Sarbanes-Oxley Information Technology Compliance Audit of an Outsources Microsoft and SAP System for a Specialty Manufacturer*. Las Vegas: SANS Institute.