CHAPTER

34 Physical Security

Traditionally, physical security has remained completely segregated from the IT world, but as technology continues to displace paper and manual processes, physical security is increasingly becoming more IT centric. The IT and physical security worlds are quickly converging, and the proactive IT manager would be wise to embrace this convergence. The goal of this chapter is to address everyday physical security topics, concepts, and practices as they relate to the day-to-day security practitioner with a network security background.

Classification of Assets

Classification of assets is the process of identifying physical assets and assigning criticality and value to them in order to develop concise controls and procedures that protect them effectively. These asset categories have inherent and common characteristics that allow you to establish baseline protective measures by category. The classification of corporate physical assets will generally fall under the following categories:

- **Computer equipment** Servers, network-attached storage (NAS) and storage area networks (SANs), desktops, laptops, tablets, pads, etc.
- **Communications equipment** Routers, switches, firewalls, modems, private branch exchanges (PBXs), fax machines, etc.
- **Technical equipment** Power supplies, uninterruptable power supplies (UPSs), power conditioners, air conditioners, etc.
- **Storage media** Many older systems use storage media devices like magnetic tapes, DATs, CD-ROMs, and Zip drives, so it is still good to be familiar with them. Most systems today use hard drive arrays, solid-state drives or thumb drives, and the various types of memory cards such as Secure Digital (SD), microSD, Compact Flash, and Memory Stick, to name a few.
- **Furniture and fixtures** Racks, NEMA-rated enclosures, etc.
- **Assets with direct monetary value** Cash, jewelry, bonds, stocks, credit cards, personal data, cell phones, etc.

Value and business criticality of assets should be assessed and documented. For critical assets, the following minimum criteria should be included in your matrix: depreciative value, initial cost, replacement cost, asset owner, vendor, version, and serial number (if applicable). This information can normally be gleaned from business continuity and disaster recovery documentation. If you don't have a disaster recovery or business continuity plan in place yet, this exercise will help quite a bit when the inevitable time comes to draft it (as discussed in Chapter 32). "Low/Medium/High," "Not Important/Important/Critical," or a similar, numerically based scoring and weighing system can be used effectively to assign protection priorities to assets.

Physical Vulnerability Assessment

A physical security vulnerability assessment, much like its information security counterpart, relies upon measurements of exposure to an applicable risk. An asset must already be classified, and its value to an organization must be quantified. Once this is accomplished, a simple walk-through should be performed as a starting point to identify potential areas of physical security laxness. For example, is that network connection in the reception area or public conference room active? Is Wi-Fi connectivity available for visitors? If so, is it getting an IP address via DHCP? Is it segmented on a VLAN? Is a username and password combination required to log in? Identify the problem, but also assess what (if any) business need justifies its existence. If a legitimate business need does not exist, or the risk exceeds any potential return, it's a liability for that condition to exist and it should be remediated. Four main areas should be a part of any physical vulnerability assessment: buildings, computing devices and peripherals, documents, and records and equipment. Your situation may vary, depending on various factors.

Buildings

Take a walk around the building and look for unlocked windows and doors. Check for areas of concealment/obstruction such as bushes/shrubs directly beneath windows. Check for poor lighting conditions. Are you able to tailgate into the building behind someone without being challenged? Can you walk in through an unattended loading dock entrance? Once inside, are you challenged for identification? Are building passes displayed prominently and collected after the visit is concluded?

Computing Devices and Peripherals

Verify lockdown and accessibility of systems and peripherals. Unattended systems should be logged off or have their screens locked. For servers, the minimum criteria that apply are these:

- Place critical servers in a locked room that utilizes a card reader to gain entrance. This provides an audit trail of everyone who enters the room and limits entry to only those who are authorized. Due to space or business limitations, it may not always be possible to place *all* of your servers in a locked room. One example of this might be product test or development environments. In situations such as these, logical isolation of systems may suffice. Bear in mind that if this method is used, it is imperative that mitigating controls, such as data and network segmentation from critical data, be maintained at all times.

- Make sure that the case has a physical lock.
- Password-protect the BIOS with a complex password.
- Disable system booting from floppy/CD/DVD/USB drives in the system setup.
- Position the monitor and keyboard such that neither is visible to anyone else except the operator. You don't want someone watching when an administrative password is typed in.
- Remove or disable unused modems and network ports.
- Store tools separately, preferably locked up.
- Limit the number of people with access to the server room, and document their access. Place a sign-in sheet inside the door, or electronically track access with a card reader or biometric entry control.

Documents

Documents should already be classified as part of your data classification and information owner matrixes and policies. Look for Confidential or "Eyes Only" documents lying around, Post-it notes with passwords and credentials, documents not collected from print jobs and faxes, and documents in the trash or recycle bin that should have been shredded. Take a walk around and see if you can successfully "shoulder-surf" confidential or restricted information. People will generally assume that you don't care about what they are reading. This is a dangerous assumption. Take the time to educate your employees on corporate espionage techniques, and ensure that they understand the consequences to what may seem like a harmless situation at the time.

Records and Equipment

The category of records and equipment deserves the same consideration as any other crucial asset. No matter how dependent we become as a society upon electronically storing and processing records, there will always be the file cabinet containing paper records. Records differ slightly from documents in that records encompass anything of record. Employee timesheets, receipts, accounts payable/receivable, and so forth are all forms of records. Make sure records are locked up when not in use and are accessible to only those authorized to access them. Equipment items such as faxes, printers, modems, and copiers and other equipment have their own security recommendations, depending upon their use and location. Does your CEO leave his smartphone or tablet sitting unlocked on his desk, with his office door wide open, when he goes to lunch? In this situation, even though his workstation may be locked, his e-mail is still accessible.

Choosing Site Location for Security

As they say in real estate, "Location is everything." When it comes to physical security this particular saying hits close to home. When choosing a location for a data center or office site, survivability should be considered more important than cost. Low-cost sites may have risks associated with them that outweigh their cost savings. If the site is in a flood zone, an

area likely to be hit by a tornado or hurricane, an earthquake zone, or high-crime area, there is a significant risk that one of these events could cause a lot of expensive damage. A well-designed and well-maintained site will have a backup power generator, security guards, and other compensating factors, but you don't want to have to use them. And if you do, they can be expensive. So choosing a secure and reliable site location makes sense from a financial perspective as well as from the security point of view.

There are many security considerations for choosing a secure site location, a few of which are

- Accessibility
  - To the site
  - From the site (in the event of evacuation)
- Lighting
- Proximity to other buildings
- Proximity to law enforcement and emergency response
- RF and wireless transmission interception
- Utilities reliability
  - For a data center, the loss of power may be overcome through the use of generators, but if the water supply is cut off, the AC units will be unable to cool the servers
- Construction and excavation (past and present)

Let's consider each of these briefly to address applicability to common business environments.

Accessibility

Accessibility of the site is typically the first consideration, and with good reason. If a site is located too remotely to be practical, usability and commutability are affected. However, by the same token, if the site is accessible easily to you, it probably is to others also. Conversely, you must consider potential evacuation. For example, bomb threats, fires, terrorist attacks, anthrax mailings, and SARS are potential catalysts for evacuation.

Lighting

Proper lighting, especially for organizations with 24×7 operations, should be evaluated and taken into consideration. Threats to employee safety, as well as the potential for break-ins, are more common under poor lighting conditions. Establish from the outset as many physical barriers between your business environment and undesirable people and circumstances as practical. Mirrored windows or windows with highly reflective coatings should face north-south rather than east-west to avoid casting sun glare into trafficked areas. Lighting should be positioned in such a way that it never blinds those leaving the building at night.

Proximity to Other Buildings

Know who your neighbors are. For instance, sharing a building with a branch of law enforcement would be considered less of a risk than sharing a building with "XYZ Computer Ch40s Klub." The closer the proximity to other buildings and companies, the higher the probability is for a physical security incident to occur. Also consider the fact that whatever problems an adjacent or connected building might have could potentially become *your* problem as well.

Proximity to Law Enforcement and Emergency Response

Another consideration is the location's relative proximity to law enforcement and/or emergency response units. If the area has a history of crime, but you've chosen the site anyway, consider the possibility that the incident may not get a response within a framework that you consider ideal. Similarly, if an emergency service unit were to be called to respond to an incident at this location, consider what the impact would be for any delay and if this latency in response would be justified.

RF and Wireless Transmission Interception

As wireless networking becomes more prevalent, especially in metropolitan areas, wireless hacking and hijacking become more of a threat. Other "airborne" protocols that should be taken into consideration include radio frequency devices, cordless phones, cell phones, PIMs, and mobile e-mail devices. Test drive for existing protocols with scanners, and avoid heavily trafficked frequency ranges wherever possible. Using encryption for sensitive traffic is indispensible.

Utilities Reliability

Office buildings provide work space for employees who need to be productive and reliable in their work. Power outages can seriously interfere with productivity, as can phone service and network outages. Some of these things can be compensated for, but some can't. For example, power outages can be compensated for with the use of UPS systems and a generator—up to a point. UPS batteries only last for a short time, and generator fuel can be expensive and difficult to get in a serious emergency. Phone, network, and Internet service can be more problematic. If they go down, you can often switch to another provider—but not always. The "last mile" is always a problem. If there are reliability problems in the connection between your site and your provider, due to old wiring, bad fiber, or construction events like a "backhoe failure" (in which a digging machine cuts through your building's communications cabling), there's not much you can do until the wiring is repaired. Downtime can be expensive.

For a data center, loss of power can have a serious impact. UPSs and generators can supply power for a while, but systems in the data center need to be constantly cooled or they will melt down. More than one organization has had to replace a lot of expensive equipment due to AC failure.

Construction and Excavation

Construction and excavation can take your entire network and communications infrastructure down with one fell swoop of a backhoe's bucket. Take a look at past construction activities in the area, and the impact (if any) that they had on the immediate vicinity. Town or city records will usually provide the information you need regarding any construction/excavation/demolition, both past and present. Make it a point to ask people in the vicinity about power/telecom outages.

Securing Assets: Locks and Entry Controls

This section discusses a few of the many different factors you should consider when securing your assets with physical security devices.

Locks

Locks aren't just for doors anymore. Anything of value that is capable of "growing legs and wandering away" should have a lock or be secured in a location that has a lock. Your physical security vulnerability assessment probably came across a few unsecured laptops, smartphones, tablets, MP3 players, jewelry, keys, and other assorted items. Lock up the device or valuable and make it a point to educate the asset owner on the importance of securing the item.

Doors and File Cabinets

Check for locked doors where applicable; you'll be surprised at the results. Make sure the lock on the door functions correctly and can withstand sufficient force. A broken or nonfunctioning lock is only slightly better than no lock at all. File cabinets containing sensitive information or valuable equipment should be kept locked when not in use. The keys to these should also be kept out of common reach.

Laptops

Laptops at the office, when not in transport, should be physically locked to the desk or in the docking station. Cable locks are a relatively small price to pay to ensure the laptop (and confidential information) doesn't fall into the wrong hands. Laptop theft is at an all-time high; most disappear right under the nose of the owner. One second it's here, the next it's gone. All personnel should be instructed to be especially wary when traveling with a laptop. For example, whenever going through a metal detector at the airport, keep your eye on the laptop bag at all times. Don't be afraid to tell the screener to stop the conveyor until you can get to it. If possible, transport your laptop using a bag that does not resemble a computer bag, such as those that resemble backpacks. In some areas, traveling with a computer bag is equivalent to taping a note on the side that says "Steal Me." Operating system security and software safeguards are only as good as the physical security protecting access to the device. If someone has unlimited physical access to a system, half the battle is already over. From there, it's only a matter of time before these safeguards are overcome. One example of this is using a Linux boot disk to reset a Windows Administrator account password.

Data Centers, Wiring Closets, Network Rooms

All of these areas should have common access controls, as they all perform a similar function. Make sure these rooms are kept locked. If automatic entry-tracking mechanisms are not in use, ensure an access log is kept.

Entry Controls

Entry controls have their own security considerations that will undoubtedly vary with your security plan and business needs. When looking at the various options, you must first consider the site in which the entry controls will be deployed. Some of the most common types of deployment scenarios are for an existing structure with a single tenant, for a suite in a multitenant building, for a campus group of buildings with specific public entrances, and for a high-rise building.

Building Access Control Systems

For existing structures, there may be equipment already in place that can be reused. Multitenant buildings typically have access control systems that control entrance into the building or entrance to a special parking lot that is common to the entire building. If you plan to implement an access control system that is not compatible with an existing system, multiple access cards may be necessary. Many of the access control systems can support many of the card technologies, and there are even cards that support multiple types of technology and can work on several different incompatible systems.

The most important factor when dealing with a multitenant building is to make sure that you never have to allow anyone from the unsecured side of the suite to pass into the secured side unless they are authorized to do so. This can be difficult in multitenant buildings that lack a "Z corridor"—a public corridor that links two stairwells to the elevator lobby. The freight elevator should also exit into this public space. This ensures that the public, and other tenants, will not have to enter your suite to get to another part of the building. Most cities have building codes that require high-rise buildings to have a Z corridor on every floor, but in a building without that public corridor, there may be situations when you have to let people enter your suite unrestricted.

Mantraps

A *mantrap* is an area designed to allow only one authorized individual entrance at any given time. These are typically used as an *antitailgating* mechanism—to prevent an unauthorized person from closely following an authorized person through an open door, for example—and are most commonly used in high-security areas, cash handling areas, and data centers.

Building and Employee IDs

Typically, one of the first things any organization does after hiring new employees is to provide them with ID badges. Building and/or employee identification should be displayed at all times, and anyone who lacks a visible ID should be challenged. Far too often, an individual becomes friendly with the security guard and, eventually, the guard just waves them through without showing valid identification. What happens if that guard doesn't receive notification that the employee is no longer with the organization? Unfortunately, in most cases, the former employee is waved through as if she still works there. This situation has many security implications associated with it.

Biometrics

Biometric devices have come a long way in the past several years and continue to gain traction both in the entry control market and the network authentication market. A *biometric device* is classified as any device that uses distinctive personally identifiable characteristics or unique physical traits to positively identify an individual. There are many types of biometric devices, and use will be dictated by the situation. Some of the more common devices use one or more of the following characteristics or traits to confirm identification: fingerprint, voice, face, retina, iris, handwriting, hand geometry, and keystroke dynamics. For entry control, the most commonly deployed biometric technologies are currently fingerprint and hand geometry devices. The latest fingerprint readers now read the corpuscles under the skin, so they can be used for nearly everyone, even individuals who do not have strong fingerprint ridges. The recent trend of implementing fingerprint readers in commercial devices such as laptops and time and attendance devices has resulted in this technology becoming more cost effective.

Security Guards

The best deterrent seems to be security guards. But guards are not there merely as a deterrent. Here's what the New York State Department of Labor says a security guard's responsibilities include: "A security guard is employed by an organization, company, or agency to patrol, guard, monitor, preserve, protect, support, and maintain the security and safety of personnel and property. Security guards deter, detect, and report infractions of organizational rules, policies, and procedures. Security guards help limit or prevent unauthorized activities, including but not limited to trespass, forcible entry or intrusion, vandalism, pilferage, theft, arson, abuse, and/or assault." A security guard is not just a person but also a resource. Accordingly, guard placement, number, and use will be dictated by business requirements and needs. Background checks should be done for all security guards, and appropriate licenses and clearances obtained wherever applicable.

Physical Intrusion Detection

Physical intrusion detection, much like its information counterpart, requires forethought, planning, and tuning to obtain optimal effectiveness. Some security considerations for physical intrusion detection are discussed in the following sections.

Closed-Circuit Television

CCTV is in use just about everywhere now. Placement of CCTV devices should be thought out with financial and operational limitations in mind. Some possible initial areas for device placement include: high-traffic areas, critical function areas (such as parking structures, loading docks, and research areas), cash handling areas, and areas of transition (such as the hallway leading from a conference room to a sensitive location). Ensure that the cabling used for CCTV devices is not readily accessible, so that no one can easily tap into transmissions. Lighting will also play a critical role in the effectiveness of the camera.

If you are considering the use of a wireless CCTV setup, take into account that anything transmitted through airwaves was also meant to be received, and can be intercepted.

Alarms

Alarms should be tested at least monthly, and a test log should be kept. Points of entry and exit should be fitted with intrusion alarms. A response plan should be in effect, and everyone who will be responding to an incident must know exactly what their roles and responsibilities are. Duress alarms should also be taken into consideration for areas that may require them.

Compliance with Standards

If you are following a specific security framework, here's how ISO 27002 and COBIT tie into this chapter. Both have much to say about physical security, because gaining physical access to computer systems makes compromising them much easier for an attacker.

ISO 27002

ISO 27002 contains the following provisions, to which this chapter's contents are relevant:

- **9.1.1** Physical security perimeter: Security perimeters (barriers such as walls, card controlled entry gates, or manned reception desks) shall be used to protect areas that contain information and information processing facilities. (Comparable to COBIT DS12.1 and DS12.2.)
- **9.1.2** Physical entry controls: Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. (Comparable to COBIT DS12.2 and DS12.3.)
- **9.1.3** Securing offices, rooms, and facilities: Physical security for offices, rooms, and facilities shall be designed and applied. (Comparable to COBIT DS12.1 and DS12.2.)
- **9.1.4** Protecting against external and environmental threats: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. (Comparable to COBIT DS12.4.)
- **9.1.5** Working in secure areas: Physical protection and guidelines for working in secure areas shall be designed and applied. (Comparable to COBIT DS12.3, PO4.14, PO6.2, and AI3.3.)
- **9.1.6** Public access, delivery, and loading areas: Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. (Comparable to COBIT DS12.1, DS12.3, and DS5.7.)
- **9.2.1** Equipment siting and protection: Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. (Comparable to COBIT DS12.4 and DS5.7.)
- **9.2.2** Supporting utilities: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. (Comparable to COBIT DS12.4 and DS12.5.)

- **9.2.3** Cabling security: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. (Comparable to COBIT DS12.4 and DS5.7.)
- **9.2.4** Equipment maintenance: Equipment shall be correctly maintained to ensure its continued availability and integrity. (Comparable to COBIT DS12.5, DS13.5, and AI3.3.)
- **9.2.5** Security of equipment off-premises: Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises. (Comparable to COBIT DS12.2, DS12.3, and PO4.9.)
- **9.2.6** Secure disposal or reuse of equipment: All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. (Comparable to COBIT DS11.4.)
- **9.2.7** Removal of property: Equipment, information, or software shall not be taken off-site without prior authorization. (Comparable to COBIT DS12.2 and PO6.2.)

COBIT

COBIT contains the following provisions, to which this chapter's contents are relevant:

- **PO4.9** Create and maintain an inventory of information assets (systems and data) that includes a listing of owners, custodians, and asset classifications. Include assets that are outsourced and those for which ownership should stay within the organization.
- **PO4.14** Require contractors to comply with the organization's policies and procedures, for example: requirements for security clearance, physical and logical access control requirements, and requirements for client and personnel equipment.
- **DS5.7** Ensure that all hardware, software, and facilities related to the security function and controls are tamper-proof.
- **DS11.4** Sanitize equipment and media containing sensitive information prior to reuse or disposal. Such processes should ensure that data marked as 'deleted' or 'to be disposed' cannot be retrieved (e.g., media containing highly sensitive data should be physically destroyed). To maintain an audit trail, log the disposal of equipment or media containing sensitive information. Define a procedure to remove active media from the media inventory list upon disposal. Transport unsanitized equipment and media in a secure way throughout the disposal process. Require disposal contractors to have the necessary physical security and procedures to store and handle the equipment and media before and during disposal.
- **DS12.1** Select a site for IT equipment that meets business requirements and the security policy. Take into account special considerations such as geographic position, neighbors, and infrastructure. Other risks that need consideration include, but are not limited to, theft, air, fire, smoke, water, vibration, terror, vandalism, chemicals, or explosives. Ensure that the selection and design of the site take into account relevant laws and regulations, such as building codes and environmental, fire, electrical engineering, and occupational health and safety regulations.

- **DS12.2** Define and implement a policy for the physical security and access control measures to be followed for IT sites. Regularly review the policy to ensure that it remains relevant and up to date. Limit the access to information about sensitive IT sites and the design plans. Ensure that external signs and other identification of sensitive IT sites are discreet and do not obviously identify the site from outside. Confirm that organizational directories/site maps do not identify the location of the IT site. Design physical security measures to take into account the risk associated with the business and operation. Physical security measures include alarm systems, building hardening, armored cabling protection, and secure partitioning. Periodically test and document the preventive, detective, and corrective physical security measures to verify design, implementation, and effectiveness. Ensure that the site design takes into account the physical cabling of telecommunication and the piping of water, power, and sewer. The installation must be concealed, so it is not directly visible. The piping of water and sewer must also be redirected away from the server rooms. Define a process for the secure removal of IT equipment, supported by the appropriate authorization. Safeguard receiving and shipping areas of IT equipment in the same manner and scope as normal IT sites and IT operations. Define and implement a policy and process to transport and store equipment securely. Define a process to ensure that storage devices containing sensitive information are physically destroyed or sanitized. Define a process for recording, monitoring, managing, reporting, and resolving physical security incidents, in line with the overall IT incident management process. Ensure that particularly sensitive sites are checked frequently (including weekends and holidays).
- **DS12.3** Define and implement a process that governs the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorized by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access. Define and implement procedures to ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas, or zones) on job function and responsibilities. Define a process to log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site. Define and implement a policy instructing all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorization. Define and implement a policy requiring visitors to be escorted at all times while onsite by a member of the IT operations group. If a member of the group identifies an unaccompanied, unfamiliar individual who is not wearing staff identification, security personnel should be alerted. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. The devices record entry and sound an alarm in the event of unauthorized access. Examples of such devices include badges or key cards, keypads, closed-circuit television, and biometric scanners. Define a process to conduct regular physical security awareness training.
- **DS12.4** Establish and maintain a process to identify natural and man-made disasters that might occur in the area within which the IT facilities are located. Assess the potential effect on the IT facilities. Define and implement a policy that identifies how IT equipment, including mobile and offsite equipment, is protected

against environmental threats. The policy should limit or exclude eating, drinking, and smoking in sensitive areas, and prohibit storage of stationery and other supplies posing a fire hazard within computer rooms. Situate and construct IT facilities to minimize and mitigate susceptibility to environmental threats. Define and implement a process to regularly monitor and maintain devices that proactively detect environmental threats (e.g., fire, water, smoke, humidity). Define and implement procedures to respond to environmental alarms and other notifications. Document and test procedures, which should include prioritization of alarms and contact with local emergency response authorities, and train personnel in these procedures. Compare measures and contingency plans against insurance policy requirements, and report results. Address points of noncompliance in a timely manner. Ensure that IT sites are built and designed to minimize the impact of environmental risks such as theft, air quality, weather, earthquakes, fire, smoke, water, vibration, terrorism, vandalism, chemicals, and explosives. Consider specific security zones and/or fireproof cells (e.g., locating production and development environments/servers away from each other). Keep the IT sites and server rooms clean and in a safe condition at all times, i.e., no mess, no paper or cardboard boxes, no filled dustbins, no flammable chemicals or materials.

- **DS12.5** Define and implement a process to examine the IT facilities' requirement for protection against environmental conditions, power fluctuations, and outages, in conjunction with other business continuity planning requirements. Procure suitable uninterruptible supply equipment (e.g., batteries, generators) to support business continuity planning. Regularly test the uninterruptible power supply's mechanisms and ensure that power can be switched to the supply without any significant effect on business operations. Ensure that the facilities housing the IT systems have more than one source for dependent utilities (e.g., power, telecommunications, water, gas). Separate the physical entrance of each utility. Confirm that cabling external to the IT site is located underground or has suitable alternative protection. Determine that cabling within the IT site is contained within secured conduits, and wiring cabinets have access restricted to authorized personnel. Properly protect cabling against damage caused by fire, smoke, water, interception, and interference. Ensure that cabling and physical patching (data and phone) are structured and organized. Cabling and conduit structures should be documented, e.g., blueprint building plan and wiring diagrams. Analyze the facilities housing high-availability systems for redundancy and fail-over cabling requirements (external and internal). Define and implement a process that ensures that IT sites and facilities are in ongoing compliance with relevant health and safety laws, regulations, guidelines, and vendor specifications. Educate personnel on a regular basis on health and safety laws, regulations, and relevant guidelines. Educate personnel on fire and rescue drills to ensure knowledge and actions taken in case of fire or similar incidents. Define and implement a process to record, monitor, manage, and resolve facilities incidents in line with the IT incident management process. Make available reports on facilities incidents where disclosure is required in terms of laws and regulations. Define a process to ensure that IT sites and equipment are maintained as per the supplier's recommended service intervals and specifications. The maintenance must be carried

out only by authorized personnel. Analyze physical alterations to IT sites or premises to reassess the environmental risk (e.g., fire or water damage). Report results of this analysis to business continuity and facilities management.

- **DS13.5** Establish a preventive maintenance plan for all hardware, considering cost-benefit analysis, vendor recommendations, risk of outage, qualified personnel, and other relevant factors. Review all activity logs on a regular basis to identify critical hardware components that require preventive maintenance, and update the maintenance plan accordingly. Establish maintenance agreements involving third-party access to organizational IT facilities for onsite and offsite activities (e.g., outsourcing). Establish formal service contracts containing or referring to all necessary security conditions, including access authorization procedures, to ensure compliance with the organizational security policies and standards.

Summary

There are many physical security considerations that should coincide with your data security goals. Both physical and data security are centered on the protection of assets, so some concepts apply directly to both worlds. Common sense, forethought, experience, and clear, logical thinking are an essential part of any security plan.

References

Craighead, Geoff. *High-Rise Security and Fire Life Safety*. Butterworth-Heinemann, 2003.

Fennelly, Lawrence J. *Effective Physical Security*. Butterworth-Heinemann, 1997.

Matchett, Alan R. *CCTV for Security Professionals*. Butterworth-Heinemann, 2003.

National Institute of Standards and Technology. *NIST Special Publication 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*. NIST, 2008. http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

Roper, C.A. *Physical Security and the Inspection Process*. Butterworth-Heinemann, 1996.