Chapter 10

Security Measures: Physical Security

Brian Gouin

In this chapter . . .

- Introduction
- Types of Physical Security Countermeasures
- Integration of Multiple Physical Security Countermeasures
- Integration of Physical Security Countermeasures with Personnel and Policies and Procedures Countermeasures
- Determining Physical Security Countermeasure Needs
- Matching Product to Need
- Defining Cost and Cost-Benefit Analysis
- Best Practices
- Codes and Ordinances

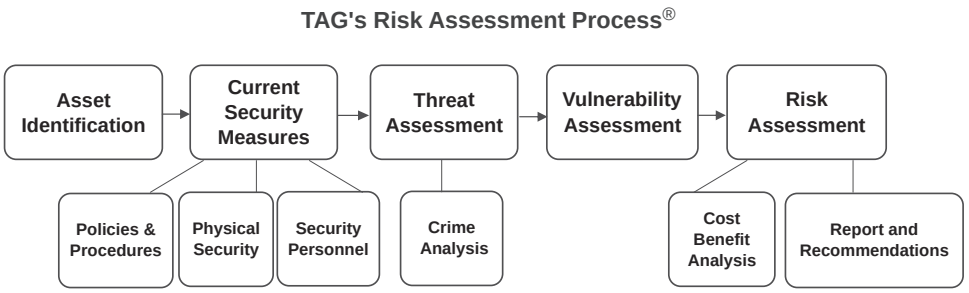

Figure 10-1.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

INTRODUCTION

Physical security countermeasures are the third critical part of an overall physical protection system, in conjunction with personnel and policies and procedures countermeasures discussed in the previous two chapters. It is important not only to have an understanding of the types of physical security countermeasures, but also to learn how they are integrated with each other as well as personnel and policies and procedures to form a complete physical protection system.

With an understanding of the options available and of the potential integration of those options, a determination can be made about the physical security needs of a facility or application. These needs should be based on asset identification, threat assessment, and vulnerability assessment, keeping in mind that the object of a physical protection system is to detect, deter, and respond to the threat. Once the needs are defined, products can be found to meet those needs, keeping in mind cost-benefit and industry best practices.

He that will not apply new remedies must expect new evils; for time is the greatest innovator.

—Francis Bacon

TYPES OF PHYSICAL SECURITY COUNTERMEASURES

In order to determine what, if any, physical security countermeasures are needed in a facility, you first must have an understanding of what countermeasures exist and what their functions are. This is not as easy as it might seem. Not only is the sheer volume of products overwhelming, but marketing material has a tendency to blur the core functions of individual pieces of equipment.

Below are types of physical security countermeasures broken down by category along with their individual functions and applications. This is not meant to give details of the workings of each countermeasure or every item required for a functional system, but is merely intended to give an overview of what is available in the market and the general functions of each countermeasure. A security professional; be it consultant, integrator, or whatever other professional, should be consulted for the specific countermeasures required.

Electronic Burglary Systems

Burglary systems are what people traditionally think of when they think of security systems. Although security professionals understand that a comprehensive physical protection system is usually much more than a burglary system, this technology still has a prominent place in the protection of assets.

Control Panels/Communicators and Keypads

A burglary alarm control panel is a circuit board enclosed in a metal (or sometimes plastic) cabinet. This panel is the brains of the system. All the field devices described here, which have their individually specific functions, are either wired to terminal strips on the circuit board or communicate with the control panel through a wireless transmitter and receiver. The control panel interprets the information from the device, which is usually just an open or closed loop, and determines what to do (go into alarm, nothing, etc.). Most control panels can be programmed via a PC or a keypad.

Most control panels today include a digital communicator built into the circuit board, which allows the panel alarms to be monitored by a contract or proprietary monitoring station. This is done for the most part over regular phone lines. System tests, open/close reports (who armed and disarmed the system), and power outages can also be monitored in this manner.

In addition to digital communication, a siren can be wired to a control panel for audible notification. These sirens can be internal or external to the area being protected and come in a wide variety of shapes, sizes, and enclosures.

The most important things to look for in a control panel are number of zones (to make sure the panel can handle the number of devices needed), expandability, and flexibility. Newer control panels come with a myriad of bells and whistles, some of which are helpful in streamlining installation time and making the system more user friendly and others that will probably never be used. Although it is always important to compare features in security equipment, there is little difference in performance between reputable manufacturers. In addition, the cost of control panels is relatively low.

The keypad is the device that turns the control panel on and off. This is usually done using a four- or six-digit code. Each individual user can have his or her own code, depending on the number of users and the capacity of the control panel. Keypad versions include digital displays or custom alpha.

Function and Application

- The function of a burglary alarm panel is to notify someone, by siren or alarm signal, that an event has occurred at a field device (opening in alarm, motion, fire, shock, etc).
- Burglar alarm panels are used in a variety of applications:
  1. When a building or office needs to be protected after hours. This can be a stand alone or part of an overall physical protection system that includes cameras, access control, and so on.
  2. When a particular area needs extra protection for notification to security personnel on or off site.

Door and Window Contacts

A door or window contact is a device that indicates when the door or window has been opened. These contacts are wired into the control panel for notification and communication. These contacts are typically in the following categories.

1. Magnetic: These contacts consist of a switch and a magnet. When the magnet is removed from the close proximity of the switch, the switch opens. The switch is installed in the jamb of the door or window, and the magnet is installed in the door or window sash. These contacts come in recessed and surface-mount versions.
2. Mechanical: These contacts use some mechanical means of opening the switch rather than a magnet. It may be in the form of a plunger, pull cord, spring-loaded bar, and the like. There are a wide variety of mechanical contacts to fit all types of different applications.

Function and Application

- The function of door and window contacts is to operate when the door, window, or other opening being monitored is opened, thereby notifying the control panel of that event.
- Door and window contacts are used mostly for perimeter protection of the building or room, and so on, that you are protecting. They are widely used because they are very reliable, and forcibly opening a door or window is a common burglary option.
- Door contacts are also used as a "door ajar" notification in conjunction with an access control system that will be discussed later in this chapter.

Motion Sensors

Motion sensors, also called motion detectors and intrusion detectors, are space detectors that detect motion within a certain area. These sensors are wired into the control panel for notification and communication. The most commonly seen types of motion sensors are as follows.

1. Passive Infrared (PIR): Passive infrared detectors sense the movement of infrared radiation through the optical field of view of the detector. This field of view stops at any solid objects and is a function of the range of the sensor. The radiation can come from a human, animal, or other temperature-altering objects or events. As a result, they are susceptible to false alarms and very inexpensive.
2. Microwave: Microwave detectors create a radiofrequency (RF) electromagnetic field in a set frequency range and when there is movement that frequency changes. Microwave detectors are volumetric, so they cover the entire room or area where the detector is located. It is

rare to see a stand-alone microwave detector except for certain outdoor applications and indoor high risk areas.

3. Dual-Tech: "Dual-technology" motion detectors are a combination of passive infrared and microwave and are the most common detectors on the market today. Both the infrared and microwave portions of the detector have to be activated for the detector to go into alarm. This allows for the most reliable type of detector while decreasing the potential for false alarms.
4. Tri-Tech: "Tri-technology" motion detectors are the same as dual-technology motion detectors, with the added feature of pet immunity so that the detector will not go into alarm if a pet up to about 100 pounds goes through its field of view. While this is mostly for residential applications, it is also helpful for commercial or industrial areas where mice or other such creatures are a problem.
5. Ultrasonic: Ultrasonic detectors use a low-frequency sound wave, and when there is movement that frequency changes. These detectors are very rare nowadays, and someone would have a difficult time even trying to find one to purchase. The major problem is that older versions or newer versions that are degrading give off a ringing noise that a small percentage of the population can hear and that gives others headaches. These detectors are even banned in many school systems throughout the country.
6. Photoelectric beams: These detectors shoot an infrared beam that is interrupted when an object breaks the beam. Because of the small detection pattern, they are mostly used for outdoors or to protect a small indoor space.

Function and Application

- The function of motion sensors is to detect movement in a defined area, thereby notifying the control panel of that event.
- Motion detectors are mostly used in conjunction with perimeter protection as a "second wave" of protection in case an intruder gets past the perimeter detectors. Although they can also be the primary intrusion detector, they should not be by industry standards.
- Infrared detectors are also used as "request for exit" devices in conjunction with an access control system that will be discussed later in this chapter.

Glass Break Detectors

Glass break detectors detect, through shock or sound, when glass has been broken within their field of detection. These detectors have sensitivity settings for different environments and are wired into the control panel for notification and communication.

Function and Application

- The function of glass break detectors is to detect glass breakage within a defined area, thereby notifying the control panel of that event.
- Glass break detectors are used as a perimeter detection device where there is some amount of fixed glass that cannot be protected by door or window contacts.

Spot (Object) Detectors

Spot detectors are sensors that attach directly to the object being detected and activate when the object is touched or moved. These detectors are wired into the control panel for notification and communication. The two main types of spot detectors are as follows.

1. Capacitance/Proximity Detectors: These detectors create an electrostatic field around the object (metal only). When someone or something approaches or touches the object, the field becomes unbalanced and the detector is activated.
2. Vibration Detectors: These detectors sense the vibration of the object when it is moved. They have sensitivity settings for different applications.

Function and Application

- The function of spot detectors is to detect when a protected object is touched or moved, thereby notifying the control panel of that event.
- Capacitance/proximity detectors are used for metal objects only, safes and small expensive machinery being the most common applications.
- Vibration detectors are used mostly for art objects and the like.

Miscellaneous Detectors

The following are other detectors that can be wired into the control panel for notification and communication.

1. Temperature: These detectors are basically thermostats that activate when the temperature goes above or below set points.
2. Water: These detectors activate when water rises to a certain level.
3. Smoke: These detectors are also used in a fire system that can be wired into a burglary control panel.
4. Heat: These detectors are also used in a fire system that can be wired into a burglary control panel.

CCTV Systems

Closed circuit television (CCTV) systems have become a major, and in many cases indispensable, part of a physical protection system. Technology has improved dramatically over the last 10 years to provide quality video images, storage, and viewing. The technology is actually changing month to month, but the system concepts remain relatively stable.

Cameras

Cameras are devices that capture the displayed image. Camera "systems" are actually made up of three components: camera, lens, and housing. There are also different types of transmission for the video signal. Some cameras also have an audio option, although legal advice should be sought before using the audio option on a camera.

Camera Options

1. Black and White (Monochrome): This camera provides black and white images. B/W is particularly effective in low-light conditions.
2. Color: This camera provides color images.
3. Day/Night: This camera automatically changes whether the images provided are B/W or color based on the light conditions.
4. All the above camera options are also available in different resolution quality. Standard and High are the common terms, although they may mean different things to different manufacturers.

Lens Options

1. Fixed: Lenses are generally available from 2.9 mm to 25 mm. The smaller the lens, the wider and taller the image from the same distance. Tools and charts are available to help determine the correct lens size based on image distance and height and width.
2. Vari-focal: These lenses can be adjusted to the desired size. They are typically available from about 3 mm to 8 mm and 9 mm to 22 mm. These have made it much easier to achieve the desired image size for the camera.
3. Zoom: These lenses have the ability to zoom in and out manually or automatically. They require specific housings and operating equipment.
4. Lenses are also available in manual or auto-iris versions. The iris makes adjustments for light so that the image is not too light or too dark. The auto-iris versions make that adjustment automatically based on light conditions.

Housing Options

1. Traditional: These are the housings most associated through the years with cameras. They require some kind of mounting bracket and must be in an environmental enclosure if installed outdoors.
2. Dome: Dome housings have become extremely popular because of their vandalism resistance and clean look. They are available in round, square, corner mount, flush, and gripless varieties.
3. PTZ: Pan/Tilt/Zoom (PTZ) housings are dome housings with the mechanical equipment added necessary to rotate the camera in all directions in order to effectively use the zoom option on the camera. PTZ cameras are largely used only when personnel are on duty to operate the cameras. Although they can be set to automatically pan and tilt, multiple fixed cameras would be better suited for that application.
4. Covert: These housings look like other devices, thereby disguising the fact that they are cameras. They may look like motion detectors, smoke detectors, clocks, exit signs, and other devices. Some of these devices also have a working function to what they look like (i.e., the motion detector is real and also has a camera within).

Transmission Options

1. Coax: The traditional and most well-known form of transmission for cameras is coax. Each camera has one piece of coax wired back to the

Figure 10-2.
Dome Camera.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

"head end" equipment. Power for the camera is through another wire and either runs back to a centralized power supply or to an individual power supply for that camera.

2. Fiber optic: This option uses fiber-optic cable instead of coax. One pair of fiber-optic cable is required for each camera. Power is still handled separately.
3. Unshielded Twisted Pair (UTP): This option uses twisted-pair wiring instead of coax. One pair of twisted wire is required for each camera. Power is still handled separately.
4. Internet Protocol (IP): IP cameras are the newest device on the market. An IP encoder is built into the camera, and it allows the camera to wire directly into a Local Area Network/Wide Area Network (LAN/WAN). A decoder is installed on the network at the "head-end" equipment location. In some instances, power can also come through this network connection.

Function and Application

- The function of a camera is to capture images and transmit them to other devices for viewing, recording, and archiving.
- The applications for CCTV cameras are numerous. They are a staple in security system design both as a deterrent to crime and as a means of identifying people and events. Here are just a few of the possible applications:
  a. Picture of everyone entering a facility
  b. Deterrent for crime, including vandalism and employee theft
  c. Verification that an event did or did not occur
  d. Identification of crime perpetrators

Termination Options

Cameras can be terminated into the following types of devices.

1. Switcher: A switcher is a device that takes one to eight cameras and scrolls through them at a set timed interval. They also can manually hold on one camera. Although they are inexpensive, they can only record what you see, so most images on every camera are permanently lost. They are available in B/W and color versions. Switchers are rarely used today.
2. Quad Splitter: A quad splitter takes four cameras, breaks the screen into four quadrants, and uses one quadrant for each camera image. Although a recorder will record all four images, four cameras is the maximum threshold of the device. They are available in B/W and color versions. Quad splitters are also rarely used today.

3. Multiplexer: A multiplexer is a device that takes anywhere from 2 to 16 cameras and allows the user to display the images in a multitude of configurations. Newer versions called duplex multiplexers allow the recording of all cameras regardless of what cameras are currently displayed. They are available in B/W and color versions. Virtually all multiplexers insert a time and date stamp on the video images. Most systems that still use time-lapse recording (explained later) currently use multiplexers.
4. Matrix Switcher Controller: A matrix switcher controller usually takes up to 32 or 64 cameras, including PTZ cameras, and allows personnel to display the images in a multitude of configurations. Included with a matrix is a keypad controller that personnel use to operate the PTZ camera functions. Multiple monitors, recorders, controllers, and alarm inputs can be used with a matrix switcher. Matrix switchers are generally used only where PTZ cameras are used and where personnel are available to operate the system. Matrix switchers also insert a time and date stamp on the video images.

Function and Application

- The function of these termination devices is to take more than one camera and consolidate them for viewing and recording.
- The application of these devices is self evident by their function; a termination device is needed for camera systems with more than one camera.

Monitors

Monitors are the device on which the camera images are displayed. The following options are available.

1. CRT monitors: CRT monitors are what traditionally are thought of as monitors. In simple terms, a monitor is a television without the tuner. CRT monitors are available in a wide variety of sizes and come in either B/W or color with or without audio.
2. LCD monitors: LCD monitors, or flat-panel monitors, are similar to computer flat-screen monitors. They take up less space and can be more easily mounted on a wall. However, they are considerably more expensive than their CRT counterparts. They are also available in a wide variety of sizes and come either in B/W or color with or without audio.
3. Computer monitor: Many newer camera systems are completely PC controlled, as will be explained later in this section. In those cases, a standard computer monitor attached to a PC acts as the camera image display.

Function and Application

- The function of these monitors is to display the images from the cameras as organized by the termination device.
- The application of these monitors is self-evident by their function; some sort of monitor is needed for the camera system in order to see the images.

Recording

Recording options are as follows.

1. Time-lapse recorders: Time-lapse recorders served as the standard for recording for two decades until just a few years ago. They look like a regular VCR, but they compress the video images so that you can fit anywhere from 24 to 168 hours of images on one tape. The inherent problems associated with time-lapse recorders are that the tapes degrade quickly, which affects the image quality, and the number of images per second per camera declines as longer time is compressed onto the tape. Therefore, the video is "choppy," and many images are simply not recorded. While time-lapse recorders are now very inexpensive and are still in widespread use, most of the new systems designed and installed do not use them because of their inherent deficiencies.
2. Event recorders: Event recorders are similar to time-lapse recorders except they do not record continuously but only when triggered by an alarm event, such as a motion detector being activated. With the dawn of digital recording, event recorders are rarely used today.
3. Digital recorders: Digital recorders store the video images on a hard drive as opposed to a tape. This has many advantages. First, the quality of the digital image is far superior to the tape's analog counterpart. Second, images can be retrieved by time and date in a split second rather than by playing and rewinding a tape. Third, a high number of images per second per camera are possible because of compression rate technology, making the video more real time and less "choppy." Digital recorders are a direct replacement for a time-lapse recorder or combination of time-lapse recorder and multiplexer (they are also called digital recorder/multiplexers). As such, they insert a time and date stamp on the video images. When digital recorders were first introduced, they were extremely expensive, but they are not cost effective even for small applications. They have become the industry standard for recording. Digital recorders can be divided into two main categories:

1. Stand alone: These recorders are stand alone because they can replace a time-lapse recorder and multiplexer directly and can be controlled right from the recorder. They come in options of 1 to 16 cameras (usually 1, 4, 10, and 16) and 80 gigabyte to 1 terabyte hard drives (varies by manufacturer). Many units are also capable of connecting to a network so that the images can be viewed on a PC on the network with the appropriate software. Most recorders are capable of viewing past images and recording live at the same time. A regular monitor or computer monitor can be used on most recorders.
2. PC based: These recorders are totally PC based and have controls on the unit; instead, a computer keyboard attached to the recorder is used. A computer monitor is also attached to the recorder for viewing. All of these styles of recorders are network compatible. They are available for a larger number of cameras (up to 64) and larger hard drives (many multiple terabytes).

Function and Application

- The function of a recorder is to store the video images so that they can be reviewed at a later time.
- The most obvious application of recorders is to determine if an incident has occurred or to view the details of an incident that has been determined to have occurred. They also are important to determine that an incident did not occur.
- The storage of video images is helpful to law enforcement for prosecution.

IP Video

The newest technology on the market is IP Video systems. It is widely believed that this style of CCTV system will be the standard in a short time, but that remains to be seen. In essence, this is a complete CCTV system that uses a computer network instead of traditional cabling or recording. IP cameras (a camera with an IP encoder installed) are wired directly into the network. Any computer on the network (with the right pass codes) can use the software and view the cameras. Decoders can be installed anywhere on the network if the signal needs to be transferred to analog for viewing on a standard monitor by security personnel and so on. Recording is done using computer hard drive storage methods such as RAIDS. The number of cameras and the amount of data storage for these systems are virtually unlimited.

Function and Application

- The function of this system is to act as a complete CCTV system using an existing or new computer network.
- Currently, the application of these systems, which is becoming more popular, is for larger systems with hundreds of cameras and a very large data storage capacity. Also, this system can be used if there are multiple sites in different areas (even countries) that want to have one CCTV system.
- Because of cost restraints and the specialized knowledge necessary for installation (heavy on IT), these systems are not yet used for small or medium-sized systems. However, as time goes by that may change.

Intelligent Video

Intelligent video, or smart video as it is also called, is simply what software technology allows people to do with the video images created. Here are a few examples.

1. Video motion: If there is motion within the video image or a set determined portion of that image, recording can begin, an alarm for notification can happen, and so on. Also, certain tendencies can be programmed so that if a person in the video image performs certain functions or acts in a certain way they are tracked and there is some notification. This sort of detection can be extremely precise and complicated.
2. Tracking: An object or person can be "tagged" by the video system operator, and that object or person can be tracked from camera to camera throughout the system.
3. Facial recognition: This software uses specific points on a person's face which create unique distances for identification purposes. This information can be inputted into a database for comparison to known criminals, and so on. This software can also be used in access control applications.

Function and Application

- The function of intelligent video is to aid CCTV system operators by processing the activities within the video images and giving the operators that information.
- At this time, the application for this technology is limited to high-risk situations and larger systems, but as time goes by these will become more affordable and common.

Electronic Access Control Systems

Access control systems have also become a major and indispensable part of a physical protection system. The ability to allow or deny access to facilities or areas within a facility and the ability to track the identity and times of those entries or exits have become critical security tools.

The main purpose of an electronic access control system is to allow or deny access to some area based on one or a combination of the following factors: What You Have, What You Know, and Who You Are. The level of security desired determines what combinations of these factors are necessary and therefore what devices are chosen.

Stand-alone Devices

Stand-alone devices are keypads or card readers that control only access points (door, gate, etc.). They are generally programmed via a "deck" of programming cards, dip switches, or through the keypad. They are relatively inexpensive but have a limited number of potential users and little to no tracking ability. These devices will determine either What You Have or What You Know in order to allow or deny access.

Function and Application

- The function of a stand-alone access control device is to control access to one point where there are a small number of users and tracking is not necessary.
- The application for these devices is where there is only one access point on the system, such as a gate, and tracking is not important. An additional application may be where there are multiple access points but no viable way to get wiring between the points.

System Controllers

Electronic access control system controllers are circuit boards mounted in a metal (or sometimes plastic) cabinet and are the brains of a multipoint access control system. Readers, egress devices, door-ajar contacts, and locking devices are all wired into a controller to form a complete system. Controllers typically come in 2-, 4-, 8-, or 16-point versions where multiple controllers can be interconnected to create as large a system as is required. These systems are PC based and are programmed from software on a computer wired directly to the controller or from a computer on a network where the controller is wired.

Typically, this style of system allows or denies access based on access point, card, time, day, or a multiple of those things; reporting of door ajar; anti-

passback; and reporting of denied access; and a multitude of reports and charts of user activity based on various criteria. This type of system controller is currently the industry standard for access control systems.

Function and Application

- The function of the system controller is to combine multiple access control points into one integrated system controlled via software from one location or network.
- There are an infinite number of applications for this type of controller, basically anywhere where multiple access points are required and control and monitoring is centralized.

Readers

Readers are the electronic devices that accept an input from a user and transmit that information to the controller to allow or deny access. Readers are wired directly into the controller. There are different types of readers, as follows:

1. Magnetic stripe readers: These are readers for magnetic stripe cards, similar to credit cards, which read the information on a magnetic stripe on the back of the card. Because of better technology, these cards and readers are rarely used today.
2. Wiegand readers: Wiegand readers are for Wiegand cards, which use a wire embedded into the card to transmit information. Although the Wiegand protocol is still the industry standard today, the cards and readers are rarely used.
3. Proximity readers: Proximity readers are for proximity cards or key tags that use a chip embedded within the card or tag to transmit information. These are the industry standard for readers and are available in a variety of read ranges and mounting options. This type of reader as well as the magnetic strip and Wiegand readers deal with What You Have.
    a. These readers are also used with smart cards, a relatively new but promising technology that embeds a great deal of information about the user on the card. In that way, the same card can be used for access, payment on account, personal identification, and more.
    b. Proximity cards also have the option of Photo ID badging, so that the person's picture, name, and other vitals are on the card for additional identification by personnel as well as being used for access.
4. Keypads: Keypads usually use a four- or six-digit code to determine access. This type of reader deals with What You Know.

5. Combination Card/Keypad reader: This reader combines both a card or key tag proximity reader and a keypad. Both the card or tag and keypad have to be used for access. This type of reader deals with both What You Have and What You Know together.
6. Biometric readers: These readers measure and verify a unique physical characteristic of the individual to determine access. These readers deal with Who You Are. Although they are becoming more popular, this type of reader is not very common and is used almost exclusively in high-risk areas. However, it is recommended that these devices not be on the only access device for a point but rather be used in conjunction with either a card reader or keypad. Here are some types of biometric readers.
   a. Fingerprint scan
   b. Retina eye scan
   c. Hand scan
   d. Voice recognition

Function and Application

- The function of a reader is to accept the inputted information from a user and transmit that information to the controller to determine whether access will be granted or denied.
- The application of these devices is self-evident by their function. However, the type or combination of types of readers used is determined by the level of security desired based on What You Have, What You Know, and Who You Are.

Locking Devices

Locking devices are what keep the door or gate closed and secure until an accepted user activates a reader and the opening is unlocked. Locking devices are generally wired directly into the controller but also usually require their own power source. Common locking devices include:

1. Electric strike: Electric strikes replace the strike plate on a door and keep the door latch from moving until it is activated. This lock is available in fail-safe (releases on loss of power) and fail-secure (remains locked on loss of power) versions. This is the most common locking device.
2. Magnetic lock: Magnetic locks, commonly called mag locks, consist of a large magnet mounted on a door or gate frame and a plate mounted on the door or gate itself. These devices are used where electric strikes are impractical owing to installation difficulties or where sturdier door

security is needed. Mag locks require specialized egress devices due to building code regulations. Mag locks are a very popular locking device.

3. Electric panic hardware: These are installed on the inside of a door and retract a latch bolt when activated. They are used primarily for egress-only doors.

Function and Application

- The function of a locking device is to secure a door, gate, or other opening until an authorized user activates a reader and releases the locking device.
- The application of these devices is self-evident by their function. However, the type of door or gate, along with the individual installation issues, will determine the type of locking device used at each opening.

Egress Devices

Egress devices allow exit from an opening by releasing the locking device without activating a reader. Keep in mind that some applications will also employ a reader to exit instead of an egress device, although certain building code issues must be dealt with when that is the case. Electric strikes do not require an egress device because using the existing door handle or panic bar will allow exit. Egress devices include the following.

1. Request to Exit motion detectors: This motion detector is installed above the door on the wall or ceiling and is activated when someone walks up to the door.
2. Exit button: This button, when pushed, releases the locking device.
3. Touch sense bar: This device looks somewhat like a crash bar except it is electrically charged. When someone touches the bar, the lock can release, or there can be an alert sounder that someone is trying to exit with a delay time for release.
4. Electric panic hardware: This locking device is also its own egress device.

Function and Application

- The function of egress devices is to allow exit from the opening by releasing the locking device without the use of a reader.
- The application of these devices is self evident by their function. However, which one or combination of these devices varies greatly on specific individual application and is determined by federal, state and local building codes as well as function.

Door Hardware

Existing door hardware will have to be changed in many cases with the installation of an electronic access control system. A door hardware specialist will need to be involved. If the installation is at a completely new facility, door hardware should be addressed up front when doors are specified.

Turnstiles

Turnstiles are an access control device meant only to allow authorized users to enter an area one by one. These devices are commonly seen in subways and stadiums. The popular version of the turnstile for security uses is called an optical turnstile. There is no rotating bar that manually stops entry as in a subway; in fact, there is no manual stop at all. The turnstile reads the access card of the individual before he or she walks through. If the user is authorized, nothing happens and the next person continues. If the user is unauthorized, some sort of alarm goes off, alerting security personnel of the issue. This type of turnstile allows a very good throughput rate (throughput is the number of people who can go through the device in a given time period).

Function and Application

- The function of an optical turnstile is to allow people to easily enter a facility but still alert security personnel if an unauthorized person attempts entry.
- These devices are very popular in corporate offices and similar types of buildings where each individual does not need to be viewed before entering but access needs to be controlled.

Perimeter Security Systems

Perimeter security systems are defined for this purpose as systems designed to restrict access to the grounds of a facility.

Fencing

Fencing is a very common way of denying access to facility grounds. It generally comes in chain link and ornamental varieties. There are industry standards based on application for the height of the fence, amount buried underground, and so on. The chain link variety also can have barbed wire on its top for extra security, which also has its set of industry standards based on application. Fencing is installed so that there is a "clear zone" between the fence and other objects or buildings on the grounds. This clear zone helps in both detection and delay in order to respond. Fence sensors are available, which sense the movement of the fence, such as someone climbing it, and set off an

alarm for notification. Pedestrian and vehicle gates are added within the fence line to allow authorized access to people and vehicles.

Function and Application

- The function of fencing is to keep unauthorized people and vehicles off facility grounds.
- The applications of fencing are many, from government to corporate to housing facilities. Retail would be an obvious application where fencing would not be used.

Gate Operators

Gate operators are electronic devices that allow automatic rather than manual operation of gates within the fence line. They include the following categories.

1. Slide gate operators: These operators move a gate made from the same material as the fence side to side to create an opening. They are available in chain- or belt-driven as well as hydraulic versions.
2. Swing gate operators: These operators move a gate made from the same material as the fence in a swinging motion across the ground to create an opening. They are also available in chain- or belt-driven as well as hydraulic versions.

Figure 10-3.
Slide Gate Operator.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

3. Barrier arm operators: These operators move an arm usually made of wood or aluminum in an upward-swinging motion to create an opening.

Gate operators require a variety of safety accessories that could include:

1. Loop detectors: Wire loops are installed by cutting into the pavement, creating an electrical field that is disturbed when a car drives over it. They are used as both safety devices and free exit devices.
2. Photo beams: These are the same as their security versions described in the burglary section of this chapter except they are used as safety devices.
3. Safety edge: This device is installed on the gate itself to reverse the gate operator action if the edge is touched.
4. SOS: These devices automatically open the gate when a siren is activated like the kind used in emergency vehicles.

Because the addition of these safety devices can create a potential lapse in security, gate operators are usually manned or have additional electronic systems used in conjunction with them, most notably CCTV cameras.

In addition, access control readers are commonly used to open the gate operator. Remote controls similar to garage door openers are also used for this purpose.

Function and Application

- The function of a gate operator is to automatically open the gate when it is required so that it can remain closed for security when not in use and does not have to be manually opened when it needs to be.
- The application of gate operators is found anywhere that a fencing system exists and the gate must be opened and closed multiple times during the day.

Bollards

Bollards are physical barriers that are installed on the perimeter some distance from a building. They range in height and in other physical attributes and are generally made of concrete or steel. They can be fixed or hydraulic so that they can be raised or lowered as desired. They are usually installed in bunches in such a manner that a vehicle cannot get between them.

Function and Application

- The function of bollards is to prevent a vehicle from getting past them and close to a building.

- The application of bollards is for facilities where it is a concern that a vehicle filled with such things as explosives would drive into or near a building.

Locks

Locks are one of the most basic physical security countermeasures but all the same an important one. They can be used to delay a threat while waiting for response if the threat has already been detected. Otherwise, locks are used mostly as a deterrent. They come in rim-mounted, mortise, tubular, cylindrical and unit types. Here are a few things to keep in mind:

1. Locks are only as good as the door, jambs, and walls around them. A lock does no good if the door can be kicked in easily.
2. Key management is important when dealing with a complete lock system. If anyone with a little ingenuity can obtain or make a key to the lock, it doesn't do much good. Many manufacturers' products are designed to improve key management.
3. All locks can be compromised by an expert in a very short period of time. Locks work best as part of the overall physical protection system and not all by themselves.
4. If there is no way to detect a threat in order to create a response and a lock is the only countermeasure being used, the question is not whether the opening will be compromised but how long or short a period of time it will take.

Function and Application

- The function of locks is to stop an adversary from easily entering without having to perform another task to do so.
- The application of locks is widespread—basically any door or window that allows access to a protected area.
- Locks are best when used in conjunction with other physical security countermeasures.

Lighting

Lighting is a critical part of the detection element of a physical protection system. A threat cannot be detected, either by camera or in person, if there is no light. Lighting also helps in response to the threat. Another factor in lighting is deterrence. A threat may be more likely to attack an asset in relative darkness as opposed to in bright light.

Long book chapters and whole books have been written about the science of lighting as it pertains to security. Research should be done to determine what

type and style of lamp is best for every application. Factors to consider include color of light, re-strike time, efficiency, and brightness. Types of lamps include incandescent, fluorescent, halogen, low-pressure sodium, high-pressure sodium, metal halide, and mercury vapor.

Function and Application

- The function of lighting is to illuminate a protected area in order to detect a threat in order to elicit a response.
- The application for lighting is a part of virtually every physical protection system.

Fire Systems

Although fire systems may not be regarded as physical security countermeasures, they are crucial life safety systems and in many cases are integrated with security countermeasures in some form or another, either in some common equipment or through monitoring. In addition, security and life safety functions can be handled by the same department. While fire systems are in some respects a separate discipline, some basic knowledge of the equipment available is important. Here is a very brief and condensed description of fire system devices:

Fire control systems are broken down into two major categories:

1. Addressable: Addressable fire systems assign an "address" to each field device in order to program and identify the device in case of an alarm. While the cost of this equipment is higher than that of its counterparts, the money is theoretically made up in lower installation and wiring costs. Addressable panels are used for larger systems and even smaller modern systems. Addressable fire devices are not interchangeable with analog devices or with other addressable devices of different manufacturers.
2. Analog: Analog fire systems use a "zone" approach similar to burglar alarm systems and wire multiple devices onto a zone. All older panels are analog, and still a good many new smaller systems use analog panels. Analog fire devices are generally interchangeable by manufacturer between systems.

Here are the more common fire system devices found in the field:

1. Smoke detectors: Smoke detectors come in two major styles: ionization and photoelectric. As a general, but not absolute, rule, ionization smoke detectors are for residential use, and photoelectric smoke detectors are for commercial use. In the general operation of a smoke detector, the air passes through the detector chamber, which senses the presence of smoke.

2. Duct smoke detectors: Duct smoke detectors are smoke detectors installed in forced hot-air duct work. A tube is inserted in the duct work that captures the air and brings it to the detector located outside the duct for sensing.
3. Beam smoke detectors: These smoke detectors use beams of light, similar to a motion detector, to sense smoke. They are used to cover larger areas than traditional smoke detectors.
4. Heat sensors: Rather than smoke, these sensors detect either a fixed temperature point or a rate of rise of temperature over a set period of time.
5. Pull stations: These devices feature a lever that can be manually pulled in order to activate an alarm.
6. Sprinkler flow switch: These switches tie into the water feed of the sprinkler system to activate an alarm if the water flows.
7. Sprinkler tamper switch: This switch ties into the sprinkler shutoff valve to sense if the valve is rotated.
8. Horn/strobes: These are signaling devices that use a visual strobe and audible horn when the alarm is activated.
9. Strobes: These are signaling devices that just use the visual strobe.
10. Speaker/strobes: These are signaling devices that use the visual strobe and either a prerecorded announcement or a live announcement when the alarm is activated. They are used in conjunction with a voice evacuation panel.
11. Door magnets: These devices hold open smoke doors, usually located in hallways, and release the doors so that they close when the alarm is activated.

The number and location of these devices on a premise are strictly regulated by NFPA 72 National Fire Alarm Code and NFPA 101 Life Safety Code. These systems must be designed by a trained and in some cases licensed professional.

Function and Application

- The function of fire alarm systems is to detect the presence of smoke or fire and to alert all the occupants of the facility so that they may exit the facility.
- Fire systems are required in facilities of minimum sizes and number of occupants depending on the type of facility as described in NFPA 101 Life Safety Code.

Specialized Protection Systems

In many cases specialized protection countermeasures are needed in order to combat more serious threats. These needs include explosion protection, bal-

listic protection, weapons identification, and chemical and biological protection. The design and installation of these countermeasures is a very specialized field and may include

1. Metal and explosive detectors—to identify weapons and bomb-making material as it enters a facility.
2. Ballistic-resistant rated materials and products—includes such things as window film and special doors and windows.
3. Structural hardening designs and materials.

Function and Application

- The function of specialized protection systems is to detect or repel a specific special serious threat.
- The application of these countermeasures is in high-security applications or any other application that may be deemed a target of terrorism.

INTEGRATION OF MULTIPLE PHYSICAL SECURITY COUNTERMEASURES

The basic function of a physical protection system is to detect, deter, and respond to a threat. Except for the smallest of systems, this always requires multiple physical security countermeasures. These measures must be integrated in order to form the entire physical security aspects of the protection system.

Some manufacturers have already integrated multiple countermeasures into one functional system. For instance, currently some products on the market combine CCTV, access control, burglary, and even fire systems into one software package with compatible head-end equipment. The combination of access control and CCTV or access control and burglary are the most common combinations. The more common method of integration of physical security countermeasures is simply to provide multiple measures and design them in a way in which they work in concert with each other.

The more common method of integrating physical security countermeasures is simply to provide multiple measures and design them in a way in which they work in concert with each other. For example, for a whole facility, detection can include a fence detector, CCTV cameras, outdoor motion sensors, a burglar alarm, and lighting. The deterrence can include fence razor wire, a gate operator, door locks, and access control devices. Response can include a guard office with internal monitoring facility. Similar examples can be used for just a building itself or just an area within a building using the same principles as for a whole facility.

Integration of Physical Security Countermeasures with Personnel and Policies and Procedures Countermeasures

Physical security countermeasures are never used alone; rather, they are always used in conjunction with personnel or policies and procedures countermeasures, or both. While this may be self-evident for large systems, even the most basic stand-alone burglar alarm has a procedure and/or policy for turning the alarm on and off and if it is monitored it now involves personnel.

All electronic physical security countermeasures and most mechanical ones are not just installed and expected to work on their own. They require some kind of human interaction, in various degrees, for them to perform their function to their full potential. Therefore, not only must the personnel exist to interact, but they must have an understanding of what to do. Here are just a few examples of that interaction:

1. An access control system cardholder attempts on multiple occasions to enter an area of the building for which he or she is not authorized and is denied access. The system software sets off an alert on the appropriate PC. The person in charge of monitoring and running the system must acknowledge the alert and determine how the situation should be handled. This scenario requires the personnel to monitor the system and the policy and procedure to determine what to do.
2. A retail store has CCTV cameras throughout the store with Pan-Tilt-Zoom (PTZ) capability to identify shoplifting and employee theft. Security personnel are watching the cameras and looking for criminal actions. When a crime is spotted, they must notify the appropriate security personnel and determine the correct course of action. This scenario also requires the personnel, in this case specifically trained personnel, to monitor the system and the policy and procedure to determine what to do.
3. There is a manned security shack on a fence line with an automatic gate operator. Employees of the facility use an ID badge and card reader to open the operator and gain access, but visitors and deliveries must be checked in at the gate and the operator must be opened by the security officer for the person to gain access. Not only must the security officer exist, but a policy and procedure must be in place for the security officer to determine who is allowed access.
4. An electronic turnstile at the employee entrance of a facility reads the employee's ID card and allows access. Inevitably, some employees will have lost their ID badge or for whatever reason may have a hard time getting through the turnstile. Some personnel must be in place and follow some procedure for such occurrences.

5. A security force patrols the grounds and interior of a facility, but that requires adequate lighting for the security officers to effectively see what is happening and an appropriate locking system for the security officer to move around the facility. In addition, they must have a set of policies to deal with situations that arise.

Determining how, to what degree, and in what manner there exists a meaningful interaction between physical, personnel, and policies and procedures security countermeasures requires a degree of expertise and experience. Whether that is obtained internally or externally, making this determination is a necessary step taken to determine the exact physical security countermeasure needs.

Determining Physical Security Countermeasure Needs

This is the most important step in the process of a physical protection system project. Although it takes skill to determine which products are the best fit for the requirements and needs, if the needs are incorrectly determined, the results are guaranteed to be ineffective. Determining those needs requires that the correct steps have already been taken.

Up to this point, there should have already been an identification of the assets that need protecting, an assessment of the threats to those assets, and an assessment of the current vulnerabilities of the facility in protecting those assets against the threats. That information will help determine the overall level of security required. Once all that has been identified, a series of questions should be asked, including (but not limited to) the following.

1. What functions do the physical security countermeasures need to perform in order to counteract the vulnerabilities? For instance:
   a. Is it necessary to have tight control over access to the facility or parts of the facility? (This would be different for a retail store vs. a corporate headquarters.)
   b. Is it necessary to have visual identification of people in the building or the actions they take? Again this could be quite different for a retail store vs. a corporate office.)
   c. Is it necessary to have tight control over access to the entire grounds surrounding the facility?
   d. Is it necessary to provide additional safety for employees or visitors?
   e. Does the facility require additional security deterrents after hours?
   f. Are there specific areas of the facility that require additional security measures?

   g. Does the specific threat require special considerations (i.e., ballistic, chemical countermeasures)?
2. What number and type of personnel can or will be committed to the overall physical protection system? For instance, if the facility can't or won't have personnel to continually monitor CCTV cameras, you would not use PTZ cameras. Will systems be monitored internally or externally?
3. What policies and procedures are acceptable based on the culture of the facility and its management? You would not at this point, for instance, ask employees at a normal corporate office to have their persons and belongings searched every time they enter the building, whereas you would for a sensitive government office.
4. What makes common sense for the facility? Although it would be effective to have an armed security officer posted all night at a secondary school, does that really make sense? By the same token, does it make sense to just have door locks and good lighting at a manufacturing facility?
5. What is a realistic budget for the system? Although to some degree the needs define the budget, in the real world there are constraints and there must be a convergence of meeting the needs of the facility and the money that can be spent.

Physical countermeasures should be designed in layers, with the underlying theme being a combination of measures to detect, deter, and respond. Here are a couple of examples of the thought process.

1. If there is a medical research facility that conducts tests on animals, the threat assessment would determine that radical groups like PETA are a concern. In that case, among other things it would be important to control access to the grounds of the facility as well as the facility itself, to have special security measures in the specific research areas, to provide specific policies for the safety of the employees, and to have some sort of security force in close proximity should a threatening event be detected.
2. If a corporate office houses employees and a data center with sensitive information, among other things it would be important to control access to the building itself, provide special security measures for the data center, provide some surveillance for the safety of the employees, and have a burglar alarm with external monitoring for after hours.

Being able to assess the answers to the questions posed earlier and the large number of other questions that need to be asked and from that determining the physical security needs requires skill and should be done by someone trained in that field. If there is any part of the acquisition of a physical

protection system process where proven expertise should be sought, this is it. If the needs of the facility are determined incorrectly, nothing else will matter in providing an effective system.

MATCHING PRODUCT TO NEED

Once you have an understanding of which physical security countermeasures are needed for your protection of assets, you must match the specific product to that need. Notice the wording here: MATCH PRODUCT TO NEED and not NEED TO PRODUCT. This may seem like logical common sense, and it is, but it is here that many critical mistakes are made for various reasons.

The best way to avoid falling into this trap is to create an Invitation to Bid rather than an RFP when bidding the installation of these systems. An RFP gives the requirements of the system based on the needs and asks the responders for the equipment solution to the requirements. In an Invitation to Bid, the specific equipment has already been chosen and the bidders are simply being asked to submit a price for its installation. In many cases, particularly public bids, alternative equipment must be allowed to be bid, but if the specifications are written clearly enough, it can be reasonably guaranteed that any equipment bid will meet the requirements and therefore the needs.

Note that all products specified in an RFP response or an Invitation to Bid may be equipment that meets the requirements and needs, but not the BEST equipment for the needs. The goal is to choose and provide the best solution for the required needs.

If an RFP must be issued for these systems, avoid these pitfalls:

1. Do not rely solely on an integrator to determine which products meet your needs. Integration (installation) companies tend to represent a small number of manufacturers most of the time. This is because they have a comfort level with those manufacturers, volume quotas that need to be met, incentives from manufacturers, and sometimes it's just easier. Maybe the manufacturer they choose has a piece of equipment that exactly meets your need and maybe the manufacturer does not. An independent review is needed to verify that the equipment bid meets the requirements and needs.
2. Be even more careful with very large companies that manufacture, sell, and install their own equipment. The problem described above becomes even more of an issue, and the "slickness" of these companies makes it difficult to recognize that you are not getting the best product match for your needs.
3. In both of the cases in (1) and (2), beware of equipment that can only be installed by one company in your geographical area. This may not be the best long-term solution for your needs if you become locked in to one integration firm, especially if you are unhappy with them in the

long run. You may not have a choice but to choose equipment that only a few integrators in your area can install, but if you can choose equipment that any reputable firm can install that would be best.

If an Invitation to Bid is prepared, it is critical that the individual writing the specifications has total independence from any particular manufacturer or equipment supplier to make sure that the equipment chosen is the best fit for the needs. If there is no internal expertise that can wade through the maze of equipment types described in this chapter and make the proper decisions, outside design expertise should be sought. This may come in the form of a security consultant or architect or engineer. Whichever is chosen, the same due diligence and oversight must be applied as is applied with the evaluations of an RFP to make sure the best equipment is chosen.

It cannot be stated enough that independence is key for the consultant or architect determining the correct equipment for the needs. These issues should be kept in mind:

1. Some manufacturers have a tendency to wine and dine system designers, particularly architects, with the goal of having the system design specify their equipment almost exclusively. A well-known fire system manufacturer (whose name shall be omitted) is notorious for this behavior. While this manufacturer is not being unethical, it can be legitimately argued that the designer is unethical. Steps should be taken to make sure the chosen designer is not specifying equipment for this type of reason.
2. In addition, some manufacturers will offer to write the specifications for the designer, of course specifying their equipment, at no charge. A well-known burglar alarm manufacturer and installation company (whose name again shall be omitted) does this as part of its normal business operations. The designer's behavior is definitely unethical because he is charging for work performed by others. This behavior seems to happen more with architects than security consultants or engineers.
3. As with integrators, designers sometimes develop a comfort level with certain manufacturers and specify their equipment regardless. They may not have the same financial obligation that the integrator has with quotas, but they may believe they have a loyalty obligation. This results in not providing the best option for the client.

There are plenty of reputable security consultants, architects, and engineers who do not behave in these ways. It is important to make sure that is the case and that the designer is choosing equipment based solely on determined requirements and needs.

Whether the equipment choices are being made internally or externally, these criteria should be used when making the choice:

1. Function: Does the equipment perform all the functions required to meet the needs? Does the equipment perform considerably more functions than is required, or is another piece of equipment a better match?
2. Reliability: Does the manufacturer have a reputation of reliability in the industry? Is there any track record with this equipment?
3. Compatibility: Is this equipment compatible with the rest of the equipment that will be used for the total physical protection system? If things need to work in concert with each other, will they?
4. Price: Is this equipment within the prescribed budget for the system?
5. Ease of Installation: Will installation costs be reasonable for this equipment, or is the equipment too burdensome? Is there a wide range of integrators that have the ability to install this equipment?
6. User Friendliness: Is this equipment easy to use for the ultimate end user?
7. Expandability: Is this expandable to cover the anticipated potential future requirements?

If these general criteria are followed, it is reasonably assured that equipment choices will be based on the product matching the need and not the need matching the product.

Defining Cost and Cost-Benefit Analysis

When determining what physical security countermeasures to implement, it is obviously important to have an understanding of what those countermeasures will cost. This is not as simple as finding out how much the products cost to purchase or getting a proposal from an integrator for product installation. The following aspects of cost must be taken into account:

1. System Installation Cost: This is what would normally be considered the cost of the system, what would be put in an Invitation to Bid. When estimating this cost for planning purposes before the bid process, take into account all these components of the installation cost:
   a. Product costs: This is what the equipment cost is to the integrator.
   b. Shipping costs: The equipment has to get to the integrator and then to the site. Where is the equipment chosen coming from?
   c. Labor costs: This is always a major part of the system cost. What is the typical wage rate in your area? Will this be a prevailing wage job? There may be different wage rates for different functions. What must be done for each of these functions with the system chosen?
      - In field supervision
      - Site installation

- Programming
- Testing
- Training

d. Fixed costs: There are always fixed costs for a project that could include the following:
   - Material cost
   - Subcontractor cost
   - Engineering
   - Bonding fees
   - Permit fees
   - Taxes
   - Tools

e. Profit/Overhead costs: There must actually be a profit made from the installation of the system.

2. System Operation Costs: It is necessary to look at everything that must be done on a regular basis because of the installed system, including how if affects personnel and policies and procedures. All these added functions have a cost associated with them that must be taken into account when determining the overall cost of the countermeasure. For instance:
   a. Do personnel have to be added in order to operate the system? Security officers or central station personnel?
   b. Does someone have to regularly review the output of the system? (CCTV images, access control reports, etc.)
   c. Does a policy or procedure have to be added because of the system that affects someone's productivity?
3. Maintenance Costs: How much will this system cost to maintain? Does regular routine maintenance have to occur, and if so how often and in what detail? For instance, a gate operator has a far greater need for routine maintenance than a burglar alarm. What is the track record of the equipment from a breakdown point of view? How often will the system not be functional? What extra costs, particularly with personnel and repair costs, will be incurred when the system is down? These are not easy questions to answer, but the analysis must be done.
4. Replacement Costs: What is the life cycle of all the equipment within the system? When will products have to be replaced, and what is the anticipated cost of those products at that time?

Once you have analyzed all of the above costs, you now have the overall cost of the countermeasure and can analyze that cost versus the benefit.

Cost-Benefit Analysis

It now must be determined if the benefit of protecting the asset is worth the cost. You would not spend $10,000 (as an example) to protect a cash register with $100 in it. However, $10,000 would be a bargain to protect $1 million worth of jewelry inventory. Also, keep in mind that assets are not just property but people and information as well. Is $10,000 worth protecting employees in a parking lot? Is it worth protecting the formula for your signature product?

The answers to these questions are determined by simple factors such as the size and budget of the facility and complex factors such as the criticality of the potential loss. The larger the cost the more professional expertise, internally or externally, must be used to evaluate the loss criticality and make the cost-benefit analysis.

Best Practices

Best Practices means exactly what it seems—to perform one's duties in the best manner possible according to industry standards. The first step in the process of applying Best Practices to a physical protection system is to actually want to do so. While that may seem obvious to those of us who want to, the sad fact is many people simply want go through the motions and produce perhaps a workable system but not the best one possible. If an individual performing any of the functions of implementing a physical protection system does not stress the use of Best Practices, find one that does.

If it is not possible to hire an external consultant to perform the necessary functions, it will require someone internally to understand the Best Practices. How does one gain Best Practices knowledge when it comes to Physical Security Countermeasures and integrating them with a comprehensive physical protection system? Here are a few ways:

1. Reading: Reading books such as this one and other industry and system-specific books will teach a lot about physical security countermeasures.
2. Seminars/Conferences: Organizations such as the American Society for Industrial Security (ASIS) and the Security Industry Association (SIA) routinely sponsor seminars and conferences that cover a broad range of subjects regarding all aspects of physical protection systems. They are generally taught by well-regarded experts in the security industry.
3. Research: With the Internet and some time, a lot can be learned about any subject, this being no exception.

Keep in mind: there is no substitute for experience. All the above education is great, but it must be combined with real-world practices in order to ultimately achieve the use of Best Practices.

Codes and Ordinances

The government at all levels, federal, state and local, has adopted codes and ordinances relating to the design and installation of physical security countermeasures. The local Authority Having Jurisdiction (AHJ), which could be a building official, fire marshall, or other inspector, verifies that the design and installation of the countermeasures meet or exceed all the applicable codes and ordinances. Regardless of the physical security countermeasures chosen for the facility, it is essential that they meet or exceed the codes and ordinances that apply to the particular application. While this is important for all measures, it is particularly important for access control and fire systems.

Following is a list of some of the codes and ordinances that must be adhered to when designing a physical protection system:

1. NFPA 70 National Electrical Code
2. NFPA 72 National Fire Alarm Code
3. NFPA 101 Life Safety Code
4. Americans with Disabilities Act (ADA)
5. Underwriters Laboratories, Inc., Standard for Safety
6. BOCA Building codes
7. Local and State Building codes
8. All requirements of the AHJ

Summary

In order to design and implement the most effective physical security countermeasures as part of the overall physical protection system, security decision makers must first understand what types of countermeasures exist and what their functions are in the larger security program. Then it is necessary to understand how those countermeasures relate and integrate with each other and with both personnel and policies and procedures countermeasures.

That knowledge is then used to determine which physical security countermeasures or combination thereof meet the needs for the asset being protected against the threats. Once the type of physical security countermeasure needed is determined, the specific product must be found to match that need. Part of that process is also determining the cost of that countermeasure and analyzing the benefit versus that cost. Finally, both industry best practices and applicable codes and ordinances must be followed in the implementation of those countermeasures.

This page intentionally left blank