Physical Security and Operations

Important Note

While the suggestions offered in this chapter can be quite detailed, it is important to recognize that no manual can anticipate the unique circumstances at any institution. Therefore, use the suggestions given below as starting points for discussions with a security professional who will be able to assess your institution's particular set of circumstances and make specific recommendations.[1]

Physical security starts with a rather simple basic premise: those who do not belong on your institution's property should be excluded from your institution. This may happen in three (often interrelated) ways:

1. When those who do not belong are identified, stopped and denied admission by a person.
2. When those who do not belong are denied admission by a physical device, such as a locked door.
3. When those who do not belong are denied admission because they decide that your institution is too difficult to enter and thus they do not even try.

This section will consider the various methods of excluding those who do not belong:

- Access Control
- Key Control and Locks
- Protective Devices and Alarms
- Windows and Doors
- Fencing and Gates
- Protective Lighting
- General Deterrance

[1] Given the specific information discussed in this chapter, it is important to again specifically mention that neither this guide nor this chapter is intended to provide comprehensive, institution-specific advice on security matters nor is it meant to replace the advice of a security professional. For comprehensive, institution-specific security advice, a security professional should be consulted. ADL specifically disclaims any and all responsibility for, and is not responsible for, any loss or damage arising out of use, nonuse or misuse of this information.

Access Control

Access control means that, when your facility is open, no visitor, delivery service person or unknown individual is able to enter your facility without being both *observed* (directly or indirectly) and *approved*. Several techniques to accomplish that goal may include any or all of the following.

Security Desk

A security desk should be set up in the main lobby of each building which has an open-access or open-door policy. A sign-in/-out log, supervised by an employee who validates identification *prior* to allowing visitors to proceed into the building, is highly advisable.

Monitored Entrances

Ideally, an institution should have a single entrance only, monitored by a staff person and equipped with an intercom system for communicating with anyone who comes to the door. Simply, an open door policy does not mean that every door need be left open and unlocked.

Checking Credentials

Before allowing a person to enter institution property, seek to make certain his/her identification papers or other credentials (including membership cards) are valid. Police and most utility employees carry identification cards and other documents. It is critical to remember that your employees can probably not tell the difference between valid and forged documentation or credentials. It is questionable whether your staff can be expected to tell the difference between the real and the fake. It is very easy to purchase a uniform or equipment that enables an intruder to pretend as if he/she has legitimate reason to enter your facility, and without verifying a person's identity or legitimacy, it will be difficult to identify a potential intruder. It is worth a few moments to contact the person's company or organization to determine the legitimacy.

NEVER BE EMBARRASSED TO ASK FOR MORE IDENTIFICATION OR TO ASK A PERSON TO WAIT UNTIL HIS/HER IDENTITY MAY BE CHECKED. ANY INDIVIDUAL WHO BECOMES AGITATED OR ANGRY AT SUCH A REQUEST SHOULD BE CONSIDERED OF QUESTIONABLE LEGITIMACY.

Visitors

At no time should visitors be allowed to roam freely through your property unescorted or without being observed. That is especially true for individuals who expect to work on your most sensitive systems such as burglar alarms, fire alarms, communication systems or computers. Special diligence should be applied to those individuals when they visit your institution even if they are legitimate. For larger institutions, certain areas should be considered off-limits to all but authorized personnel.

Note: Some institutions specialize in open and free access, e.g., facilities with gymnasiums. Allowing visitors free access to your facility does not mean that they should be allowed to go anywhere (e.g., into restricted areas such as office spaces) or that they should be given a sense that their actions are entirely unnoticed by the institution's personnel.

Stay-behinds

End-of-day locking procedures should include a visual examination of all areas to prevent "stay-behind" intruders.

Photo Identification:
Employee Photo Identification Cards and Badges

All employees should have and wear identification. Such badges make identification of non-employees immediate. Moreover, such cards will not only enable visitors to immediately identify those who work in an institution but will psychologically help employees understand that they are part of their agency's security team. Photo identification should only be provided with accompanying education regarding their care, the procedure to be followed if they are lost, as well as the manner in which employees should approach unknown individuals.

Creating ID badges requires thought. Cards should have clear pictures along with the employee's name. The institution's name should not necessarily be placed on the card. In any event, employees should be instructed that their card should be prominently worn while in the building and, for their own safety, kept from view when away from the building. There is no reason why a person in the street or in a train should be able to identify who you are and where you work. Lost cards should be reported immediately.

Key Control and Locks

Key Control

Knowing who has which keys to which locks at all times is a vitally important issue. Failure to maintain such control may defeat the entire purpose of creating a security system. Institutions often simply assume that no one leaving their service — either an employee or volunteer — will subsequently break into their building or office. A sound key-control policy is essential to an effective security program. There should be a central key control location where masters are kept and access to which is strictly controlled.

Other Thoughts

- **Registry.** A central key control registry should be established for all keys and combinations. Employees and leadership should be required to sign for keys when they are received and the return of keys should be an important part of an exit process.

- **Issuance.** Supervisory approval should be required for the issuance of all keys and locks. Spare keys and locks should be kept in a centrally located cabinet, locked under the supervision of a designated employee. *Master keys* should be issued to a very restricted number of employees and these should be inventoried at least twice each year.

- **Re-keying.** When key control is lost, it may be worthwhile to have an institution's locks re-keyed.

- **Combination Locks and Codes.** Where combination locks and coded locks are used, those combinations and codes should be changed *at least* every six months or when employees or leadership leave your employ. Combinations should also be kept under strict control of management.

- **Special Keys.** It is good policy to use locks with keys that cannot be duplicated on the outside without special key blanks.

- **Key Card Readers.** Key card readers, while expensive, make key control and locking more effective. You should designate who receives what form of access; i.e. time/day/weekend, etc.

Locks

Locks are, of course, particularly important to security. **We encourage you to consult a professional locksmith.** While the suggestions offered in this section are especially detailed, it is important to recognize that no manual can anticipate the unique circumstances at any institution. Therefore, use the ideas addressed below as starting points for discussions with a professional locksmith who will be able to assess your institution's particular set of circumstances and make specific recommendations.

Door locks should be chosen and installed to provide proper security for the location involved. Locks with single cylinders and interior thumb turns, installed on doors with glass panels, should be placed more than 36 inches away from the nearest glass panel. Dead bolt locks are the most reliable and should seat at least an inch into the door frame or lock-bolt receiver. Padlocks should be of high-grade material designed to withstand abuse and tampering.

AT ALL TIMES, THE DOOR-LOCKING SYSTEM MUST MEET THE FIRE CODE TO ALLOW EMERGENCY EXITING WITHOUT IMPEDIMENT.

- Further Considerations

  Exterior Locks. All exterior door lock cylinders should be protected with metal guard plates or armored rings to prevent cylinder removal. The guard plates should be secured with round-head carriage bolts. Some highly pick-resistant cylinders have a guard plate assembly built around them.

All exterior locks should conform to the following.

- Lock cylinders should be highly pick-resistant.
- Where possible, dead bolt locks should have a minimum bolt extension of one full inch.
- Drop-bolt locks should be installed with the proper strike: wood frame, angle strike; metal frame, flat strike.
- Metal guard places or armored rings to prevent cylinder removal. The guard-plate should be secured with round head carriage bolts. Some highly pick-resistant cylinders have a guard plate assembly built around them.
- The jamb must also be sufficiently strong. A strong lock entering a weak jamb will fail in its purpose.
- At all times, the door-locking system must meet the fire code to allow emergency exiting without impediment.

Automatic Closers. Doors that have air, hydraulic or spring returns should be periodically tested to ensure that doors consistently return to their fully closed or locked position.

Lock Management. Your institution's security manager should be responsible for the following:

✓ Regularly inspecting and reporting all defective and damaged locks; repair quickly.

✓ Establish a chain of responsibility for all locks (doors, windows, etc.); ensure locks which are to be locked are in fact locked and report all failures to do so.

✓ See that keys are not left unattended.

✓ Recommend installation of additional locks where necessary.

Remember: locks are present not only on doors, but on windows, offices, filing cabinets and storage closets as well.

Protective Devices and Alarms

This is an area where professional advice is particularly needed. Begin by contacting your local law enforcement agency and request help from the crime prevention, crime resistance or burglary prevention officers who are specially trained and can offer expert guidance. Keep in mind that an officer is not selling a product or system but is there to help you.

Protective Devices

Protective devices — intrusion detectors, fire detection, alarm systems and cameras slaved to a closed-circuit TV (CCTV) system — can be an important (and sometimes costly) part of an institution's security system. CCTV coverage may also be useful as such systems permit surveillance of exterior exits and interior halls by one trained security officer at a master console. However, even the most sophisticated and costly devices are limited by the human factors involved. The best CCTV system will be ineffective if it is not properly monitored or if those tasked with monitoring the cameras are overworked, poorly trained, tired or distracted. Additionally, most institutions are unlikely to have the resources for continual monitoring. An alternative is a videotape system, but here, too, the best video surveillance system will fail when not properly used, e.g., when no one is assigned the job of checking, reviewing and changing the tapes.

Other Thoughts

- ✓ Surveillance cameras should be conspicuously placed at the entrance points to your institution to act as a deterrent to potential intruders. Cameras may also document criminal acts that may occur on your property. This documentation can be used to identify and prosecute perpetrators. Although expensive to purchase initially, these cameras generally prove to be economical when compared to potential loss.
- ✓ Use a wide-angle lens to survey entrances.
- ✓ Consider using cameras that employ infrared illumination to enhance nighttime video or provide adequate lighting.
- ✓ Couple the camera with a time-lapse recorder for permanent recording.

- ✓ Make sure your camera has a time/date recording capability, and it is working.
- ✓ Compare the cost of color versus black and white.
- ✓ Save video film for a minimum of 72 hours, permanently if anything of a suspicious nature is seen.
- ✓ Replace video film at least every six months.

Alarms

This is another area where professional guidance is strongly recommended. Alarm systems are designed to protect your institution from intrusion. The installation of an alarm system can materially improve the security of most institutions. The sophistication and coverage provided vary widely from system to system.[2]

The size, location and type of institution will help determine the type of system required. Special features such as emergency panic buttons and robbery signal circuits should also be considered.

Motion detectors or automatic sensors that respond to sound or movement are excellent protective devices used alone or in conjunction with your institution's lighting system. These detectors and sensors are economical and they can be used inside or outside of your setting.

Because there are many alarm systems on the market, you should research each system and select the one that best suits your needs.

Two effective, inexpensive solutions are alarms that use magnetic contacts and trip wires. Alarms with motion, sound or light detectors are more expensive but are also generally more dependable. Whatever the amount of money you choose to invest in a dependable alarm system, it is generally less than the amount of damage that might be caused to your institution by an intruder gaining access.

[2] Most alarm systems are made up of three components: (1) a sensor, which detects an intruder, (2) a control, which receives information from the sensor and (3) an enunciator, visibly, audibly, or elecronically alerting someone of the intrusion.

When installing an alarm system, consider the following.

- ✓ Make sure all alarm systems have emergency backup power sources.
- ✓ Conceal the alarm control box, lock it, and limit access to it.
- ✓ Every system should have an electronic circuit delay of at least 30 seconds.
- ✓ Ensure that the alarm can be heard throughout the property and have the alarm system monitored by a central alarm monitoring company.
- ✓ Make sure all wiring components and sirens are protected from tampering.
- ✓ Make sure the alarm comes with a "test" option. Testing the system regularly is a vital component of maintaining the effectiveness of your alarm.

Windows and Doors

Windows

Windows should provide light, ventilation and visibility, but not easy access. Glass bricks can be used to seal a window, allowing a continued light source while providing increased security, although visibility and ventilation will be diminished. Gates and expanded steel screening, while often unattractive, will provide a high degree of security. Local building codes and fire safety regulations should be consulted prior to all such installations to avoid costly violations. Also, note that skylights, ventilators and large door transoms can provide easy access to intruders unless properly protected. If permanent sealing is not possible, steel bars or screens of expanded metal may be required (if permitted by fire codes).

A Critical Note on Glass

Flying glass can be as dangerous in an explosion as the actual explosion itself. Consider replacing traditional glass with safety or shatter-resistant glass or using a clear protective film to secure the glass to the frame.

Doors

All external doors, main building doors, and lobby doors leading to common halls should conform to the following guidelines.

- Solid core, wood or metal.
- Glass door panels or side panels should be reinforced either with metal or some form of steel mesh. Barring that, they should be replaced with a glass that does not shatter easily.
- Where there is an alarm system, "glass breaker" sensors that detect glass breakage should be installed close to glass doors or windows.
- Door frames should be sturdy and appropriate for the type of door. Weak frames should be replaced or rebuilt.
- Exterior door locks should conform to the guidelines found in the section on locks.
- Interior or office doors should be equipped with heavy-duty, mortised latch sets that have dead bolt capability. Rim-mounted, dead bolt or drop-bolt locks can be installed to increase security of important offices or rooms.
- Doors that have external or exposed hinges may be vulnerable to pin removal. The hinge pin should be made unremovable by spot welding or other means or the hinges should be pinned to prevent separation.
- Doors to utility closets should be equipped with dead bolts and kept locked at all times. Such closets, if unsecured, can become hiding places for "stay-behind" criminals or for the placement of explosive devices.
- All exterior doors which do not have glass vision panels should be equipped with wide-angle viewers (peepholes).
- Interior doors should have two-way visibility at stairways, corridors, etc. There should be a clear view of room interiors from the doorway. Note, however, lockdown procedures (see section on lockdown procedures) may require the use of rooms without windows, or, at least, doors whose windows can easily be covered.
- Access to offices, kitchens, electrical and mechanical rooms and storage rooms should be limited to appropriate staff and be locked when not in use.

- Fire doors must conform to all local fire and building codes and should have an underwriter's laboratory rating.
  - Fire doors should be secured with approved latching or locking hardware, such as a panic bar with a spring latch or safety lock.
  - If a fire door has a solid core, the interior material must be fire resistant.
  - An adjustable spring or air return will ensure that the door is always closed.
  - Consider the possibility of placing height marks next to exit doors to help employees estimate the height of suspicious persons.
  - As with all doors, sensor devices connecting to a sound device or system will announce their opening.
  - All doors or gates not observed either directly or remotely should be kept secured.
  - Staff should be discouraged from using wedges to keep outside doors open.

Fencing

Fences make an intruder's entry more difficult and give the appearance of a more secure institution. The following thoughts need to be prefaced with an important warning applicable to all sections of this manual: take note of all local building and zoning codes regarding fences and walls prior to planning or contracting.

Some thoughts to bear in mind:

- Consider open ornamental fences — in preference to walls — as they do not block visibility, are less susceptible to graffiti and may be more difficult to climb.
- Fences should be at least six feet high. Therefore, an institution should take advantage of any small incline or hillock along which to build the fencing.

- Fences should also be designed so that a person cannot reach in with his/her hand or a wire to open the fence gate from the outside.
- If a panic bar is required on the inside of a fence gate, a solid metal or plastic shield should be used to prevent a person on the outside from opening the gate.
- It is important that whatever physical barrier one erects should be in concert with the aesthetics of the neighborhood or environment.
- **It is unwise to alienate neighbors who may serve as part of a neighborhood watch and provide additional "eyes and ears" as part of your overall security program.**
- Walls should be constructed where there is a need for privacy and/or noise control.
- Fence lines should be kept free of trash and debris. Clear away trees and vines that might aid a climber. Weeds and shrubs along fence lines, sides of buildings, or near entrance points could hide criminal activities. Keep shrubs low — under 36 inches — or clear them away completely. Cut back vines attached to buildings in order to prevent determined intruders from gaining access to upper windows or unprotected roof doors.

Note: No barrier is foolproof. It is impossible to erect an impenetrable physical barrier that is unprotected by personnel. Even when protected by personnel, human beings grow fatigued, inattentive, bored or simply make mistakes.

Protective Lighting

The value of adequate lighting as a deterrent to crime cannot be overemphasized. Adequate lighting is a cost-effective line of defense in preventing crime.

Some Considerations on Lighting

- Lighting, both inside and outside, is most helpful and can be installed without becoming overly intrusive to neighbors.
- All entrances should be well lit. Fences should also be illuminated.
- For outside lighting, the rule of thumb is to create light equal to that of full daylight.

- The light should be directed downward away from the building or area to be protected and away from any security personnel you might have patrolling the facility.
- Where fencing is used, the lighting should be inside and above the fencing to illuminate as much of the fence as possible.
- Lighting should be placed to reduce contrast between shadows and illuminated areas. It should be uniform on walkways, entrances, exits, and especially in parking areas.
- Perimeter lights should be installed so the cones of illumination overlap, eliminating areas of total darkness if any one light malfunctions.
- Fixtures should be vandal-resistant. It is vital that repair of defects and replacement of worn-out bulbs be immediate. In addition, prevent trees or bushes from blocking lighting fixtures.
- You may wish to use timers and/or automatic photoelectric cells. Such devices provide protection against human error and ensure operation during inclement weather or when the building is unoccupied.

A security professional should be contacted to help you with decisions on location and the best type of lighting for your individual institution.

General Target Hardening

One function of security devices, lighting, fences, etc., is to make your facility look less inviting to a potential intruder. The more uninviting your institution is to such an individual, the less likely the incursion. This is called "target hardening." While an institution should not reveal the details of its security measures, providing a potential attacker with clear evidence that a security system is in place will often deter an attack before it happens. Some examples of deterrants:

- Signs indicating the presence of an alarm system.
- Visible security foot and/or vehicle patrols.
- Well-maintained fence lines and lighting.
- A general appearance of a well-maintained facility.
- Regular presence of local law enforcement on or near your grounds.

Anti-Defamation League®

Barbara B. Balser, *National Chair*
Abraham H. Foxman, *National Director*

This guide is intended to help institutions become aware of basic security considerations. It is not intended to provide comprehensive, institution-specific advice on security matters nor is it meant to replace the advice of a security professional. For comprehensive, institution-specific security advice, a security professional should be consulted. ADL specifically disclaims any and all responsibility for, and is not responsible for, any loss or damage arising out of the use, nonuse or misuse of this information

Printed in the United States of America
All rights reserved
Web site: **www.adl.org**