

SECURITY GUIDE

Facility Physical Protection

Theft, robbery, assault, vandalism, arson and other crimes against people and property can create serious problems for a business, for employees, and for others.

Some businesses never have crime-related problems, but others have more than their share. In 2016, the FBI reported an estimated 1,515,096 burglaries. Thirty percent of these burglaries were at non-residential locations (stores, offices, etc.).

A large quantity of stock and high-value items can tempt people who otherwise would not consider themselves criminals. One of the more disturbing aspects is amateurs, without elaborate equipment or planning, and sometimes on impulse, commit many crimes against property. This erratic pattern, along with the mobility of today's society, has succeeded in making almost any property a target risk.

A professional thief with intent to violate your property can be difficult to stop. Your best defense might be to delay access and detect entry points. Loaded cargo awaiting delivery can be locked inside the building or containers within a guarded fenced area. A perpetrator may decide to select a lightly protected target over more secure targets.

Consider the protection available for vulnerable points around a facility. Physical property protection strategies often develop with a consideration for the five Ds of physical security.

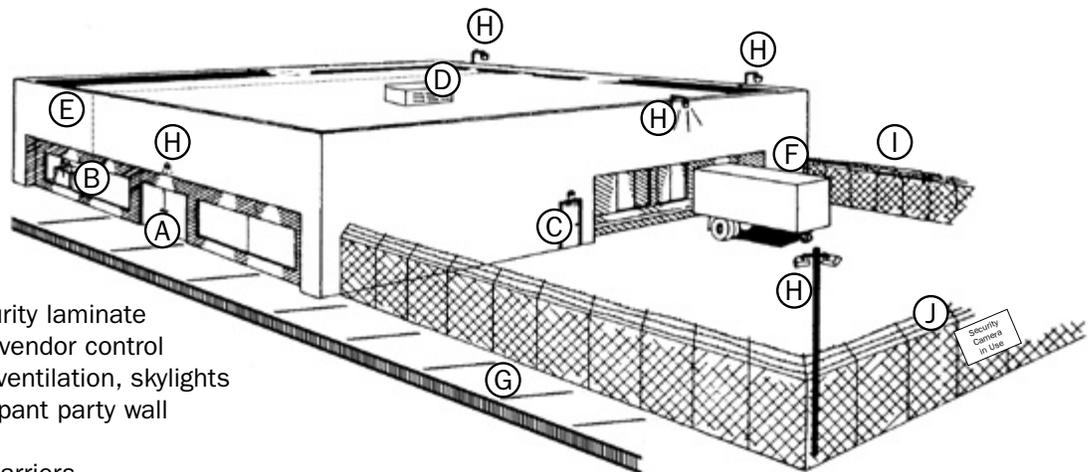
Deter — hang signage, giving the impression of security with access designs and lighting

Detect — use natural and passive surveillance, use of active sensors and alarms

Delay — reinforce the perimeter with gated fencing, door locks, and treated window glass

Deny — harden access to targeted items with safes, vaults, or interior caged areas

Defeat — arrest or use of force by police or security guards



- A. Door locks
- B. Windows security laminate
- C. Loading dock vendor control
- D. Roof access, ventilation, skylights
- E. Adjacent occupant party wall
- F. Cargo, freight
- G. Fence, curb, barriers
- H. Lighting, surveillance cameras
- I. Open lot, alley
- J. Signage

DETER

Crime prevention through environmental design

attempts to address the attitudes and behaviors that cause crime, while increasing the perception or reality of surveillance. Your local police department might suggest property management actions for establishing a perimeter and controlling access.

- Defined boundaries help identify places where people need to have a reason to be there. Keep the area around the building free of high grass, weeds, or brush that could provide cover for criminals. While fencing can be a deterrent, consider avoiding solid fences, which make easy hiding places.
- Keep control over your territory. Remove graffiti tags. Prohibit loitering. Post and enforce “Private Property” or “Customers Only, No Trespassing” signs.
- Post the use of alarm and camera surveillance.
- Maintain the property with a well-kept appearance to help show a perpetrator you are organized with a cared-for facility.
- Provide a controlled access point for employees, vendors, and visitors. Designated entry doors and a main gate are examples.

Strategic lighting is an important security element.

Burglars normally depend on darkness to conceal their actions, so lighting, both inside and outside, may help serve as a deterrent. This includes lighting areas on either side of fences, storage yards, and alleys. Illuminate all accessible building openings. Lights mounted on high poles tend to reduce shadows where outdoor items are stored, and increases the likelihood that thieves can be detected where there are fewer shadows to hide in. Exterior lights positioned low and facing toward the building tend to amplify a silhouette to identify movement and facilitate surveillance. However, the lower light location makes it easier to disable. Interior lights should be placed so that an intruder’s silhouette can be seen from the street if the building has windows.

Using timers, photocells, and motion detectors helps to ensure lights are efficiently turned on. However, lighting may not be helpful where a burglar has no fear of being caught and there is no patrol or other surveillance. If you have video cameras to record activities, the type, direction, and placement of lighting should be considered for picture quality. Also, consider the ease of lamp replacement, effects of weather, and local or state outdoor lighting ordinances that may apply.

Further guidance about security lighting is available from the Illuminating Engineering Society of North America, who published a consensus standard, IESNA G-1 Guideline for Security Lighting for People, Property, and Public Spaces¹.

DETECT

Monitoring and detection usually means alarms for:

- Perimeter protection of all building openings
- Area protection inside the building
- Object protection — safes, vaults, door contact points, or sensors to detect an approach from all sides of an object

Alarm sensors are available to detect trespassing and attempts made to go through a wall, floor, or ceiling.

Detection through monitoring may be done by direct human observation or a combination of technical security measures (alarm sensors, closed-circuit television, thermal imagers, or intelligent video) to initiate a response. The detection of a perpetrator generally should occur at a point that will provide the shortest delay between detection and the arrival of security responders.

Private security companies can survey your business to determine the number and location of monitors needed. There are several different types of electronic security systems, with most being monitored from a central location. Perpetrators are normally warned that they are under surveillance and often stop their burglary attempt.

Intrusion detection becomes more desirable if the business is located in an area where unusual activity after business hours is likely to go undetected, or, if noticed, not be reported to the police.

- Have the alarm system monitored. This means a supervised signal is sent to a remote monitoring location when activated.
- Test the system at least monthly for proper operation.
- Investigate and keep a record of false alarms. A pattern may explain why the alarm is triggered and indicate needed adjustments or repairs — or a potential burglary scheme.
- Remember to update the alarm system when a facility is remodeled, especially where new doors and windows are installed.

For more about security alarms, see Federated [F70-764 Security Guide 107 Burglar Alarms](#), which describes various types of burglar alarms and methods of detection, along with alarm transmission. Further details are also available in National Fire Protection Association, NFPA 731 Standard for the Installation of Electronic Premises Security Systems².

Surveillance cameras are a major advancement in security. For more about surveillance security cameras, see F70-729 Surveillance Cameras, which describes the use of surveillance camera systems.

Verifying physical inventory helps detect internal shrinkage or theft, and when a thief has removed items. Having up-to-date inventory records and acquisition costs can help establish the amount of loss.

DELAY

Perimeter barriers can be used in a variety of ways to help increase overall facility security.

- Controlling vehicle access to an area by roadways, paved curbing, barrier guards
- Providing a channel to a gate or controlled entry point for pedestrian access
- Delaying forced building entry by construction techniques applied to walls, roofs, doors, and windows
- Protecting assets with a physical obstruction

Fencing is the first item of concern when protecting an open lot. A good fence is an excellent first obstacle, keeping many intruders out, and encouraging casual thieves to ignore a property. Chain link fencing, which maintains visibility, is ideal. The fence should be six to eight feet high with posts set no more than 10 feet apart. Top rails, which can help support a thief climbing over the fence are often not used. Three-strand barbed wire or rolled razor wire on top of the fence is good in areas with less traffic, such as the rear and sides of the lot. Note: Some fence types are restricted by local codes.

Selected ASTM International³ consensus standards for security fences are:

- ASTM F2611 Standard Guide for Design and Construction of Chain Link Security Fencing
- ASTM F2814 Standard Guide for Design and Construction of Ornamental Steel Picket Fence Systems for Security Purposes
- ASTM E2942 Guide for Security of Tank Farm Installations for Compliance with SPCC Regulations

Life Safety Code (NFPA 101)² provides guidance for the design, operation, and maintenance of buildings and structures for safety to life from fire and similar emergencies. Physical barriers or security systems used or installed in a building should comply with applicable fire code or other life safety requirements. Exit passages should generally be unobstructed with no special knowledge needed to escape in an emergency.

Door and access control locks are crucial for security. A door with a solid core and frame, a high-strength strike plate, and strong doorjamb are key to preventing a forced entry. Prevent easy removal of doors by welding hinge pins into place or use a hinge with a setscrew on the inside of the hinge.

The type of locking mechanism is just as important. Single-cylinder locks require a key from the outside but use a thumb lever to unlock from the inside. Double-cylinder deadbolt locks require a key to unlock from the outside and from the inside. The double cylinder used on exterior doors enhances security where the lock is near a window and within arm's reach.

Additional lock or blocking mechanisms can help increase the security around the door. Brackets holding a drop bar across the inside of a pedestrian door is one example. Overhead doors locked with a padlock or bolt in the track above a roller on each side of the door also helps block this type of door from opening. Electricity to overhead door openers can also be disabled.

Keyless locks, or credentialed access, started growing in popularity a few years before the news media started reporting on lock-bumping crimes. If you decide to install a keyless lock, make sure it is bump proof. Many of the older types still have key cylinders that can be picked using a technique for opening a pin tumbler lock in a few seconds.

Electronic types of access control locks include:

- Key fob proximity lock
- Smartphone controlled
- Biometrics face recognition
- Mobile credentialing
- Touchpad
- FIPS-201 credentials
- Two-factor authentication
- Enterprise card systems

A fail-safe lock uses electrical current to keep the door locked. It unlocks during a power outage or when an emergency alarm is triggered. A fail-secure lock is one that remains locked and needs electrical current to disengage. These locks are often used in higher-security situations.

Windows made with force-resistant glazing or a retrofitted security laminate can be effective at preventing or slowing down forced entry. Such protection is also useful on showcases, especially if displaying items of significant value. This can help prevent a smash-and-grab loss. Additional security can be provided by the use of metal roll-down gates on the inside of windows and doors, if appropriate for the location.

Reinforced walls and secured roof openings strengthen security. Although it is concrete, a hollow block wall is easy to break through. If possible, plan for extra security needs during construction. Use of reinforcing bars or expanded metal sheeting is often required for a security vault room. Roof-top building ventilation is often a point of entry. Ladders fixed to the side of a building for maintenance access should be blocked and locked.

Make sure the facility cannot be easily entered through a neighboring occupancy. Cutoff walls between tenants, which are made of solid masonry construction, complete from the floor to the roof, are best. Any openings, including rooftop mechanical services for the building, should be locked with suitable hardware. Be especially alert if a neighboring business becomes vacant. Thieves could cut a hole in the wall from a vacant occupancy to enter your area during the night. A perpetrator can also be waiting on the inside for you to open a safe or vault in the morning.

DENY

Consider the use of case hardened locks with chains or cables to immobilize large valuable items.

Indoors or outdoors, fenced or caged partitions should be used for high-value items or target stock. Electronic access controls to these areas provide an audit trail for who entered and when, and help identify a perpetrator of internal theft.

Consider storing valuables in a UL burglary-rated safe or vault that is appropriate for your level of needed security. Federated [F70-763 Security Guide 104: Burglary-Resistant Safes](#) provides more information on different classifications and characteristics of safes, as well as other security considerations.

Pre-employment testing or investigation of applicants who would have a security-sensitive or safety position can help keep businesses from hiring a security threat. Consider evaluating applicants who would handle currency, have routine access to building master control and key systems, work in an area designated as a security-sensitive, or drive company vehicles and/or equipment. Federated has arranged for IntelliCorp® to offer a cost-effective package to simplify your background check process. More information is available online at federatedinsurance.com.

DEFEAT

Collaborate with other businesses to work with private security and law enforcement in your area. Check your insurance policy to see if a temporary security guard service may be covered when it is necessary to provide security because of a covered loss or a failure of an alarm system.

Security dogs can present a risk if the dog is aggressive to a customer. Having the dogs securely restrained or kept in a fenced area during business hours is generally advised. Using a service that delivers perimeter guard dogs after business hours helps manage the efforts.

Develop a daily walk-through of the facility to detect any tampering. Encourage employees to report anything suspicious. Be deliberate about how security concerns should be reported.

Establish a closing final inspection.

- Double-check all doors and windows.
- Verify that high-value items are secured.
- Check to see that no one is hiding in or around the building.
- Turn on night lights.
- Check and activate the alarm system.

Endnotes:

[1] Illuminating Engineering Society 120 Wall Street New York, NY 10005-4001

[2] National Fire Protection Association 1 Batterymarch Park Quincy, Massachusetts 02169-7471

[3] ASTM International 100 Barr Harbor Drive West Conshohocken, PA 19428-2959

This publication is for general information and risk prevention only and should not be considered legal or other expert advice. The information herein may help reduce, but is not guaranteed to eliminate any or all risk of loss. The information herein may be subject to federal, state, and local, rules and regulations. Qualified counsel should be sought with questions specific to your circumstances.



Federated Mutual Insurance Company • Federated Service Insurance Company*
Federated Life Insurance Company • Federated Reserve Insurance Company* • Granite Re, Inc.*†

*Not licensed in all states. †Granite Re, Inc. conducts business in California as Granite Surety Insurance Company.
F70-762 Ed. 10/19 | federatedinsurance.com | © 2018 Federated Mutual Insurance Company