TRAVELERS

Insurance. In-synch.SM

Risk Control

Premises Security & Burglary Risk Management Guide

Unfortunately, crime is a fact of life in the business world, but that doesn't mean you have to be a victim. By taking the necessary security precautions, you can minimize the potential for crime.

This guide provides general information on work practices, procedures and technology that can help protect your business, employees and bottom line. It is not a comprehensive resource, however, and you should review your particular needs with your own legal counsel. You also may want to consult with a certified security consultant or security integrator.

Put the protections in place.

Fact

> In 2000, estimates indicate business and economic crime cost the U.S. economy more than $200 billion annually.

> The retail sector experiences 30 percent of crimes.

> Inventory shortages may total 3 percent of sales nationwide.

> The Small Business Administration estimates that two-thirds of the money lost by the business community is a result of robbery.

> Burglary is the most prevalent crime in the country.

> Non-residential burglaries total about 30 percent.

> According to the U.S. Justice Department, shoplifting has increased at a rate of 5 percent per year over the last nine years, costing U.S. businesses approximately $10 billion annually.

> According to the Association of Certified Fraud Examiners, businesses with fewer than 100 employees were most vulnerable to fraud (small businesses had a median loss per occurrence of $120,000).

Employee Selection

The most serious threat to businesses is internal theft and no business is immune from it. The first line of defense is to hire honest employees.

> Develop a comprehensive employment application form that will allow for an in-depth exploration of the applicant's background. The form should be consistent with federal and state requirements and should include, at a minimum, information

about residence, education, job history, criminal arrest and bankruptcy filing and references.

- Require applicants to fully complete and sign the application form, accounting for any gaps in information.
- Check references and previous employers by mail or phone. All questions by telephone should be direct. Letter inquiries should be designed as check-off type questions, not requiring narration-type answers and should include a self-addressed, stamped envelope.
- Perform five years of criminal and credit checks depending on the importance or sensitivity of the job. The Fair Credit Reporting Act provides general guidelines that employers must follow when performing background investigations. Employers should also become familiar with federal and state laws regarding applicant/employee screening.
- Develop a list of questions for the job interview that will provide insight into the applicant's character.

Negligent Security

- Damages have been awarded to plaintiffs in premises security suits in which they were injured as a result of a crime. In these cases, plaintiffs try to demonstrate that the business failed to meet its security responsibilities. This could easily happen to you without the proper security measures in place.
- Plaintiffs in the cases typically bring up the following circumstances. Business owners should look at these areas and act where improvement is necessary.
  - Earlier, similar incidents – references to past incidences.
  - Local crime – reference to neighborhood crime information and statistics
  - Character of the neighborhood – reference to the surrounding areas
  - Type of businesses – references to statistics with regard to crime data on that type of business
  - Patron complaints – references to any relevant past complaints
  - Expert advice – references to improvements recommended by police, for example, but not completed
  - The business did not meet the standards defined for that type of business – references local ordinances, state or federal laws, comparable local businesses or industry association guidelines

Contact your local police department to learn if they offer a community crime prevention program. If one exists, it could be a great resource as you evaluate your premises for crime control measures. It's to your advantage to learn from, and work with, your local law enforcement officials.

Access Control

You may want to restrict access to certain areas of your business facility, such as high-value storage areas, safes/vaults, computer/telephone rooms, a back room office, a warehouse or an entire building, depending on the nature of your operation. With more incidents of workplace violence, the threat of terrorism and equipment theft, many companies now use access control systems. These systems can range from simple push-button locks to sophisticated card access systems integrated with closed circuit televisions. The access control system is designed to screen or identify individuals prior to allowing entry. It also assists in providing area access reports to satisfy recent federal legislative mandates, such as Sarbanes Oxley.

Stand-Alone Systems

Stand-alone systems are used to control access at a single entry point and are available either as one integral unit or two separate components – a reader/keypad and a controller. While stand-alone systems can be networked, they generally do not require a CPU – data for the entire user population is stored within the server or workstation unit.

Enterprise Security Systems

Enterprise security systems are part of a large network of readers connected to a workstation, which regulates activities at more than one entry point at a time. These systems can be more expensive because of the need to connect to a CPU from multiple ports. These devices are networked together by using the company LAN/WAN. User access verification is made locally as a mirror copy of the database is held in the local door controller.

Card Technologies

Several types of card encoding technologies are now available with the following options and considerations:

- Encoding security
- Susceptibility of the card reader to environmental damage
- Resistance of the reader to vandalism
- Cost – initial and long term

Magnetic Stripe

This used to be the most widely used system. Today, proximity cards have overtaken magnetic stripe units. It is the same application commonly used on ATM cards. Although these systems are relatively inexpensive, they are one of the most insecure cards. They should only be used in low-security areas. For high-security areas, this type of card should be used in combination with a biometric device like a PIN pad or hand geometry reader. This type of technology is also subject to wear because of contact between the card and reader and vulnerability to the environment.

A disadvantage of the magnetic stripe cards is that they can easily be cloned or counterfeited by use of magnetic stripe encoders, which are readily available via the Internet.

Infrared

Data is stored on this card by means of a bar code written between layers of plastic. The card is read by passing light through it. Duplication is almost impossible. These systems are not frequently used because of the high cost, both initial and ongoing costs; however, they do provide a high degree of security.

Bar Code

Like magnetic stripe cards, this type of card is not widely used because the encoding security is very low and the bar code strip can be easily damaged. This technology can be easily compromised. Bar code readers are encoders that are readily available via the Internet.

Optical Storage

Optical storage cards can contain more than 4 megabytes of information. The data on the card is secure from compromise since the information on the card is usually encrypted and written into a reflective layer of plastic. The card reader is equipped with a solid-state laser. The user typically enters a passcode before inserting the card. These systems are initially expensive and require regular maintenance.

Hollerith

This system is the oldest technology in use. Data is written on the card by punching holes in the card. The card is read by either passing light through the holes or by fine contact brushes that connect with an electrical contact. It is very inexpensive, but also low in security.

Proximity

This type of card is gaining popularity because it simply has to pass near the reader instead of through the reader. Operating ranges are from 2 to 12 inches. Since the card is factory encoded, it is difficult to copy or counterfeit. The life of this system can be longer than others because there is no repeated contact between the card and the reader. Card access control systems are commonly used in these facilities:

- Hotels and motels
- Office buildings
- Universities and colleges
- Manufacturing facilities
- Warehouses
- Research facilities
- Hospitals

Other Technologies

- Smartcards – contactless and extended read range
- Biometric devices

For more information regarding access control, visit securityinfowatch.com.

Burglar alarm systems

An alarm system is generally a reliable safeguard to protect your business. Underwriters Laboratories, Inc. (UL) now has a Burglar Alarm Certificate Program that lists installation companies authorized to issue UL certificates on individual systems installations. The UL certificate states that the installer has completed UL’s required maintenance and testing. The benefits of the certificate program include quality installations, follow-up inspections, maintenance, false alarm reduction and more. You should insist on a UL certificate when you have an alarm system installed. For a list of UL-authorized dealers, visit their Web site at ul.com.

Central Station Systems

A central station burglar alarm system is designed to automatically transmit a signal to a central station in the event of an intrusion on protected premises. This station is staffed by trained operators and investigators who supervise, record and respond to the signal. The operator follows these steps if an alarm goes off:

- Obtains the premise information
- Dispatches alarm investigators
- Telephones the police for alarm incident investigation
- Notifies the point of contact via a predefined call list

Mercantile Systems

This type of system activates an alarm and sounds inside and outside the premises by means of electrical protection circuits. This system may not have remote location transmission equipment and is controlled by the property owner.

Bank Burglar Alarm Systems

This system also may not have remote location transmission equipment and is controlled by the property owner. It is most commonly used for bank safes, vaults, ATM machines or night depositories.

Proprietary Burglar Alarm Systems

A proprietary burglar alarm system is constantly monitored, but the personnel are responsible directly to the owner of the protected property. The response to an alarm would be similar to that of a central station alarm. When selecting an alarm system, be sure to get several estimates and insist on a UL-listed system and installer.

An alarm system is generally a reliable safeguard to protect your business.

Closed Circuit Television (CCTV)

CCTV is now part of safety and security systems in many places of business, including parking garages, warehouses, convenience stores, department stores, apartment buildings and office buildings. The applications are typically:

- Visitor identification
- Detection of criminal activity and employee theft
- Monitoring for criminal activity in parking lots or other public areas
- Surveillance on valuable items
- Deterrence to vandalism
- Remote facility identification and admittance
- Virtual security escorts

The typical CCTV system has a monitor and a television camera, with each camera needing its own power supply. CCTV offers a real-time or time-lapse video recorder, and records the actual crime, which may be useful in prosecuting the criminal and recovering stolen merchandise. Be sure to install cameras high enough to provide an unobstructed view and prevent tampering. Typical CCTV systems use both stationary and pan/tilt/zoom cameras. These units can be conventional or IP (internet protocol) units. They are interfaced with a digital video recorder (DVR) or Network Video Recorder (NVR). Video images are archived locally on the unit hard drive and accessed via a software application. It's important to identify the recording rate for each camera, also known as Frames Per Second (FPS) and the minimum number of days that they want to retain archived video. A rate of 5-10 FPS and 15 days storage is common. Users can use Windows Media Player to review exported video clips.

The camera selected for the application must be capable of operating with the available level of lighting. A system used during the day and night is required to operate in wide variations of light levels. Since different cameras respond to different wavelengths or colors, it is important to select a camera sensitive to the ranges of lighting that exist. Another factor to consider is whether you need a color or black and white camera. Color cameras tend to be more expensive, but you will be able to distinguish different items in a field of view. However, color cameras do not perform well in low light. Black and white cameras cost less and can perform better in low light. Most installed cameras are color models. Interior cameras are commonly color and exterior units can be combination units - color during daytime hours and converting to black and white in low light or evening hours.

The resolution of the camera also is an important feature. The higher the resolution, the better the picture. The camera defines the lines of resolution. Typical CCTV cameras are 640x480 lines of resolution. New high-definition cameras or IP cameras record at higher rates. The use of low-light lenses with an auto iris also is critical. Be aware that new DVR/NVRs use computer monitors with higher monitor resolution.

Take note that it is important to have someone constantly monitor the system if it is for the protection of the public. There have been cases brought to suit where CCTV systems were in place without any monitoring. A crime took place and nobody responded, resulting in a lawsuit against the business owner. If you install CCTV, establish a written policy regarding response, recording, monitoring, storage of tapes and incident documentation. Communicate that policy to the appropriate employees and make sure the policy is followed.

For more information regarding CCTV systems, visit asisonline.org.

Employee theft is considered the most serious crime exposure for retail businesses.

The term burglar alarm system is becoming out dated. The new term being used is Intrusion Detection Systems (IDS). You should be aware that most IDS systems are fully integrated with access control systems and CCTV systems. This way, they can incorporate card readers, report alarms and, if there is a camera in the area, can produce video of the alarm event.

Lighting

Lighting systems increase the chance of an intruder being detected and enhance the safety of customers and employees entering and leaving a facility after dark. Lighting systems also enhance the effectiveness of CCTV by increasing the visual range of CCTV cameras in low-light situations. We suggest the following guidelines for your lighting system:

- Provide proper illumination of all exterior areas in a facility, including pedestrian and vehicular entrances, perimeter fence line, sensitive areas or structures and parking areas.
- Make detection certain.
- Avoid glare affecting the view of a guard, passing traffic or nearby buildings.
- Direct the glare at intruders.
- To avoid CCTV camera detection – use tinted domes or surreptitious cameras.
- Install enough lights so the outage of a single lamp does not cause a dark spot and leave an area vulnerable.
- Provide back-up illumination in the event of a power failure.
- Inspect and maintain lighting systems on a regular basis.
- Use white or other light colors to improve the effectiveness of the lighting system.
- Adequately light entrances, exits, elevators, walkways and parking areas for safety and security. The Illuminating Engineering Society (IES) Lighting Handbook (available for purchase at iesna.org) describes minimum illumination requirements. Parking facility requirements, for example, are defined based on the level of activity.
  - High-activity facilities include sports stadiums, civic events facilities, regional shopping centers and fast food facilities.
  - Medium-activity facilities include community shopping centers, office parks, hospital parking areas, transportation parking, events parking and residential complex parking.
  - Low-activity facilities include neighborhood shopping centers, industrial facility employee parking, educational facility parking and church parking.
- Ensure foliage and trees near light fixtures and entrances are properly trimmed and maintained so they do not adversely affect lighting dispersion.

Employee Theft

Employee theft is considered the most serious crime exposure for retail businesses, and is often called white-collar crime, workplace crime, internal theft, pilferage or stealing.

Many studies point to two common elements when discussing the causes of employee theft, including employee attitude and management responsibility. An employee who is dissatisfied may feel justified in stealing. They don't feel they hurt anybody by stealing from the company. Hard economic times can contribute to employee theft, as well as employment uncertainty, which may cause an employee to lose their sense of loyalty to a company.

Sometimes employees learn from their managers. Managers serve as role models and their behavior may establish a norm for other employees. Since managers hold a position of trust, they often tend to have the advantage over other employees with regard to their potential for theft. According to the U.S. Chamber of Commerce, employee crime is a sign of mismanagement because of these reasons:

- Inadequate supervision of employees.
- Work standards not provided.
- Work standards not enforced.
- Low priority for establishing basic controls.
- Poor attitude toward prosecution.

What to watch for:

- Employees who appear to be living well above their means.
- Employees who are incapable of handling their own finances and are constantly being pursued by creditors.
- Employees who are drug abusers; studies have shown that there is a high correlation between drug usage and pilferage.
- Employees who always come in early, leave late and never take a vacation; they feel their presence can cover up their illegal activities.
- Employees who are compulsive gamblers.

To help control employee theft:

- Establish a good pre-employment screening process.
- Arrange work flow and task assignments so the work of one employee acts as a control of another.
- Divide responsibilities so no one employee has control over all facets of a transaction.
- Reduce inventory exposure by keeping the shipping and receiving docks and warehouses clean and unobstructed.
- Establish a system of random inventory checks, audits and petty cash counts.
- Improve job satisfaction and enhance employee morale.

Laptop Computer Theft

Laptop computers, by virtue of their portability, are more vulnerable to theft than desktop systems. According to Safeware, The Insurance Agency, Inc., an insurance agency that specializes in insuring computers, electronics and high-tech equipment, laptop/notebook computer theft rose 21 percent from an estimated 319,000 units in 1999 to 387,000 in 2000. That's more than 1,000 laptop computers stolen every day. Assuming the price of the average laptop/notebook computer is $1,800, the cost to replace these stolen computers exceeded $700 million. Although most notebook computers are stolen for quick cash, 10 to 15 percent are stolen solely for the information on the hard disk.

In the Office:

- Never leave a laptop unattended or unsecured. A laptop locking device is available for any laptop, whether used in a docking station or not. Obviously, the key should not be kept in the locking device. The head of the MIS Department of a Washington, D.C.-based research firm stated that "5 percent of the company's laptops were stolen over the past year. Eighty percent of the thefts occurred in the office when the laptops were left unattended for a short while, or after hours."
- Mark the laptop with a serial number, which can be etched on the laptop or on self-adhesive plates. This will not prevent theft, but should help recover the laptop. Some companies use a bar code identification system.
- Electronic article surveillance systems can be used for protecting laptops. These are similar to systems used in department stores to prevent shoplifting.
- Install software on the laptop that uses the modem through a phone line to call a monitoring center. It can be programmed to call a predetermined call center the next time a phone connection is established. The number of the location making the call is identified and recovery is coordinated with local law enforcement.
- If docking devices are not available, use a laptop cable locking system.
- Many new equipment manufacturers are providing laptop GPS or tracking systems and working cooperatively with law enforcement crime prevention personnel to share serial number information for theft recovery.

While Traveling:

- Carry the laptop in a case that does not identify it as a laptop.
- When carrying a laptop bag, hold a hand on the strap to avoid becoming a victim of a "snatch and grab" thief.
- Don't ask a stranger to watch the laptop.
- Watch out for common distraction techniques like being bumped or having something spilled.
- Lock laptops in the trunk if it has to be left unattended in the car.
- Never check a laptop as luggage.
- Keep the laptop in clear view at all times.
- Never place the laptop on the conveyor belt of the X-ray scanner at airport security checkpoints until you're certain it is clear to proceed.
- Use hotel room safes for temporary laptop storage.

Dismantling containers, removing the goods and resealing the container is an example of cargo crime.

Transit/Cargo Security

As the prevalence of high technology products continues to increase in today's society, so does the amount of theft involving these products. The loss of high-valued, difficult-to-trace products, whether they are computers or microchips, is increasing at an alarming rate. Factors contributing to this trend include the following:

- A significant increase in the level of global trade.
- Larger shipments.
- Significant increases in the value of shipments, particularly with electronics products.
- Low priority placed on property thefts by law enforcement.
- Lack of traceability of many electronics products.
- Involvement of organized crime.
- Larger volumes of "just in time" deliveries of stock.

Methods of Cargo Crime:

- Opening containers stacked at terminal yards or transfer facilities, removing goods and transferring them from ports by automobiles or trucks.
- False claims of truck hijacking.
- Dismantling containers, removing the goods and resealing the container.
- Organized networks for spotting, stealing and fencing merchandise.
- Falsifying paperwork.
- Stealing loaded trucks off the street or yard.

Prevention Measures:

- Request a review of packing materials and shipping procedures by an expert in transit procedures.
- Survey the loading, storage and discharge procedures.
- Avoid high-risk shipping locations.

Construction Site Security

Theft of equipment and vandalism are key concerns on any construction site. Whether you are a building owner who is having an additional building constructed on your premises, or the contractor actually performing the work, these guidelines can help reduce the occurrence of loss, keeping the project on schedule and minimizing the bottom line impact. In some jurisdictions, a vandal or someone not authorized to be on the site can bring suit if they are injured on the job site. It could be determined that there was a duty to provide security on part of the owner or the contractor or both.

What can be done? First of all, pre-job planning should include a written job site security plan and a budget should be established to ensure that the proper level of job site security can be maintained. Make superintendents and forepeople aware of the policies and hold them accountable for enforcement.

- Instruct new employees and subcontractors on security practices. Superintendents and forepeople should be responsible for ensuring the policy is communicated during orientation.
- Fence job sites when feasible. Maintain only one gate with some type of security control.
- Control access to job sites at all times. Only authorized visitors, contractors, inspectors and vendors should be permitted on the site. In some cases, it might make sense to accompany visitors through the site if it is necessary for them to go beyond the

trailer area. Parking for visitors and workers should be limited to a controlled area near or outside of the gate.

- Install good nighttime lighting. As discussed previously, lighting should be positioned high enough to eliminate dark areas and minimize the likelihood of vandalism.
- Post warning signs at the job site to keep unauthorized persons off the site.
- Lock and immobilize all equipment during non-working hours. Consider additional anti-theft/anti-vandalism devices such as:
  - Locked hood-side plates
  - Locking steering wheel devices
  - Locking filler caps for fuel, oil, radiators and hydraulic tanks
  - Lockable electrical switches
  - Locked trailer hitches and hitch receivers
  - Protective covers for gauges and window glass
- Consider stolen vehicle recovery systems, such as LoJack®,* which can aid in tracking stolen equipment.

* Travelers has a strategic alliance with LoJack Corporation to provide policyholders with anti-theft products at a reduced rate. A police recovery system is used to recover stolen vehicles and equipment. A small radio transmitter is hidden within the vehicle or equipment and, if reported stolen, a signal from a police radio tower activates the LoJack unit, which then sends a silent signal to police, leading officers directly to its location. While this system is not available in all states at this time, coverage areas are expanding.

- Double stamp tools and equipment with a conspicuous and inconspicuous identification number.
- Verify and document all deliveries of material and equipment.
- Develop an inventory control system for all tools and equipment. Photographs of equipment with accompanying documentation would be very helpful. Remove materials no longer needed at a job site.
- Establish a tool check in/out system.
- Invest in an alarm system, as well as CCTV, depending on the nature of the job site.

Since many job sites now require computers, be sure to do your best to secure the office or trailer where the computer is stored. Back up all important data and store duplicates off site.

The Benefits of Prompt Reporting

By being proactive, you can work to minimize losses and accidents. But when a loss or accident does occur, reporting your claim promptly is extremely important.

When you report your claim promptly, you benefit from:

- A proven, efficient claim handling process.
- Effective cost control for damages, injuries and other expenses.

For more information, visit our Web site at travelers.com/riskcontrol, contact your Risk Control consultant or email Ask-Risk-Control@travelers.com.

TRAVELERS

The Travelers Indemnity Company
and its property casualty affiliates
One Tower Square
Hartford, CT 06183

The information provided in this document is intended for use as a guideline and is not intended as, nor does it constitute, legal or professional advice. Travelers does not warrant that adherence to, or compliance with, any recommendations, best practices, checklists, or guidelines will result in a particular outcome. In no event will Travelers or any of its subsidiaries or affiliates be liable in tort or in contract to anyone who has access to or uses this information. Travelers does not warrant that the information in this document constitutes a complete and finite list of each and every item or procedure related to the topics or issues referenced herein. Furthermore, federal, state or local laws, regulations, standards or codes may change from time to time and the reader should always refer to the most current requirements. This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers, nor is it a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law.