Who is Knocking at your Door? - Burglary and Theft Controls for your Business

Author: Robert Morris, Information Technology Risk Control
Published: January 2021

Executive Summary

The owner of a consumer electronics company locks the doors and arms the burglar alarm system and the end of a workday. Later that night, she receives a call from the police informing her that thieves have driven a truck straight through a loading dock door, filled the truck with the most popular video gaming system products and left the scene before they could respond.

One of the nation's largest pharmaceutical theft [1] was a multi-million dollar heist of prescription products with a high street value from the company's warehouse/distribution center. The intruders used a ladder to access the roof of the building, cut a hole in the roof, lowered themselves down and disabled the burglar alarm system. This gave the thieves enough time to load 40 pallets of high demand prescription drugs into a tractor-trailer and drive away.

Both of these thefts resulted in the loss of valuable inventory, damage to the building and a prolonged disruption to their business operations. These are just two examples of why all businesses should have a site-specific, written security program. A written program consists of the security policies, procedures and controls a business should follow to manage its security risks. One approach is to divide the program into policies and controls that cover:

- Physical Security Controls
- Facility Security
- Employee Oversight
- Inventory Management

The focus of this paper is primarily on the Physical Security Controls a business can implement to help protect its assets and sustain daily operations.

Physical Security Controls

Biometric Physical security measures should be designed to deter, deny, delay and detect unauthorized access to the property's exterior grounds and both the perimeter and interior of the building. These controls include protective barriers, exterior lighting, Closed Circuit TV (CCTV) surveillance, security guards, locks, access control, intrusion detection and other systems designed to protect persons and property. In the words of security expert Bruce Matthews, "The basic role of physical security is to keep unwanted people out, and keep 'insiders' honest."[2]

A company first needs to complete a site specific, physical security threat assessment of the building and grounds. A Certified Security Specialist or qualified Security System Integrator, who will identify vulnerable points of entry and make recommendations on how best to improve the property's defenses, should perform the assessment. A preferred strategy is to create layers of physical security, which would include 1) the outside grounds of the property, 2) the perimeter of the building and 3) the building interior. The extent and strength of the security measures at each layer will primarily depend on the attractiveness from a theft perspective of the facility, its operations and inventory.

The ultimate goal is to have sufficient security for the property to reduce its attractiveness as a potential target for a would-be burglar. Dr. Joseph B. Kuhns of the University of North Carolina at Charlotte, Department of Criminal Justice and Criminology conducted a survey titled "Understanding Decisions to Burglarize from the Offenders Perspective." The researchers examined the decision-making processes and methods of 422 randomly selected incarcerated male and female burglars from three states to understand what motivates and deters them from committing a burglary. Some of the key findings include:[3]

- About 50% reported engaging in residential burglary and 31% committed commercial burglaries.
- A majority of the burglars considered the presence of deterrents such as burglar alarms, outdoor cameras and other surveillance equipment when choosing a potential residential or commercial target.
- 83% said they would attempt to determine if a burglar alarm system was present before attempting a burglary and if present, 60% said they would seek an alternative target.
- 50% reported they would discontinue a burglary attempt if they discovered the presence of a burglar alarm system.
- Video surveillance systems were also cited an as an effective deterrent. Nearly 60% of the burglars said they consider the presence of outdoor cameras and other surveillance equipment when selecting a target, and more than 40% said that would be a factor in prompting them to choose another target.

This study strongly indicates that investing in a well-planned physical security system may very well prevent a burglar from striking your building.

External Security Controls

The first layer of security is the outer perimeter of the building grounds. Physical barriers like walls, fences, bollards and gates are commonly used. Some properties also use natural barriers such as ponds, trenches, embankments or heavy shrubbery. These barriers can act as a psychological deterrent by defining the perimeter grounds of the facility and making an intrusion seem more difficult. Other security measures that help prevent or delay a possible attack include:

- Utilizing heavy-duty padlocks, monitored contact switches or on-site security personnel to secure the gates of a wall or fence.
- Monitoring the more vulnerable sections of the outside perimeter or areas that are difficult to observe with a microwave, infrared beam, vibration detection or another suitable detection system that will initiate an alarm if a person is detected. These motion detection systems will need to be properly maintained and routinely tested to ensure their integrity since the hardware components are exposed to outside elements. Another consideration is that an animal may cause a false alarm.

- Paying attention to the Landscaping around the building to avoid blind spots created by high shrubbery and trees. Good hiding spots for burglars can be prevented by keeping the shrubbery trimmed low to the ground and removing the lower limbs/branches on trees.

- Using exterior lighting within the building grounds. It does not physically prevent a person from entering the grounds but is an effective deterrent at night as the intruders are less likely to enter well-lit areas for fear of being seen. Good lighting around the exterior of the building will also improve the quality of images produced by a CCTV/video surveillance system.

- Installing standard CCTV systems with static or moving cameras are a good start but may result in data overload with the recording of video data from multiple cameras 24 hours per day. To reduce the amount of data being recorded, motion sensor based cameras are available that can be programmed to respond and record automatically only when motion in the camera's frame is detected. Motion activated CCTV camera recording systems can be either based on motion detected through software or passive infrared (PIR) sensors.

- The software based motion activated camera detects motion by comparing pixel changes between successive frames. If a human or animal passes by, different pixels will be counted and the software will trigger a motion activity alert. Smarter systems may use machine learning to distinguish animals or motion caused by wind.

- The PIR motion based camera can detect infrared body heat. When a warm body passes through the viewing area, the ambient IR energy level rapidly changes and will set off a motion activity alert. PIR cameras can have a range up to 100 ft.[4]

- The activity notification alert can be sent by text message and/or email to a mobile device to remotely view live footage. Other available camera features include a siren and light that can be remotely enabled, two-way audio communication to listen to or speak with the person (friend or foe) that triggered the camera, and facial recognition technology to identify familiar faces. The CCTV system can be monitored by an on-site security guard or remotely by a central station alarm monitoring service if rapid response is necessary.

Building Perimeter Security Controls

Physically securing the accessible openings of the building's exterior prevents unwanted entry into the building. The primary method of reducing a "smash and grab" type of theft is through compartmentalization or by layering security controls. The idea is to have the burglars go through multiple barriers before they gain access to high value target items. This slows down the burglar and provides enough time for the police or security service to respond. A number of these controls include:

- Burglar bars installed on windows and skylights.

- Exterior windows and glass pane doors protected with security glazing that meets UL Standard for Safety Burglary Resisting Glazing Material.

- Use of accordion/folding metal gates if loading dock doors need to be left open during the workday. The expandable metal gates should be kept locked when in use.

- Bollards (concrete filled metal posts) located inside the building, to protect ground level or ramp based loading dock doors from being rammed and broken into by a vehicle.

- Roof access is limited to authorized personnel only. Exterior roof access ladders can be provided with a lockable ladder guard and roof hatches can be padlocked from the inside and/or monitored by a magnetic contact switch connected to a burglar alarm system.

- Within the building, store high value target items in a secured room or within a chain link fenced enclosure.

- Avoid storing high value target items next to walls shared with other tenants. Typically, these walls are sheetrock and can be readily penetrated by burglars from an adjoining tenant space. Maintain an open clearance of three to four feet next to a sheetrock wall shared with a tenant and protect the space with beam detectors or motion sensors.

- Secure exterior doors with either a keyed or an electronic locking device to limit access into the building to authorized personnel only. If keys are being used - minimize the number of keys issued to employees, keep a log of who has a key and ensure that key(s) are returned when an employee leaves the company. Strongly consider changing locks if a key is lost or after an employee leaves the company. Traditional lock and key systems are being replaced with electronic locking devices such as keypads, card swipes, biometrics readers and key fobs. These “keyless” access control methods monitor and control traffic through building entry points and maintain detailed entry and exit logs.

- A CCTV/video surveillance system is used to cover the building entrances so the activity can be recorded and/or viewed remotely.

- Magnetic contact switches are used on doors and windows to detect when the door or window has been opened. This type of contact switch is also used on gates, hatches, and other types of accessible openings. A magnetic contact switch has two components installed side by side, with one attached to the door or window while the other is attached to the frame. An alarm is triggered when the two components are separated if a window or door is opened. One way to readily bypass a magnetic contact is to cut through a door or break the window without separating the two parts and triggering an alarm. For this reason, intrusion detection may be necessary to detect such entry.

- Protect exterior window or glass door using a vibration detector that can sense glass breakage. This sensor detects the sound frequencies generated by broken glass and will trigger an alarm. Glass breakage detectors are installed inside the building near the accessible glass windows and doors they are protecting.

Interior Security Control -Visitor Management System

A visitor management system consists of controls that limit the access of visitors within the facility. Special provisions should include verification of the visitor’s identification, handling of “official” visitors (e.g., OSHA, Fire Marshall, etc.) and contractor/utility employees, escorting visitors, restricted areas, and photography restrictions. One effective control is to issue color-coded or readily identifiable ID badges for non-employees such as visitors, contractors, vendors, etc. that will permit or restrict access to sensitive areas. Use of these badges will also easily differentiate company personnel and outsiders within your building.

A CCTV/video surveillance system that covers critical areas can be used to record and/or provide real-time monitoring.

Interior Security Control - Intrusion Detection System

If an intruder manages to gain access into the facility, an intrusion detection system should detect the presence or movement of the intruder and trigger the alarm. The sensor alarm signal is sent to the control panel, triggers the alarm panel, activates local alarm devices like a siren or flashing strobe lights and notifies the central station alarm monitoring service. The typical intrusion alarm system consists of the following four basic components and should use UL listed equipment:

- Detection Devices - Detection devices are the components used to detect the entry of an intruder into the building and send an alert to the alarm control panel. There are many different types of detection devices and each uses a different method to detect the presence of an intruder. The most common types of intrusion detection devices at commercial facilities are:

    - Photoelectric Beam Detectors – These detectors often use a pulsed infrared beam where a transmitter sends out a beam that is detected by the receiver. When the beam is broken by an object, an alarm is generated. The transmitter produces a long, narrow precise beam so multiple transmitters can be stacked to increase the height of the detection area and build a fence-like barrier. This type of detection system may be used behind an exterior perimeter fence (to detect someone cutting through the fence and entering the area) but is most commonly found inside warehouse/distribution buildings located behind the string of loading dock doors. A photoelectric beam detection system is different from a passive infrared (PIR) detector system (see below) because a PIR does not emit a beam but can sense motion when there is a rapid change in the ambient IR energy level - such as when a warm body passes through the sensor's viewing area.

    - Audio/Sound Based Detectors – This detection device is activated by impact/sound and is most often used with a video surveillance system. Upon activation, an alarm is sent to a central station alarm monitoring service where the operator can actually listen and watch the alarm event. The operator will then determine whether this is a legitimate or false alarm and if valid, will notify law enforcement. Sonitrol is a leading vendor in this space and claims their audio sensor can cover up to 5,000 sq. ft. of open space.[5]

    - Passive Infrared (PIR) Motion Detectors – This device looks for a change in infrared energy and can detect the body heat of a person as they pass within the viewing area of the detector. When there is a large enough change in IR energy detected, the device/sensor will alert the system. PIR detectors should be kept 10 to 15 feet away from HVAC vents, not be installed where sunlight would shine directly onto and heat the sensor, and away from heating radiators. This will help prevent a possible false alarm if the sensor detects a rapid change in infrared energy such as an air vent blowing hot or cold air. The detection range for PIR detector can vary significantly. A typical PIR detector can cover an approximate area of 35 ft. x 40 ft. while a long-range detector intended for commercial use like a warehouse and can cover a 60 ft. x 80 ft. area or the range could be extended to 100 ft. x 20 ft.

    - Microwave Motion Detectors – This device is used to detect the presence or movement of people within the building by transmitting microwave signals that reflect/bounce off objects and return to the sensor. An alarm is generated if the pattern of microwave signals is changed by a person or object entering the detection area. Microwave motion detectors can cover a larger area than a PIR motion detector but since the microwave signals can pass through walls and windows, they can possibly sense movement outside the building. For that reason, a microwave sensor is typically paired with a PIR sensor and marketed as a Dual-Tech motion detector.

  - Dual-Tech Motion Detectors - These types of detectors have two sensor technologies in one device such as a glass breakage and a PIR sensor, but the most popular dual-tech motion detector uses a PIR and microwave sensor. With this type of detector, both the PIR sensor and the microwave sensor must be activated within a certain time period before an alarm signal is generated. This greatly reduces the probability of a false alarm since there is very little chance both sensors would accidentally activate at the same time.[6]

  - Other - It is worth noting there are also devices/sensors that detect environmental conditions such as temperature, humidity and moisture. Temperature alarms are commonly used on refrigerators, coolers and freezers for storage of temperature sensitive materials. Moisture sensors can be used to detect water from a broken water pipe.

- Control Equipment -The control panel is the hub of an intrusion alarm system. It is a specialized computer that processes the system's operations and activities. The detection and signaling devices, and the arming station are all connected to the control panel. When a sensor detects a problem, it will transmit a signal to the control panel, which will then activate a signaling device (siren, strobe) and can be programmed to automatically contact an alarm monitoring service. Most control panels operate on batteries that are constantly charged through a low-voltage transformer connected to the building's power supply so they will operate during a power failure.[7] Due to the critical nature of the control panel, it should be installed in a secure closet or equipment room to prevent it from being compromised, disabled or damaged by an unauthorized person. The alarm signal from a detection device is transmitted to the control panel through either a wired or a wireless system.

  - Wired System - A wire is run from the detection devices to the control panel. This type system provides external power to all the detection devices sensors and are typically found in larger buildings. The disadvantages with a wired system are that it can be costly to install and require a professional installer to relocate detection devices if the building's occupancy and/or configuration changes.

  - Wireless System – It will send a signal from the detection devices to the control panel wirelessly using RF communication protocols such as ZigBee, Z-Wave and Wi-Fi. This eliminates the need to run wires but the detection devices will require a battery. Wireless systems are less costly to install and the detection devices can be readily relocated. Disadvantages with wireless signaling devices include:

    - A battery operated sensor has a more limited range so the wireless system may require a repeater to provide a reliable signal to the control panel depending on the distance and the construction materials of the walls and floors.

    - The detection devices have a battery that is subject to failure if not maintained, and the detection device may experience electromagnetic interference from a nearby radio transmission tower, high current machinery, power lines, microwave oven or fluorescent lighting.

    - Although rare, the interference could cause the sensor to fail or possibly trigger a false alarm.[8]

- Signaling Devices - These are the local alarm devices that are activated by a detection device when an intrusion is detected. Both audible and visual signaling devices are available. Examples of audible signaling devices include bells, sirens and voice announcement systems that can deliver a broadcast message to an intruder. Visual signaling devices include revolving, blinking and electronic strobe lights. Most often both audible and visual signaling devices are used and they are normally installed on the inside and outside of the building. Ideally, the local alarm signaling device should cause the intruder to abandon their attempt. The alarms will also alert nearby tenants or neighbors and any employees that may be in the building when an intrusion has been detected.

- Alarm Transmission Equipment - In addition to the local alarm signaling devices, the intrusion alarm detection system generally is connected to a central station alarm monitoring service. The connection can be over the public switched telephone network (PSTN), also known as the plain old telephone service (POTS), a Cellular network or an IP/Broadband signaling path. The alarm monitoring service will then notify law enforcement and/or personnel on the company's call roster that the burglar alarm system has been activated and a response is needed. The alarm transmission equipment can also be arranged to report system troubles, the status of the system such as when the system is armed and disarmed, and condition of the signaling sensors. All three of the alarm signal transmission systems have reliability concerns:
  - POTS lines can be cut by a burglar or aboveground telephone lines can be damaged during inclement weather
  - Cellular systems will not operate if power to the building is lost and there is no battery back-up and the cell signal may slow down during severe weather delaying the alarm signal
  - IP/Broadband communication connection will be lost if the cable leading to the router is disconnected or cut, building power is lost and the router is down (if an Uninterrupted Power Supply has not been provided) or there is a problem with the internet service provider.
    To improve the reliability of an alarm transmission, two separate communication paths should be used to send an alarm signal to the central station. That way, the alarm system has built in redundancy to transmit an alarm signal successfully.[9]
- Central Station Monitoring - The central station for the alarm monitoring service should be UL listed and adhere to UL 827 – Standard for Central-Station Alarm Services. This means the central station building's power supply has a back-up power system, their servers and internet have redundancy, there are at least two trained operators are on duty at all times and more. Compliance with UL requirements demonstrates the alarm monitoring company has met rigorous safety, security and reliability standards.

Conclusion

A major burglary/theft can cause a loss of inventory and property damage. It may also result in a significant disruption to business operations and loss of customers due to delays in restoring the stolen equipment and inventory. Proper insurance coverage and limits can protect your business against theft losses, but it can't financially restore your lost customer base.

Additionally, a robbery during business hours could negatively affect employee safety and in the long term, employee morale. The indirect costs of a robbery could be high.

Good security risk management is essential to ensure adequate protection of your employees, operations, property and inventory from theft due to either external or internal threats. Using the security strategies outlined in this paper, along with administrative controls such as employee oversight and inventory management should reduce the likelihood of a theft. With proper implementation of these controls, the extent of loss from a burglary can be greatly mitigated.

Contact Us

To learn more about how Intact Technology can help you manage online and other technology risks, please contact Dan Bauman, VP of Risk Control at dbauman@intactinsurance.com or 262-951-1455.

References

[9]Ibid 7.

[8](October 9, 2020). Safe Wise. "**Are Wired or Wireless Home Security Systems Better?**" Accessed October 2020.

[7]Home Security Simplified, "**Security System Alarm Panels - The Foundation Of Any Home Security Alarm System**." Accessed October 2020.

[6]"**Dual Tech Motion vs. Traditional Motion**" Alarm Grid. Accessed September 2020.

[5]"**A Better Security System For Distribution Centers**." Sonitrol. Accessed September 2020.

[4]Luo, Flora. (Updated November 26, 2019). "**Hidden Outdoor Motion Activated Cameras: All You Care About**." Accessed September 2020.

[3](May 16, 2013). University of North Carolina at Charlotte. "**Through the eyes of a burglar: Study provides insights on habits and motivations, importance of security**. "ScienceDaily". Accessed September 2020.

[2]Mathhews, Bruce, R. (October 2001). "**Physical Security: Controlled Access And Layered Defense**." Auerbach Publications. Accessed September 2020.

[1]FBI (April 10, 2017), "**Pharmaceutical Theft $60 Million Heist Largest in Connecticut History**." Accessed October 2020.