to investigate a theft unless they have reason to believe it occurred in their city, and the FBI will not investigate unless the loss exceeds $50,000.

Human resource managers and security officers cannot eliminate cargo theft, but they can do much to reduce it by making it less convenient:

- Terminals and loading docks should be secure with perimeter fences, alarm systems, and night lighting. Doors should remain locked when not being used.
- The cargo should be shrink-wrapped with several small cartons placed together on a pallet. This practice reduces the likelihood of someone stealing a single carton.
- All packages should be carefully counted before they leave and when they arrive to make certain all shipments are complete.
- The paperwork accompanying each shipment should require verification of who handles each carton and the time when it is transferred from one terminal to another. This process can be facilitated by bar codes that automatically record the movement of each carton.
- Electronic seals can be attached to trailers that record how many times and when the trailer is opened. These seals provide an audit trail that can be studied when losses occur.
- Satellite dishes can be attached to a truck to track its movements. The dish bounces a signal off a satellite to a monitoring station, pinpointing the location of the truck at all times. Deviations from the scheduled route can be immediately detected.[117]

Control Systems

Physical Security

Physical security systems are designed to protect a company's buildings, equipment, and other assets. The first line of defense is a perimeter fence with locked gates that only allow authorized people to enter. The trend is to have more locked gates and doors and to limit access only to authorized people. Individual cards and access codes have simplified the process of limiting access to approved areas.

Some companies maintain surveillance by using a closed circuit television (CCTV) system that is monitored from a central area with dozens of monitors. Some CCTV systems are constantly operating, while others only operate when they are activated with an alarm or a sensing mechanism triggered by movement. Recordings can be made from the CCTV system and retained for a period of time. These recordings can be very useful in identifying thieves, especially at convenience stores, gas stations, and other vulnerable establishments. Recordings have contributed greatly to the apprehension and prosecution of shoplifters and armed robbers.

CCTV equipment designed to observe what is happening is often installed in full view of the public. A visible system also serves to deter crime by letting subjects know they are under surveillance. Occasionally, however, a covert installation is more useful. For example, in the produce departments of grocery stores, where sprinkler systems are used, about 90 percent of the slip-and-fall claims are fraudulent and can be exposed by a hidden camera. Using a hidden camera makes it more likely that an unsuspecting violator will be viewed, recorded,

and apprehended while committing the act. Covert installations also avoid changing the aesthetics of a building or room. The most common covert systems use lenses that are mounted behind pinholes or mirrors in walls, camouflaged in ceiling-mounted sprinkler heads, or positioned in dome-shaped mirrors where they can be directed. Using fiber-optics, the lens can be located several feet from the camera, such as on the other side of a thick wall or in a different room.[118]

Disturbance

Disturbances present difficult challenges to security personnel because the disturbance may be caused by the company's own employees. Strikes and picket lines often result in disturbances that lead to violence and damage. Companies have an obligation to protect both their assets and the lives of their employees, some or all of whom may be causing the disturbance.

When violence is threatened, companies need to notify all concerned individuals about the threat. Employees and customers should be given an overview of the situation, and they should be given new information any time the situation changes.

Additional security personnel should be put in place immediately to maintain peace. Local law enforcement agencies should be notified and asked to provide assistance.

An accurate record of the disturbance should be made—including photos, videotaped recordings, and lists of names and license plate numbers.

When strikers engage in violent and disruptive behavior, the company can seek an injunction ordering the union to cease illegal activities.

Parking and Traffic

Parking areas are most dangerous at night in high crime areas. Lighting is one of the most effective deterrents to crime in parking lots. If employees come to work or leave work at times when they would have to find their cars in a dark parking lot, employers should provide lighted parking areas. Employees who feel unsafe should be able to ask for someone to accompany them to their cars. Closed circuit television also adds to the security of a parking area.

If employee parking lots are located in areas where parking is limited, access to the employee parking area should be restricted to those who are authorized to park in that area. Access can be limited by gates and barricades that are activated by an electronic card.

Entry Systems

Entry systems are involved in controlling the ingress and egress of people using physical controls, identification systems, and security points. Typical control points include driveways, walkways, perimeter lines, front doors, back doors, and loading docks. A typical access system requires a card that is electronically coded.

Recent developments in biometrics can allow or restrict the entry of people based on their fingerprints, the iris and retina of their eyes, or their voice. These biometric features are unique to each person, especially fingerprints, the iris, and the retina. In no case have

duplicates been documented in these three features. The disadvantage of **biometric access devices** is that the instruments for reading them are considered slow, unreliable, and intrusive:

- Biometric access devices only have the capacity to admit a maximum of about six to ten people per minute.
- The instruments are occasionally unreliable because of accumulations of dirt and oils from repeated contact.
- Some people find them obtrusive and object to using them, especially retina scan systems, because of fears about the spread of communicable diseases. Iris readings are more acceptable, however, because the readings are made at a distance.[119]

Simple locks and keys have the advantage of being inexpensive and easy to install. The disadvantage of locks and keys is that keys can be duplicated or lost and re-keying all of the doors or locks can be very inconvenient and expensive. Electronic card access systems have the advantage of providing greater control and information. Cards can be coded electronically to record the time each person enters or leaves a particular area. Access can be limited to certain times of the day or week. Placing photographs on the cards or having employees use their own personal credit cards decreases the likelihood that the cards will be lost or improperly used by someone other than the employee.

A theory for evaluating and improving the accuracy of entry systems is called **"signal detection theory."** This theory is a systematic approach for studying human vigilance and categorizing the kinds of mistakes human monitors are likely to make. Exhibit 10 is a two-by-two matrix that shows the four kinds of decisions that can be made by a human monitor, such as an officer monitoring a metal detector at an airport.

Exhibit 10: Signal Detection Theory

		Environmental Situation	
		Actual Threat	*No Threat*
Officer's Action	*Detects Threat*	Hit	False Alarm
	No Action Taken	Security Breach	True Miss

According to signal detection theory, two factors influence the accuracy of a human monitor's performance: the detectability of the target and the monitor's bias or expectancy that the target will appear. The detectability of the target (such as a gun or an unauthorized

person trying to enter a facility) is influenced by the amount of "background noise" associated with the target. Background noise could be glare on an x-ray screen, weapons with too little metal to detect, forged passes, or large crowds of people trying to enter. Accuracy depends partly on the signal-to-noise ratio: as the signal from the target decreases or the amount of noise increases, the monitor's performance declines.

The bias or expectancy of discovering the target influences the likelihood that the monitor will actually see it. If the target rarely appears, monitors become accustomed to not seeing it and are more likely to miss it. If the expectancy of seeing a target increases, however, the monitor will be more likely to report seeing it both when it is there and when it isn't.

According to signal detection theory, people differ in their ability to detect visual signals within a visual background and people with this aptitude should be selected for these kinds of monitoring jobs. The performance of monitors can also be improved with frequent reinforcement, including record keeping and expressions of appreciation.[120]

Electronic Security Devices

Numerous electronic devices have been designed to make companies more secure. In deciding whether to use an electronic security device it is important to remember their limitations:

- Alarms do not prevent trouble; they only detect trouble.
- No alarm is useful if there is no person to respond to it.
- Alarms do not replace guards; they only assist guards.

Many different kinds of alarms are available to increase the security of assets, and choosing the best alarm depends on the purpose of the alarm and the nature of the threat:

- Contact alarms use a spring, a microswitch, or a magnetic switch to sense contact.
- Stress alarms sense pressure, such as mats.
- Vibration or tamper alarms use mercury switches to sense the vibrations of movement.
- Lacing alarms consist of a network of wires running through a wall to detect penetration.
- Photoelectric beam alarms are triggered when the beam is broken.
- Capacitance alarms utilize an electromagnetic field.
- Motion alarms send ultrasonic, microwave, or non-audible radio waves into an area and monitor any disruption of the established wave.
- Infrared alarms detect a change of temperature.
- Smoke or flame alarms have a chemical sensor that detects smoke.
- Duress alarms are activated when someone wants to signal danger, such as a robbery.
- Closed circuit television (CCTV) requires someone to monitor what is recorded and respond to unauthorized conditions.